

THE CO-EVOLUTION OF NETWORKED TERRORISM AND INFORMATION TECHNOLOGY

Peter J. Cluskey, MA

THE CO-EVOLUTION OF NETWORKED TERRORISM AND INFORMATION TECHNOLOGY

THESIS SUBMITTED FOR THE AWARD OF THE DEGREE OF
DOCTOR OF PHILOSOPHY
SCHOOL OF LAW AND GOVERNMENT
DUBLIN CITY UNIVERSITY

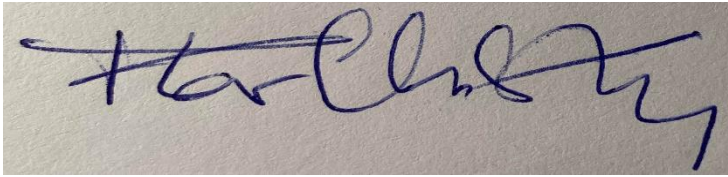
PETER J. CLUSKEY, BA, MA

RESEARCH SUPERVISOR
PROF. MAURA CONWAY

JANUARY 2023

Declaration

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of PhD is entirely my own work, and that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

A photograph of a handwritten signature in blue ink on a light-colored surface. The signature is cursive and appears to read 'Peter Cluskey'.

Signed:

Peter J Cluskey MA

Student ID No.: 17210304

Date: 2.3.2023

Acknowledgments

To my late wife, Adrienne Cullen, conferred with the degree of Doctor of Laws (Honoris Causa) by the National University of Ireland at UCC on December 10, 2018. I'm catching up, kiddo!

To my academic supervisor, Prof. Maura Conway, as patient, wise, and erudite as I could have hoped for ...

And to the family and dear friends who kept me going ... You know who you are and how much I appreciate it ...

Knowledge must become capability

Carl von Clausewitz, *Vom Kriege*, 1832

Table of Contents

List of abbreviations.....	1
ABSTRACT	3
INTRODUCTION	4
The road to co-evolution	4
Complexity: a twenty-first century perspective	6
Terrorism and the media: Updating a dated perspective.....	9
<i>Terrorism and media: the traditional perspective</i>	<i>10</i>
<i>Terrorism and media: the complexity perspective</i>	<i>12</i>
The evolutionary trajectory of information technology.....	14
The contribution of this thesis.....	16
The structure of the thesis	16
CHAPTER ONE The ‘symbiotic’ relationship between networked terrorism and information technology: A review of the literature, re-interpreted in light of complexity theory.....	20
Introduction.....	20
The road to ‘informationalism’	22
Terrorism in the new digital landscape	26
The terrorism-technology nexus and the internet.....	28
The spread of networked terrorism	30
The emergence of ‘information-age threats’	33
Information: lifeblood of a networked world.....	36
The shock of 9/11: Understanding a new and complex opponent	38
Social media: Terrorists’ ‘open social utility’	41
The contribution of this thesis: pre-complexity terrorism meets co-evolution.....	43
Conclusion	48
CHAPTER TWO The theoretical route to co-evolution: Networked terrorism and information technology as complex adaptive systems in pursuit of ‘significantly augmented performance’	50
Introduction.....	50
The historical roots of complexity science	52
Complex adaptive systems	55
Genetic algorithms: the key to co-evolution	57
How co-evolution becomes a force multiplier for terrorism	60
Terrorism and information technology as complex adaptive systems.....	63
<i>Terrorism as a complex adaptive system.....</i>	<i>63</i>
<i>Information technology as a complex adaptive system.....</i>	<i>71</i>

Terrorism, information technology and the role of communication	76
Conclusion	77
CHAPTER THREE Aligning methodology with complex ontology: Designing a template to investigate the co-evolution of networked terrorism and information technology.....	79
Introduction.....	79
Process tracing and the route to causality	81
<i>Process tracing: minimalist and systems understandings.....</i>	<i>84</i>
<i>Process tracing: assessing the causal evidence.....</i>	<i>86</i>
Process tracing in a complex adaptive world	89
<i>Causal process tracing and the importance of time</i>	<i>90</i>
<i>Causal process tracing and configurational thinking.....</i>	<i>91</i>
Process tracing and case studies.....	92
<i>Hezbollah and satellite technology</i>	<i>93</i>
<i>Al-Qaeda and the internet</i>	<i>94</i>
<i>Islamic State and social media.....</i>	<i>96</i>
<i>The order of the case studies</i>	<i>98</i>
<i>The data sources</i>	<i>99</i>
Testing causal inference across the case studies	102
<i>The Bayesian tests.....</i>	<i>103</i>
Conclusion	105
CHAPTER FOUR Deadly Embrace 1 – Hezbollah and satellite broadcasting as co-evolutionary partners in a mutually beneficial trajectory towards greater scale and interoperability .	107
Introduction.....	107
<i>Hezbollah in its political setting</i>	<i>109</i>
<i>Hezbollah in its technological setting</i>	<i>111</i>
Test 1: Hezbollah – linear tacticians or complex network?	112
<i>The Lebanese state and the emergence of Hezbollah.....</i>	<i>112</i>
<i>Hezbollah: From armed militia to international terrorism.....</i>	<i>114</i>
<i>An Iranian proxy with a global terrorism mandate.....</i>	<i>116</i>
Test 2: Hezbollah – satellite TV and autonomous communication	118
<i>Satellite television and the global village.....</i>	<i>118</i>
<i>Hezbollah and the weaponization of information</i>	<i>119</i>
<i>Hezbollah and ‘autonomous communication’</i>	<i>121</i>
Test 3: Satellite broadcasting as a force multiplier for Hezbollah.....	124
<i>Hezbollah: Spearhead of the ummah.....</i>	<i>124</i>
<i>Hezbollah: Global reach and global terrorism</i>	<i>126</i>
<i>Hezbollah: The ‘divine victory’ of 2006</i>	<i>128</i>
Test 4: Estimating the causal credibility of co-evolution.....	130
<i>Test 1 Reviewed: Hezbollah as complex adaptive system.....</i>	<i>130</i>
<i>Assessment</i>	<i>132</i>
<i>Test 2 Reviewed: Satellite TV and autonomous communication</i>	<i>132</i>

<i>Assessment</i>	133
<i>Test 3 Reviewed: Satellite TV as a force multiplier</i>	133
<i>Assessment</i>	135
Conclusion	135
CHAPTER FIVE Deadly Embrace 2 – How Al-Qaeda leveraged the internet, the most powerful new technology since Gutenberg, to stage the world’s most lethal terrorist attack	136
Introduction	136
<i>Al-Qaeda in its political setting</i>	137
<i>Al-Qaeda in its technological setting</i>	139
Test 1: Al-Qaeda – linear tacticians or complex network?	140
<i>Al-Qaeda: Why Islamic terrorism is amenable to complex structures</i>	140
<i>Al-Qaeda: From mujahideen to global jihad</i>	142
<i>Al-Qaeda: The deterritorialization of jihadist terrorism</i>	144
Test 2: Al-Qaeda – the internet and autonomous communication	146
<i>Al-Qaeda and the internet: controlling the message</i>	146
<i>Al-Qaeda: Weaponising the internet</i>	148
<i>Al-Qaeda and autonomous communication</i>	150
Test 3: 9/11 and the internet as a force multiplier for Al-Qaeda	152
<i>Al-Qaeda: How the internet enabled 9/11</i>	152
<i>Al-Qaeda: The 9/11 attacks</i>	154
<i>9/11 The Aftermath</i>	156
Test 4: Estimating the causal credibility of co-evolution	158
<i>Test 1 Reviewed: Al-Qaeda as complex adaptive system</i>	158
<i>Assessment</i>	160
<i>Test 2 Reviewed: The internet and autonomous communication</i>	160
<i>Assessment</i>	161
<i>Test 3 Reviewed: The Internet as a force multiplier</i>	162
<i>Assessment</i>	163
Conclusion	164
CHAPTER SIX Deadly Embrace 3 – How Islamic State ‘microstructures’ mimicked the decentralised architecture of social media by choosing unilaterally how and when to attack	165
Introduction	165
<i>Islamic State in its political setting</i>	167
<i>Islamic State in its technological setting</i>	168
Test 1: Islamic State – linear tacticians or complex network?	169
<i>The emergence of Islamic State, networked ‘progeny’ of Al-Qaeda</i>	170
<i>Islamic State: From local breakaway to global jihadist threat</i>	172
<i>Islamic State: the ‘caliphate’ that came ‘out of nowhere’</i>	174
Test 2: Islamic State – social media and autonomous communication	176
<i>Islamic State and the emergence of social media</i>	176
<i>Islamic State: the weaponisation of social media</i>	177
<i>Islamic State and autonomous communication</i>	180

Test 3: Islamic State and the force multiplier effect of social media	182
<i>Islamic State's capture of Mosul: 'blitzkrieg' in northern Iraq</i>	<i>182</i>
<i>How social media enabled Islamic State's reign of terror in Europe.....</i>	<i>185</i>
<i>Islamic State: The aftermath and what has changed</i>	<i>187</i>
Test 4: Estimating the causal credibility of co-evolution.....	189
<i>Test 1 Reviewed: Islamic State as complex adaptive system</i>	<i>189</i>
<i>Assessment</i>	<i>190</i>
<i>Test 2 Reviewed: Social media and autonomous communication</i>	<i>190</i>
<i>Assessment</i>	<i>192</i>
<i>Test 3 Reviewed: Islamic State and the force multiplier effect of social media</i>	<i>192</i>
<i>Assessment</i>	<i>193</i>
Conclusion	194
CONCLUSIONS	196
Introduction.....	196
Key findings of this thesis	197
Twenty-first century terrorism: a new interpretation	202
Implications for counterterrorism	204
Areas for further study.....	206
REFERENCES	210

List of abbreviations

AK47	Avtomat Kalashnikova or Kalashnikov
ABC	American Broadcasting Company
AQI	Al-Qaeda in Iraq
AQIM	Al-Qaeda in the Islamic Maghreb
ARPANET	Advanced Research Projects Agency Network
BAAD	Big, Allied and Dangerous
BBC	British Broadcasting Corporation
CAS	Complex adaptive system
CIA	Central Intelligence Agency
CPT	Causal process tracing
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
DARPA	Defence Advanced Research Projects Agency
DNA	Deoxyribonucleic acid
ENIAC	Electronic Numerical Integrator and Computer
EU	European Union
GPS	Global positioning system
GPT	General purpose technology
ICBM	Intercontinental ballistic missile
IDF	Israel Defence Forces
IRGC	Islamic Revolutionary Guard Corps
IS	Information system
MAK	Maktab al-Khidamat, known as Afghan Services Bureau
MENA	Middle East and North Africa
MIT	Massachusetts Institute of Technology
MRTA	Movimiento Revolucionario Túpac Amaru

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NBC	National Broadcasting Company
PLO	Palestinian Liberation Organization
PFLP	Popular Front for the Liberation of Palestine
RNA	Ribonucleic acid
SDF	Syrian Democratic Forces
TCP/IP	Transfer control protocol/internet network protocol
TV	Television
UK	United Kingdom
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
US	United States of America
WEF	World Economic Forum
WWII	World War Two

ABSTRACT

Thesis title: The co-evolution of networked terrorism and information technology

PhD candidate: Peter J. Cluskey MA

This thesis describes for the first time the mechanism by which high-performing terrorist networks leverage new iterations of information technology and the two interact in a mutually propulsive manner. Using process tracing as its methodology and complexity theory as its ontology, it identifies both terrorism and information technology as complex adaptive systems, a key characteristic of whose make-up is that they co-evolve in pursuit of augmented performance. It identifies this co-evolutionary mechanism as a classic information system that computes the additional scale with which the new technology imbues its terrorist partner, in other words, the force multiplier effect it enables. The thesis tests the mechanism's theoretical application rigorously in three case studies spanning a period of more than a quarter of a century: Hezbollah and its migration from terrestrial to satellite broadcasting, Al-Qaeda and its leveraging of the internet, and Islamic State and its rapid adoption of social media. It employs the NATO Allied Joint Doctrine for Intelligence Procedures estimative probability standard to link its assessment of causal inference directly to the data. Following the logic of complexity theory, it contends that a more twenty-first century interpretation of the key insight of RAND researchers in 1972 would be not that 'terrorism evolves' but that it co-evolves, and that co-evolution too is arguably the first logical explanation of the much-vaunted 'symbiotic relationship' between terrorists and the media that has been at the heart of the sub-discipline of terrorism studies for 50 years. It maintains that an understanding of terrorism based on co-evolution belatedly explains the newness of much-debated 'new terrorism'. Looking forward, it follows the trajectory of terrorism driven by information technology and examines the degree to which the gradual symbiosis between biological and digital information, and the acknowledgment of human beings as reprogrammable information systems, is transforming the threat landscape.

INTRODUCTION

The personal and social consequences of any medium – that is, any extension of ourselves – result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology.

McLuhan, *Understanding Media: The Extensions of Man*, 1967

The road to co-evolution

This thesis is a story of irresistible magnetism that has led to a long-term relationship driven by one word: co-evolution.¹ It shows for the first time how networked terrorists and information technology, the pairing at the heart of the relationship, can be seen to co-evolve in a mutually propulsive manner when examined through the prism of complexity science.² That new perspective identifies both elements of this pairing as complex adaptive systems, key components of complexity theory constantly in search of co-evolutionary partners that can ‘significantly augment’ their performance together (Holland 1992b, p. 11), ensuring the survival of both. Pairings that are mutually beneficial become stronger and more influential in their ecosystems; failures fall by the wayside. System design is parsimonious and widely replicated in nature, and this novel mechanism can be described as a classic information system, defined as ‘a set of interrelated components that collect (or retrieve), process, store, or distribute information in support of decision-making and control in an organisation’ (Laudon and Laudon 2000, pp. 44-45). Both the consistency of the mechanism’s key elements over time and the manner in which it processes information internally are examined in three case studies matching Hezbollah, Al-Qaeda, and so-called Islamic State with the new iterations of information technology that each adopted at its height and used to devastating effect over a combined period spanning more than a quarter of a century, namely: satellite broadcasting, the internet, and social media, respectively. The co-evolutionary mechanism,

¹ As McShea (1996, p. 477) notes: ‘The centrepiece of the case for a pervasive evolutionary trend in complexity has always been a story ...’

² Complexity science is a set of concepts and tools that sets out the theory behind complex adaptive systems, systems that are characterised by their constant interaction so that they are dynamic, non-linear, self-organising and unpredictable, broadly the opposite of the old mechanistic one-dimensional view of how systems worked. The body of knowledge that explains how and why complex adaptive systems function as they do is called complexity theory. Its central tenets are set out in some detail in Chapter Two of this thesis. For more on the key concepts, see also Holland 1992a and Holland 2014.

therefore, comprises three core elements, (i) a new iteration of information technology and (ii) a high-performing terrorist network leveraging that new technology, combined with (iii) evidence of a significant force multiplier effect (Hurley 2005) as a result of their frequently unpredictable interaction. As Karin Knorr Cetina (2005, p. 214) observed about 9/11: 'Complexity is geared to just such (seeming) contradictions as the disproportion between a fragile group of plotters and the devastating global effects of their actions'.

Technological change is a form of evolution (Fleming and Sorensen 2001, p. 1037), and borrowing biological frameworks to help understand both has a long and fruitful scientific history (Abernathy and Utterback 1978; Schumpeter 1942; Gilfillan 1935). In this case, the relationship between the three key elements of the co-evolutionary mechanism is not unlike the relationship between DNA, RNA and proteins and the specific process by which genetic information moves between them.³ It follows a basic input-processing-output logic typical of information systems, although that does not suggest that the information is simply transferred from one to the other. In the case of DNA-RNA-Protein, DNA contains the genetic code which is *transcribed* into RNA, where it is available to be processed. RNA then processes or catalyses that code by *translating* it into proteins, which provide structure to cells and organisms (Isaacson 2021, pp. 43-44; Clancy and Brown 2008), and for that reason are sometimes popularly known as 'the building blocks of life'. The co-evolutionary mechanism described here mirrors that design. In the case of input, the system architecture of the new iteration of information technology, essentially its code, will determine how the force multiplier effect will ultimately express itself. In relation to processing, the terrorist network in its interaction with the technology acts as a catalyst for the force multiplier effect. As a result, the output is communication (Jenkins 2015a) in the form of the terrorist attack, using the new information technology in a manner consistent with its design, while also achieving the element of 'surprise' specified by Crenshaw (1987) as characteristic of terrorism 'par excellence'.

In the detail of its structure, the co-evolutionary mechanism sits comfortably with social systems as defined by Luhmann (2002, 1995, 1987, 1986), who, uniquely in sociology, promotes communication, in particular the specifics of how information is dealt with to

³ This DNA-RNA-Protein relationship is described by Crick (1970) as 'the central dogma' of molecular biology.

achieve understanding and communication (Lenartowicz et al. 2016, p. 17), to the dominant position in the pantheon of life systems, reflecting the central position it also occupies in terrorism studies (Jenkins 2015a; Nacos 2007, p.14; Hoffman 2006, p. 198), while relegating human actors to the role of catalysts. This will be discussed in greater detail later, but it is worth noting here that the broad focus on information as the 'lifeblood' of terrorism⁴ reflects a dramatic change of emphasis in counterterrorism since 2016 when the United States added gene editing as a potential weapon of mass destruction to its annual Worldwide Threat Assessment report (Regalado 2016). Gene editing established human beings definitively as reprogrammable information systems and was the only biotechnology with the potential to be used as a 'bioweapon' that was listed as a threat by US Director of National Intelligence, James Clapper. Although it is not mentioned by name in the intelligence assessment, it is believed the security concerns refer, in particular, to the gene editing system CRISPR⁵ (Doudna 2020; Doudna and Charpentier 2014) because of its relative ease of use and low cost.⁶ These developments underline the degree to which the gradual symbiosis between biological and digital information already being expressed through artificial intelligence has the potential for 'virtually limitless recombination' in the rapidly approaching future (Gillings et al. 2016), and the degree to which complexity theory has the unique cross-disciplinary capacity to provide an appropriately multi-faceted explanatory insight into such challenges.

Complexity: a twenty-first century perspective

In the cultural history of ideas, complexity science is to be found 'right in between modern and post-modern science' (Emmeche 1997, p. 3) where the former involves normative notions such as the steady progression of knowledge and man's increasing mastery over nature, and the latter questions the possibility of that mastery and doubts the 'linear accumulative progress of knowledge'.⁷ It positions the physical world 'in the midst of a major

⁴ A paraphrase of the observation that information is 'the new lifeblood of the international system' (Conway 2003, p. 1)

⁵ CRISPR stands for Clustered Regularly Interspaced Short Palindromic Repeats (Kosal 2020, p. 599).

⁶ As a result, the Defence Advanced Research Projects Agency (DARPA) in the US launched Safe Genes, a programme aimed at defending against terrorist use of genetically engineered weapons, with grants of \$65 million (Isaacson 2021, pp. 259-263).

⁷ Deuchars (2010, pp. 161-168) attempts to 'sketch' this intermediary ground on the basis of what he says is 'a growing recognition that phenomena in the physical sciences may share similar patterns with complex social

evolutionary transition that merges technology, biology and society' to the point where digital technology has already infiltrated the fabric of civilization to a degree of 'indisputable and often life-sustaining dependence' (Gillings et al. 2016, p. 11). In essence, complexity science is a way of interpreting the world which focuses on systems as 'live' perpetual-emergence machines driven by the interaction of their components, in much the same way that weather is generated by the interaction of pressure and temperature, powered by the heat of the sun. From such interactions 'large-scale patterns and systems emerge, ones that are rarely considered optimal or well-oiled but that generally work well for at least a sizeable fraction of the people' (Downing 2015, p. 1). Systems that evolve in this way are known as 'complex adaptive systems',⁸ everything from the human brain and immune systems to economies and languages, 'a variety of systems as diverse as the planet itself' (Downing 2015, p. 1). They are self-generating through a process of interaction leading to change known as autopoiesis⁹, first introduced by evolutionary biologists Umberto Maturana and Francisco Varela (1972) in their book, *Autopoiesis and Cognition: The Realization of the Living*. Having autogenerated themselves in this way as a result of their compulsion to interact, complex adaptive systems then use that evolutionary imperative to constantly seek dominance in the environment of which they form part by identifying other systems with which they can interact and co-evolve. Beneficial interactions bias a complex adaptive system towards repeated interaction and thus co-evolution (Holland 1992a, p. 24; 1975, pp. 89-140). Look under the bonnet of a complex adaptive system and what it reveals is that all evolution entails co-evolution. 'The true and stunning success of biology reflects the fact that organisms do not merely evolve', writes Kaufmann (1993, p. 237), 'they *co-evolve* both with other organisms and with a changing abiotic environment' (author's italics). To understand complexity theory is to understand the very nature of change, says quantum physicist Heinz Pagels (1988, p. 15). 'The nations and people who master the new sciences of complexity will become the economic, cultural, and political superpowers of the twenty-first century'. Stephen Hawking agreed:

systems'. This will lead, he anticipates, to a different type of intellectual engagement between the two, and a transformation in 'thinking about what we think we know about world politics'.

⁸ Sometimes shortened to CAS for both singular and plural.

⁹ From the Greek words '*auto*' meaning 'self' and '*poiesis*' meaning 'creation'.

We have already discovered the basic laws that govern matter and understand all the normal situations. We don't know how the laws fit together ... But I expect we will find a complete unified theory sometime this century. There is no limit to the complexity we can build using those basic laws. (Hawking 2000)

Complexity theory has thus far been used predominantly on the margins of terrorism studies, mainly to model covert terrorist networks with the aim of understanding and disruption (Tsvetovat and Carley 2005; Carley et al. 2004; Carley et al. 2003; Carley et al. 2002; Carley 2002; Krebs 2002).¹⁰ This thesis, however, goes substantially further. Examining each from the viewpoint of complexity, it will demonstrate that both terrorism and information technology may reasonably be defined as complex adaptive systems. As a consequence, they can also be shown to co-evolve, a core characteristic of such systems, in a manner that is mutually beneficial and that augments the effectiveness of both (Holland 1992a, p. 19). In the case of information technology, mission-driven adoption by terrorists catalyses evolution, and each new iteration leads to greater interoperability¹¹ between systems, which, in turn, enables greater technological scale and reach (Elkhodr et al. 2016; Heubusch 2006, pp. 26-30). In the case of terrorism, the new iterations of information technology allow terrorist networks to evolve operationally in how they strategize, plan and attack, as all three case studies illustrate. At the same time, the increased interoperability amplifies their messaging, enables greater autonomy of communication (Conway 2005, p. 9), and therefore elevates the threat they pose in a 'hyperconnected world' (WEF 2013b; WEF, 2013a) where the ever-increasing speed of interaction drives unpredictability and hinders effective response. This thesis not alone identifies the novel mechanism by which co-evolution occurs in terrorism but goes on to test its applicability and consistency across its three case studies – Hezbollah and satellite broadcasting, Al-Qaeda and the internet, and Islamic State and social media – spanning more than two decades of rapid change, using the NATO Allied Joint Doctrine for Intelligence Procedures (NATO-AJP-2.1) estimative probability standard to challenge and confirm the logic of each study.¹² On the basis of that re-interpretation, it will argue that,

¹⁰ It largely replaced old-style link analysis (Harper and Harris 1975) used by law enforcement agencies.

¹¹ Interoperability is the breaking down of internal barriers in successive iterations of information technology, allowing friction-free information exchange between systems (Elkhodr et al. 2016).

¹² The NATO Allied Joint Doctrine for Intelligence Procedures (NATO-AJP-2.1) expresses the estimative probability of intelligence using five verbal terms with associated probability ranges: Highly likely, more than 90%; Likely, 60 to 90%; Even chance, 40 to 60%; Unlikely, 10 to 40%; Highly unlikely, less than 10%. Analysts are explicitly discouraged from using the term 'confirmed' which is therefore omitted from the standard 'given the nature of intelligence projecting forward in time' (Irwin and Mandel 2020). The NATO standard is applied in this

contrary to the view of the 9/11 Commission Report in its executive summary (2004, p. 9) that the most important intelligence failure on 9/11 'was one of imagination', it was instead a failure of understanding.¹³

Terrorism and the media: Updating a dated perspective

It is a thread running from beginning to end of his thesis that technological evolution drives change more relentlessly than is generally realized. Gillings et al. (2016, p. 11) note that when examined across paradigms¹⁴ it 'shows signs of being super-exponential'. Taken together with the naturally propulsive power of co-evolution, this explains not alone the capacity of high-performing terrorist networks to excel as early adopters of new information technology, but it explains the logic behind the long-standing contention that there is some form of 'symbiotic relationship' (Wilkinson 2006, p. 145) between terrorism and the media. For many years this relationship was believed to have been one of mutual manipulation (Conway 2004, p.3) between terrorists and the media in the sense of working journalists/editors/producers, whereby terrorists staged 'spectaculars' (Hoffman 2002, p. 309; Bell 1978) with the aim of achieving the maximum media coverage, and journalists worked on the cynical basis that 'If it bleeds, it leads' (Carnegie Council 2016), knowing that terrorism and bloodshed increase sales and ratings. That view, however, was simplistic. It failed to acknowledge the wide range of responsible media outlets, suggesting instead the broad complicity of an entire industry, an idea dismissed by Picard (1986), subsequently to lead the Reuters Institute at the University of Oxford, as 'dangerous charges backed by dubious science'. This thesis proposes instead that co-evolution is the logical answer to the question of why some networked terrorists and specific iterations of information technology work together to such lethal effect. It is explained by the 'super-additivity' (Downing 2015, p. 2) that is generated when technology is undergoing a 'phase transition' (Langton 1992, 1990) from one iteration to another and is therefore on 'the edge of chaos' (Kaufmann 1991, p. 1), where the rate of

thesis in three case studies, Hezbollah and satellite broadcasting, Al-Qaeda and the internet, and Islamic State and social media, set out in Chapters Four, Five and Six.

¹³ The aim of 'irregularization' in information warfare or manipulation, says Rothrock (1979) is 'the degradation of ... adversaries' capacity for *understanding*' (author's italics).

¹⁴ 'New computational platforms, from nano-technological modelling of neurons to developments in quantum computing, provide justification that artificial processing might maintain its exponential growth even beyond its silicon basis' (Gillings et al. 2016, p. 11).

evolution is naturally maximised (Kaufmann 1991, p. 3). In the case of terrorism, that super-additivity translates into a formidable force multiplier effect for high-performing terrorists, and, in terms of mutual benefits, copperfastens the co-evolutionary relationship between them. In effect, symbiosis *is* co-evolution. Because that transition from a pre-complexity view of the relationship between terrorism and the media to one mediated by complexity theory is at the heart of this thesis, it will (i) compare now in more detail the workings of both perspectives and the path between them; (ii) look at the evolutionary trajectory of the information technology involved, and (iii) preview the progression of the argument through the chapters that follow.

Terrorism and media: the traditional perspective

Much has been written about the relationship between terrorism and the media (Conway 2008b, 2007, 2004, 2003; Hoffman 2007, 2006; Nacos 2007, 2006, 1994; Ross 2007; Cohen-Almagor 2005; Chitty et al. 2003; Hess and Kalb 2003; Norris et al. 2003; Paletz and Schmid 1992; Alali and Eke 1991; Alexander and Picard 1991; Midgley and Rice 1984; Jenkins 1974). It has been well established that terrorism is fundamentally about communication. 'Terrorism, by its very nature, is a psychological weapon which depends upon communicating a threat to a wider society', wrote Wilkinson (2006, p. 145), adding that this, in essence, was 'why terrorism and the media enjoy a symbiotic relationship'.¹⁵ Jenkins (1974, p. 4) described terrorism as 'theatre' in that its violence was aimed not at its immediate victims but 'at the people watching'. For that reason, it was undeniably 'a form of psychological warfare', said Hoffman (2007). Schmid and De Graf (1982, p. 14) touched an appropriately primeval note when they likened the victim of terrorism to 'the skin on a drum beaten to achieve a calculated impact on a wider audience'. Nacos (2007, 2006, 1994) and Nacos et al. (2011) characterized terrorism as 'mass-mediated', suggesting that the proliferation of media outlets as a result of cheaper technology had resulted in 'greater competition and insatiable appetites for shocking, sensational infotainment' (Nacos 2006, p. 11). A widespread subtext was that the media in general were responsible for a calculated descent into sensationalism, often simply by reporting terrorist incidents. While critics of the media were undoubtedly correct

¹⁵ In terms of complexity theory, given our improved understanding, one might now, of course, for 'symbiotic relationship' read 'co-evolving relationship'.

in many instances – though, in fact, sensationalism is just one of six ‘difficulties’ with media coverage of terrorism identified by Ross (2007, pp. 217-218) – it was the acceptance of this proposition in some quarters as an incontrovertible truth which sent a good deal of the debate off the rails. Dowling (1986) went so far as to contend that terrorists only existed in liberal societies because of the media.

Cultural theorist Stuart Hall sounded a valid though largely ignored warning (1973, p. 181) that ‘news values’ were ‘one of the most opaque structures of meaning in modern society’. However, the very fact that media organisations were commercial enterprises whose *raison d’être* was to sell news to their target audiences was taken in some quarters as verging on the disreputable, indisputable evidence that they were incapable of any response but sensationalism. As Walter Lippmann (1997, p. 203) famously observed as far back as the 1920s, such critics expected ‘the fountains of truth to bubble’ no matter ‘how unprofitable the truth may be’. British Prime Minister Margaret Thatcher, outraged by a series of high-profile international airliner hijackings (BBC News 2001), set the tone. For her, the media, no matter how critical their journalism, were a means of channelling ‘the oxygen of publicity’ to terrorists (Thatcher 1985). In addition, there was little clarity about what exactly was meant by ‘the media’. Was it the breathless reporters on the ‘front line’ or their editors and producers; the politically influential moguls who employed them; the often deeply indebted businesses struggling to cope with runaway technological change; or, indeed, the always-new always-on technology itself, whose operational capability increasingly shaped the final media product and dictated the decisions of those apparently at the helm? In fact, all of these descriptions were legitimate at once. In that sense, the term ‘media’ rather than ‘the media’ would have been a more all-embracing and potentially productive term. This lack of clarity meant that much of the debate fell back on the easy option: accusations that the media were adopting what amounted to a cynical, almost terrorist-friendly policy, originating predominantly with analysts whose greatest media expertise was as consumers. Paletz and Boiney (1992, p. 23) described the bulk of the literature on the relationship between media and terrorism as ‘dismaying’, full of ‘shrill jeremiads’ and unfounded assertions placing ‘overwhelming responsibility on the media’. Smelser (2007, p. 111) described it flatly as ‘the least satisfactory’ area of terrorism analysis. In fact, terrorists were simply learning to use available technology to do what governments had done for centuries: ‘spin’ their narratives

to the public, knowing that ‘propaganda grants authority to its makers’ (Meyer 1991, p. 2). In recent years, the tone has generally been more nuanced, with a belated recognition that ‘a free and critically engaged media ... is best positioned to undermine violent extremist propaganda’ (Ingram 2017, p. 2). This change in tone is not unrelated to the fact that new technology has ‘effectively shattered the monopoly’ (Hoffman 2006, p. 226) of ‘one-to-many’ traditional media and enabled the rise of ‘many to many’ new media, where every user is potentially a publisher (Weimann 2014, p. 2) and where ‘the medium’, as contended by McLuhan (1967, p. 15) fully 50 years ago, is more compellingly than ever ‘the message’.

Terrorism and media: the complexity perspective

Despite the extraordinary manner in which technology has been transforming civilisation, there has to date been no thorough updating of the main propositions of terrorism studies from the twenty-first century perspective of complexity theory. Its application has been at best fragmentary. Mesjasz (2015) surveyed the possible application to terrorism of a wide range of ideas drawn from complex adaptive systems research only to conclude that, in substantive terms, ‘nothing has yet really come out of this effort’ (Mesjasz 2015, p. 53). Yet change was in fact afoot. The distinction between cyberspace and ‘real’ life was becoming increasingly ‘obsolete’ (Fussey and Roth 2020, p. 660) and this new reality was in the process of transforming both terrorism and counterterrorism. In terms of the relationship between terrorism and media, Al-Qaeda was at the forefront of early efforts to spread the jihadist message via the internet using its first website, alneda.com¹⁶ (Kimmage 2010, p. 7; Hoffman 2006, p. 226). By the start of the new millennium, Al-Qaeda’s rapid, focused, and flexible adoption of cyber-tools amounted to its own ‘stealth “revolution in military affairs”’ (Ranstorp 2004, pp. 83-96). From the point of view of messaging, here were terrorists who no longer needed the media. The evidence was clear. When it came to communication with sympathisers, followers or operatives, whether to proselytize, to raise funds, or to plan attacks, it now had a direct route to market: the worldwide web. ‘They don’t need us to get their message out’, noted Paul Hamilos (2015), international editor with new media outlet BuzzFeed. ‘Those stories of people trekking out to get a sit-down with Bin Laden, that’s just

¹⁶ Alneda translates as ‘the call’ (Jacinto 2004).

no longer the case'. This, said Weimann (2014, p.4) marked 'a new waypoint in jihadists' professional use of the new media'. That waypoint allowed Al-Qaeda and other jihadists to extend their reach far beyond 'their core support base in the MENA region to diaspora populations, converts, and political sympathizers' (Conway and McInerney 2008, p. 10). It was a striking example of the co-evolution of technology and organizational design. It demonstrated two things: firstly, Al-Qaeda's instinctive ability to spot a critical juncture in the evolution of information technology, combining it innovatively with one of its natural strengths, the networked spread of its affiliates and its community of supporters; and secondly, the capacity of information technology to evolve constantly using the opportunities presented by its environment, whether that meant transforming an economy through a new invention,¹⁷ or empowering a terrorist network by increasing its operational effectiveness virtually overnight. Here were the first indications of a more complex terrorism and a rampant information technology reaching out to test the benefits of co-evolution in pursuit of mutual empowerment.

Al-Qaeda was not, however, the first terrorist group to use the internet in this way to achieve 'autonomous communication' (Conway 2005, p. 9). The first had been the now largely forgotten Marxist guerrilla group, *Movimiento Revolucionario Túpac Amaru* (MRTA), whose aim was the establishment of a socialist state in Peru. On December 17, 1996, it took 72 hostages at the Japanese embassy in Lima,¹⁸ and within hours had a website up and running from a server in Germany. In the absence of other information, mainstream media, including highly resourced and authoritative outlets such as *The New York Times*, sourced their updates there. 'During the initial hours of the conflict, the terrorists effectively owned the information environment', wrote Denning (2010, p. 2). MRTA's use of the internet, she said, represented 'a strategic innovation in terrorism'. In a textbook example of 'cascading terrorism' (Watts 2016, 00.13-00.30), its impact was immediately 'recognised by terrorist groups worldwide' (Denning 2010, p. 2). McLuhan's issue of 'scale' was finally making itself felt through the interaction of terrorism and this powerful new information technology, though how or why remained unclear. To regard this relationship otherwise was to fall into the elephant trap of

¹⁷ For example, the iPhone. See Mazzucato 2015, pp. 93-116.

¹⁸ This attack gave its name to 'Lima Syndrome', a psychological condition where kidnappers begin to identify with their captives (Lama 1996; Correll et al. 2018).

seeing agency only in human hands, thereby excluding the transformative power of emergence in the evolution of information technology, so that technology advances ‘by capturing phenomena and putting them to use’ (Arthur 2009, p. 3), a description tantamount to one of co-evolution. Coevolution, however, could only be the logical explanation if both terrorism and information technology could reasonably be described as complex adaptive systems.¹⁹ On the face of it, it seemed that information technology could reasonably be described as such, subject to theoretical underpinning. In the case of terrorism as a phenomenon, the question clearly had to be applied to terrorist groups in general or to specific terrorist groups or networks. Anything else would be essentially meaningless. Hayden (2013, pp. 19-20; 2006) provided a clear route to the answer: that certain terrorist networks at certain specific stages of organisational development can, sometimes more fully than others, be described as complex adoptive systems. This meant that co-evolution was logically supportable as an explanation for the mutually beneficial interaction of terrorism and information technology and for the force multiplier effect that ensued.

The evolutionary trajectory of information technology

Interesting though the case of Al-Qaeda may have been, one case study purporting to show a complex mechanism at work was wholly inadequate. In addition, although Al-Qaeda’s rapid adoption of the internet was undoubtedly dramatic, its fundamental importance as a weapon was not fully understood for some years, even by the pioneers of modern terrorism analysis. ‘We missed it’, recalled Jenkins (2015), one of the original RAND research team. ‘I should have known better because my own dictum is that terrorism is about communication, primarily’. However, as new iterations of internet-based technology spun off in the form of social media, allowing users to network and to create and share content (Boyd and Ellison 2007), these iterations were adopted and exploited with equal rapidity (Weimann 2014, 2010) by other jihadist organisations,²⁰ particularly Islamic State. All the main social media platforms and messaging apps were embraced, including Facebook, Twitter, YouTube, Instagram, Flickr, Pinterest, and MySpace (Weimann 2014, pp. 1-2). This raised the question of whether the

¹⁹ A theoretical proposition that is examined in detail in Chapter Two.

²⁰ Even the Taliban started its own Telegram channel, Al-Emarah, in a number of languages, including Pashto, Persian and Turkish (Ward 2018; Bodetti 2016).

same mechanism or process was at work in the case of Islamic State and social media as had perhaps been at work with Al-Qaeda and the internet. This, in turn, begged the question of whether or not there were other possible examples of the same phenomenon. That search led to Hezbollah and its adoption of satellite television as a propaganda tool in response to Israel's invasion of south Lebanon in 1982 (Conway 2008b, 2007) but particularly in its 2006 war with Israel, often dubbed 'the First Israel-Iran War'. It was Hezbollah of whom Conway (2005, p. 9) had observed that 'autonomous communication' had long been 'a paramount objective', its aim being – in line with its socio-political strategies of 'walking on the edge' (Azani 2011) and 'social jihad' (Flanigan and Abdel-Samad 2009) – to cast its members as resistance fighters and politicians rather than as international terrorists. What made Hezbollah additionally interesting was that satellite television was pre-internet information technology, although its exploitation bore many of the same hallmarks. This suggested that any mechanism common to the three case studies was not just internet-related, it was related to something more fundamental: information itself. As Deuchars (2010, p. 166) says about the concept of an emergent 'information society': 'Information is not a value-neutral aspect of exchange. It is always enmeshed in a configuration of power ...'

What became clear across the three case studies was that – quite distinct from their terrorist adopters – there was a clear evolutionary trajectory from satellite technology onwards to the internet and beyond to internet-based social media. This progression will be examined in each case later. The breaking down of internal technological barriers between terrestrial and satellite technology increased interoperability and scale with the result that data was now 'transferred in gigabytes per second rather than megabits per second' (Orbital Today 2020), injecting a force multiplier effect that turned Hezbollah's regional threat global. In the case of Al-Qaeda and the internet the process was similar. The internet was originally developed as a system that would allow the US military to link satellite systems and to transmit information to and from the front lines of conflict. Again, enabling satellite systems to work together by creating the internet increased interoperability, scale and force multiplier effect, giving Al-Qaeda unprecedented global reach and a new weapon whose impact would be felt on 9/11: 'cyberplanning' (Thomas 2003). So too with Islamic State and social media, which allowed jihadist groups to network, to fragment into ever-smaller special interest microstructures (Knorr Cetina 2005, p. 216), and to exchange their own content, again vastly increasing their

reach in line with increasing interoperability. Where the internet had been ‘a facilitative tool’ increasing the opportunities for liaison, radicalisation, and attack planning (Conway 2017; Thomas 2003), social media platforms went much further, acting as ‘digital replicators’ (Gillings et al. 2016, p. 7; LaBar et al. 2016) capable of propagating rather than simply amplifying the messages they carried, and empowering even arms-length followers to decide which tactics would constitute their next ‘strategy of surprise’ (Crenshaw 1988). Fundamentally, however, co-evolution remained the ‘recurrent causal architecture’ in each case (Downing 2015, p.7).

The contribution of this thesis

Against that multi-tiered backdrop, the contribution of this thesis to the sub-discipline of terrorism studies is that it looks for the first time from the perspective of complexity theory at the interaction of networked terrorism and information technology and the manner in which the two can be shown to empower one another. It identifies both as complex adaptive systems, systems whose evolutionary imperative is that they co-evolve with partners that prove mutually beneficial. It then goes a step further and identifies a putative co-evolutionary mechanism which demonstrates how the interaction of the two leads to augmented performance for both, known in conflict terms as a force multiplier effect. It illustrates how that mechanism can be seen to have applied consistently in three case studies spanning a period of some 20 years, arguing that this makes a compelling case for the modernisation of key tenets of the discipline in line with complexity theory. Given the naturally interdisciplinary nature of complexity theory, this might lead to productive debate between those who see terrorism studies as very much a social science sub-discipline and those who believe it is fundamentally an inter-disciplinary field where multiple disciplines ‘coalesce in a mutually enriching exchange on problems concerning terrorism and counterterrorism’ (Reinares 2012).

The structure of the thesis

Having sketched the backdrop, and not wishing to rehearse unduly what went before, Chapter One reviews the literature on the relationship between terrorism and information technology, placing developments in their historical context while also identifying the critical junctures which reveal both as complex adaptive systems locked in a mutually beneficial

process of co-evolution. This leads to the conclusion that a twenty-first century reinterpretation of the RAND analysis of 1973 would be not that ‘terrorism evolves’ (Jenkins 1999, p. iv), but that it co-evolves, with information technology among other beneficial partners.

Chapter Two lays out the theoretical underpinning of the thesis. It deals in detail with complexity science, the theory behind it and the world view it supports (Downing 2015; Mesjasz 2015; Holland 2014, 1995, 1994, 1992b, 1992a; Rupert et al. 2008; Mitchell 2006; Bar-Yam 2004, 1997; Axelrod and Cohen 1999; Gell-Mann 1994; Kauffman 1993, 1992, 1991a; Langton 1992; Gleick 1987; Prigogine and Stengers 1984). It examines complex adaptive systems, the genetic algorithms (Holland 2014, pp. 217-218; 1992, p. 24; 1975, pp. 89-140) that allow them to evolve and adapt, and how that process leads to co-evolution, where two systems exert mutual influence over one another, affecting the evolutionary trajectories of both, with the result that together they experience ‘significantly augmented performance’ (Holland 1992b, p. 11). It demonstrates that both terrorism and information technology may reasonably be described as complex adaptive systems. That being so, it shows that the co-evolution of the two provides a logical new way of looking at their interaction (Kauffman 1993, 1992, 1991a). This new perspective allows the identification of the key elements of the co-evolutionary mechanism involved, opening the way to a much more comprehensive challenge to pre-complexity views in terrorism studies.

Chapter Three sets out why, in pursuit of a methodology that can be aligned with complex ontology, process tracing – and specifically causal process tracing (Blatter and Haverland 2014) – has been chosen as the most appropriate research methodology to test the legitimacy of the propositions at the centre of this thesis. Primarily, it was chosen because it is acknowledged as the most suitable approach for ‘unpacking’ causal mechanisms such as, in the case of this thesis, the process that leads terrorists to adopt and exploit structural change in information technology. In political terms, it has been particularly effective in uncovering the causal mechanisms behind specific policy decisions or historical events (Tannenwald 2015, p. 220) by ‘working backward from the known outcome to uncover the causal mechanism that can *sufficiently* explain the outcome’ (Beach and Pedersen 2012, p. 8, author’s italics). In that context, the aim here is to show that while the adoption of new technology by Hezbollah, Al-Qaeda and Islamic State was regarded at the time simply as part

of the terrorists' natural evolution, what in fact better explained it, then and now, is that it was the result of co-evolution, driven by the imperative to compete and exert reciprocal influence which is part and parcel of what it means for complex adaptive systems to interact. The chapter ends with the development of six tests aimed at determining whether the same causal mechanism can reasonably be said to apply in each of the three case studies. Those tests are operationalised using NATO's yardstick for gauging probability which links directly to the data (Irwin and Mandel 2020).

Chapters Four, Five and Six are the three case studies: Hezbollah and satellite television; Al-Qaeda and the internet; Islamic State and social media. Chapter Four shows the beginning of an evolutionary trajectory whereby the transition from terrestrial to satellite broadcasting transformed Hezbollah from a regional threat to a global player, and the increase in interoperability and force multiplier effect it entailed prepared it to challenge Israel more asymmetrically than expected during the 2006 war (Jorisch 2004c, 2004b, 2004a). Chapter Five and Al-Qaeda's leveraging of the internet shows how digital satellite broadcasting evolved into the ARPANET and then the internet, and the free availability of this revolutionary new communications technology without borders played to the terrorists' naturally diffuse and networked organisational structure. 'The web's shapeless disregard for national boundaries', wrote Coll and Glasser (2005), 'fits exactly with Bin Laden's original vision for Al-Qaeda', which he founded 'to stimulate revolt among the worldwide Muslim *ummah*'. The effect was leaderless jihad with 'no structure, hierarchy or centre of gravity' (Weimann 2008), 'the total deterritorialization of jihadist warfare' and 'the entire globe as the theatre of war' (Lia 2006, p. 16). Chapter Six shows how social media continue the same evolutionary trajectory towards greater interoperability (and ideally onwards towards autonomy) by disaggregating into ever-smaller microstructures which allow content generation and exchange of data so that they are acting, in effect, as 'digital replicators' (Gillings et al. 2016, p. 7). It shows how that same organisational architecture allowed individuals or small cells of Islamic State followers, with little or no structured connection to the core network, to attack unilaterally, determining not just tactics but strategy. As McShea (1996, p. 479) noted about the 'pervasive evolutionary trend' in metazoan complexity: 'The more differentiated a system is, the more complex it is'.

The concluding section brings together the findings from each of the case studies and addresses the lessons to be drawn in terms of the implications for terrorism and counter-terrorism. It emphasizes that despite the case studies examined here, co-evolution between terrorism and information technology is by no means an exclusively Islamist terrorist phenomenon. It examines the likelihood that as other terrorist groups become as networked as Islamist terrorists have become since the end of the Cold War, the same co-evolutionary mechanism will apply, and asks whether movements such as militant accelerationism (Kriner 2022), responsible for dozens of terrorist attacks worldwide over the past 20 years, may be among the next in line. It also contemplates the future of what may reasonably be called 'information terrorism' in areas such as biotechnology, described by Nobel laureate David Baltimore as on 'the cusp of a new era in human history' (Isaacson 2021, p. 292).

CHAPTER ONE

The 'symbiotic' relationship between networked terrorism and information technology: A review of the literature, re-interpreted in light of complexity theory

Introduction

Terrorism 'from below' (Laqueur 2006, p. 7) has had many faces. Its earliest manifestation dates to first-century Judea, where the Zealots²¹ – a Jewish sect known to the Romans as the *sicarii* or 'dagger men' after their weapon of choice, a short sword or *sica* – waged a campaign of assassination against their occupiers between 66 and 73 CE. They were 'a highly organized religious sect consisting of men of lower orders'. The Romano-Jewish historian Josephus²² described them as combining 'messianic hope and political terrorism' (Laqueur 2006, p. 7), an eschatology as familiar from Christianity and Judaism as from Islam (Cohn 2004), that continues among extremists to this day, and that applies to a greater or lesser extent in all three of the case studies in this thesis, Hezbollah, Al-Qaeda, and Islamic State. That mixture was characteristic too of another early sect, the Nizari Ismailis, a breakaway branch of Shia Islam found in northern Iran in the eleventh century and finally stamped out by the Mongols in the thirteenth. Known as 'the Assassins', they were infamous for sending lone attackers to kill well-guarded enemy leaders (Chaliand and Blin 2007a, pp. 55-78; Lewis 2003, pp. 1-19). As such, they were 'a profound threat to the existing order, political, social and religious' (Lewis 2003, p. 139). 'They sell themselves, are thirsty for human blood, kill the innocent for a price, and care nothing for either life or salvation', wrote Brocardus (1906), a German priest, in a dramatic note offering guidance on a new crusade to King Philip VI of France in 1332. These – the Zealots and the Assassins – are the two earliest known terrorist movements (Laqueur 2006, p. 7; Hoffman 2006, p. 83). Survival dictated that they were secretive, tightly organised, and capable of regrouping quickly. As a result, their networks were constantly changing and their tactics unpredictable. In the absence of media, notoriety spread by word of mouth. Even then, the aim of terrorism was, as it remains in the twenty-first century, not

²¹ The term 'zealot' is the common translation of the Hebrew 'kanai' (plural, kana'im), meaning one who is zealous on behalf of God (Online Etymology Dictionary at <https://www.etymonline.com/word/zealot>).

²² Titus Flavius Josephus, born Yosef ben Matityahu, best known for *The Jewish War* (c. 75) and *Antiquities of the Jews* (c. 94).

just to eliminate the enemy but 'to frighten, and, by frightening, to dominate and control' (Hacker 1976, p. xi). The medium – the *sica* – was the message.

It is clear then that there were threads running through early terrorism which can still be identified today. Given that the focus of this thesis is on the interaction of networked terrorism and information technology, the starting point of this literature review might well have been the beginning of modern terrorism research at the RAND Corporation in 1972 (Jenkins 1999, p. iii-iv) which underlined the operational importance of that terrorism-technology nexus for the first time. The RAND research began in response to two incidents that year: the Japanese Red Army/PFLP attack on passengers at Lod (now Ben Gurion) airport in Israel in May, and the seizure of 11 members of the Israeli contingent at the Munich Olympics in September. Those and subsequent incidents, including a spate of passenger jet hijackings through the 1970s, 1980s and 1990s (BBC News 2001), convinced the RAND researchers they were watching 'a new mode of warfare' reflecting 'a unique confluence of political events and technological developments that made it likely to increase and become increasingly international' (Jenkins 1999, pp. iii-iv). While they were undoubtedly correct and even prescient, it was also true that by then this mode of terrorism was already well established and a magnet for global media attention. But where had it come from? What had prompted it? What was powering it? What was the nature of the interaction between political events and technological developments? And why might this lead to terrorism becoming more international? It is to seek answers to those questions that this review begins instead by exploring the first decades of the twentieth century, the birth of quantum mechanics, and how that played into the increasingly rapid revolution in information technology that was shaping, and continues to shape, the future of humankind and the future of terrorism.

The aim of this literature review then is not alone to trace the interaction of terrorism and information technology as it is portrayed in the narrative of terrorism studies, but also to identify the waypoints in the literature which – given advances in understanding due to the development of complexity theory – retrospectively reveal both terrorism and information technology as complex adaptive systems locked, as they invariably are by their nature, in a mutually beneficial process of co-evolution. It will show (i) how the parallel development of quantum physics and information technology created an environment in which networks, for the first time, became dominant over hierarchies (Castells 2004); (ii) how, consequently, the

networked terrorist groups that emerged in the aftermath of the Cold War became early adopters of information technology in a world already in the early stages of transformation, first leveraging satellite technology, then the internet, followed by social media; (iii) how that interaction acted as a force multiplier for the terrorists' capacity to strategize and attack, as exemplified by 9/11 (Dillon 2002, p. 1); (iv) how the increasing disaggregation of the technology and the increasing power of mathematical modelling led to a new way of looking at terrorist networks as complex adaptive systems, powered by information, the new global currency (Hayden 2013, 2006; Fellman 2010, 2009; Conway 2003, p. 1; Carley 2002), and (v) how that evolutionary route map led to the central proposition of this thesis that, as complex adaptive systems, terrorism and information technology co-evolve, with terrorism using each new iteration of the information technology to drive its messaging towards ever-more-effective 'autonomous communication' (Conway 2005, p. 9) and its operational capacity towards greater and more lethal scale and reach (Elkhodr et al. 2016; Heubusch 2006).

The road to 'informationalism'

The momentous scientific change that was underway during the first half of the twentieth century was largely hidden from view by the existential horrors of the two world wars. A key date was November 25, 1915, when Albert Einstein delivered the last of four lectures setting out his general theory of relativity to the Prussian Academy of Sciences in Berlin (Einstein 1920; Isaacson 2007, p. 219). His thinking, driven largely by philosophical questioning rather than scientific experimentation (Wudka 2006, p. 151), revolutionised classical physics by showing that its world view was 'no longer tenable' (Cresser 2011, p. i), and gave birth to the new field of quantum mechanics.²³ Quantum mechanics is often thought of as 'the physics of the very small', describing the structure and properties of atoms and molecules, the make-up of atomic nuclei, and the properties of elemental particles (Cresser 2011, p. i). More than that, it shows that 'irreducible randomness' is built into the laws of nature; that the world is 'inherently probabilistic' in that things may vary by chance, without a cause; and that interconnectedness or 'entanglement' is possible between physical systems, even those separated by vast distances, an idea with no parallel in classical physics (Cresser 2011, p. i).

²³ Also known as quantum physics.

The world described by quantum mechanics was, arguably, an early blueprint of the non-linear world now so comprehensively explained by complexity theory: interactive, emergent and unpredictable (De Landa 2014, pp. 25-26; Holland 2014, 1995, 1992, 1975; Mitchell 2009, 2006, 1995; Kauffman 1993, 1992, 1991a). There were two broad offshoots of this new 'Quantum Age': first, the development of nuclear weapons a few decades later, with the doctrines of containment, deterrence and mutually assured destruction that characterised the Cold War (Gaddis 2005); and, second, information technology – which had already led to the creation of television, arguably the most underestimated societal command-and-control system in the history of technology (Chomsky 2002, pp. 20-21)²⁴ – which would later spawn the internet, a remarkable new engine of many-to-many digital communication (Pfister 2011, p. 217), bringing with it, on the one hand, unprecedented scale, and, on the other, countless cyber vulnerabilities. Each of these offshoots would reshape the world. It was the start of a complex pattern of 'promise and peril' (Mank 2017, p. 1) – scientific discovery leading to technological advancement leading to new reflexive dangers²⁵ – that would come to characterise the landscape of international security and repeatedly elevate modern terrorism to new levels of threat.

The post-WWII economic boom made the US the world's richest country, fuelling an intensification of that information revolution which had begun gathering momentum with microelectronics in the 1940s (Castells 2004, p. 5) which brought, in effect, the demise of the moving part. Instead, electronics was now powered by new 'solid state' integrated circuits so tiny they could be incorporated into a 'chip' of semi-conductor material, usually silicon (Lécuyer and Brock 2006). So sensitive was this new equipment in national security terms that a primary purpose of America's 1979 Export Administration Act was to prevent dual-use technologies such as the 32-bit architecture of the Intel 80486 microprocessor – which could also be used as a targeting system for intercontinental ballistic missiles (ICBMs)²⁶ – from falling into enemy hands (Fellman 2009, p. 1). Then came the development of the world's first general-purpose digital computer, ENIAC (Electronic Numerical Integrator and Computer),

²⁴ Chomsky (2002, pp. 20-21), 'Propaganda is to democracy what the bludgeon is to a totalitarian state.'

²⁵ In relation to complexity theory, see: Lash, S., 2003. 'Reflexivity as Non-Linearity', *Theory, Culture and Society*, 20 (2), pp. 49-57.

²⁶ Inter-continental ballistic missiles (Caston et al., 2014).

built between 1943 and 1946 to enable the US Army to calculate ballistic tables for a new generation of heavy guns in the closing stages of WWII (Mobley 2001).²⁷ Weighing 30 tons and roughly one thousand times faster than its electro-mechanical predecessors (Weik 1961), it was clear that such unprecedented computing power had huge potential to transform the economic landscape as well. This was the start of the transition from defence technology to consumer electronics (Mazzucato 2015, pp. 93-119) as the propulsive force behind key modern innovations.

The information revolution was also driven relentlessly by the space race between the US and the USSR, and particularly by the Soviets' launch of the R7, the world's first ICBM in August 1957, which, in turn, was used to launch Sputnik, the world's first artificial satellite the following October (Howell 2015; Markovich 2014; Boyle 2013). The push by the Americans to match this double international embarrassment led to the development and commercialization of television, and, subsequently, of satellite technology. This was a technological revolution 'shaped by the logic and interests of advanced capitalism, without being reducible to the expression of such interests' (Castells 2010, p. 13). It also sparked 'the democratization of technology' (Friedman 1999, pp. 41-47), with potentially universal access to the fruits of technological innovation. Not only did this democratisation have an equalising effect, but it showed that, in such a non-linear environment, 'hierarchy' could be 'the enemy of progress' (Shukla 2019) and lead to 'passive behaviour' (McKelvey n/d) where control and innovation were driven from the top down, a critical lesson for the military as well as in the asymmetric theatre of terrorism and counterterrorism.²⁸ The changes wrought by the information age would be 'as dramatic as those in the Middle Ages in Europe' and would be 'dominated by unintended consequences' (Dewar 1998). Among those unintended consequences was that terrorists were becoming 'more lethal and more agile' (Nye 2003).

In terms of the theory underpinning this new digital technology, the single most important development of the 1940s was Claude Shannon's paper, *A Mathematical Theory of*

²⁷ During WWII, a 'computer' was a person who calculated artillery firing tables using a specially designed desktop calculator (Moye 1996).

²⁸ Moghadam (2013, p. 38) observes: 'While Al Qaeda's organizational principle was erected from the "top down", its successful implementation was dependent on innovation from the bottom up.'

Communication (1948)²⁹, which set out the workings of modern digital computing (Marinescu and Marinescu 2012, p. 339). Information, it said, measured ‘surprise’³⁰ or the amount of ‘uncertainty’ it overcame (Goodman 2017). It explained how all systems that send or receive information had the same basic structure, arguably including human beings and the information technology they created. This has led inexorably in recent years to the dramatic proposition that ‘the carbon-based biosphere has generated a cognitive system (humans) capable of creating technology that will result in a comparable evolutionary transition’ (Gillings et al., 2016). Shannon’s paper also introduced the ‘bit’, allowing objective measurement of the quantity of information contained in a message. Shannon’s ‘breathtaking conceptual leap’ was that ‘once information became digital,³¹ it could be transmitted without error’ (Waldrop 2001), a point critical to the leveraging of information technology by the three case studies here, Hezbollah, Al-Qaeda and Islamic State, because it leads to more successful amplification. He took the radical step of ‘defining “information” in a new way that completely disregarded whatever meaning a signal might contain’ (Santa Fe Institute 2018). For him, ‘the statistical properties of signals sent from sender to receiver were the information’. As a result, the legacy of Shannon’s work has been a ‘70-year divide’ between what have become known in information theory as ‘Shannon information’ and ‘semantic information’, the former being information as the statistical properties of the signals and the latter being information as what is usually regarded as ‘meaning’. Those insights would become the intellectual architecture of the internet and of the digital age (Soni and Goodman 2018; MIT News 2001). Despite such remarkable progress in individual disciplines, these were but the foothills of what Castells (2004) called ‘informationalism’, a new paradigm to replace ‘industrialism’, in which (with more than a nod to McLuhan):

... what is specific to our world is the extension and augmentation of the body and mind of human subjects in networks of interaction powered by microelectronics-based, software-operated, communication technologies. These technologies are increasingly diffused throughout the entire realm of human activity by growing miniaturisation. They are converging with new genetic engineering

²⁹ In the same year, Alan Turing (1948) published ‘Intelligent Machinery’. See references.

³⁰ ‘Terrorism’, wrote Martha Crenshaw (1988), ‘is par excellence a strategy of surprise’.

³¹ In other words, once information was encoded in bits, it could be transmitted with perfect accuracy.

technologies, able to reprogram the communication networks of living matter. (Castells 2004, p. 9; Doudna 2020)³²

Terrorism in the new digital landscape

‘Revolutionary ideologies have always crossed borders with ease’, wrote Crenshaw (1981, p. 382). In the nineteenth and early twentieth centuries those ideologies were to be found primarily in Europe: the fallout from the French and Bolshevik revolutions. After World War 2, they spread. Third World revolutions in China, Cuba, and Algeria, among others – along with the work of revolutionary intellectuals such as Frantz Fanon on the psychopathology of colonization (Hook 2004, pp. 85-88; Fanon 2001) and Carlos Marighela (2002), author of *Minimanual of the Urban Guerrilla* – significantly influenced terrorist movements in the West by promoting the acceptance of terrorism as ‘routine behaviour’ (Crenshaw 1981, p. 382). Maintaining the balance of power during the Cold War resulted in a proliferation of proxy organisations carrying out campaigns of violence underwritten by Communist or Western states (Kurth Cronin 2009, p. 3-6). The Soviet Union, China, East Germany and Cuba all supported terrorism. The West, particularly the US, also supported groups who used terrorist tactics, including the mujahideen in Afghanistan, the Contras in Nicaragua, and UNITA in Angola. The plight of Palestinian refugees left homeless at the end of the first Arab-Israeli war in 1949 played into a new anti-militarism in the more affluent countries of western Europe and in North America, especially after the end of the Vietnam War in April 1975. Palestinian militants – in particular the PLO and PFLP – became mentors to Europe’s left-wing terrorist groups (Hoffman 2006, pp. 74-80). Terrorism had become ‘internationalised’ and ‘networking’ was the key.

If this was a period of considerable political upheaval, it was a period of considerable technological change as well. Television was experiencing its first ‘golden age’, from the late 1940s to the 1970s, and the ability of the new medium to bring acts of violence to a mass ‘living room’ audience (Arlen 1997) immediately drew the terrorists’ attention (Jenkins 1974, p. 4). They capitalised on it, rapidly realizing (i) the importance of the image, in the sense that ‘television pictures mattered far more than what correspondents said’ (Kurtz 1998, p. 105);

³² The 2016 *Worldwide Threat Assessment of the US Intelligence Community* described the potential misuse of genome editing as having ‘far-reaching economic and national security implications’ (Clapper 2016, p. 9).

(ii) their capacity not alone to shock but to hijack and dictate the international news agenda (Beckett 2016), and (iii) the power of media exposure to prompt equally damaging copycat attacks (Jetter 2017). A spate of airliner hijackings began with El Al Flight 426 from London to Rome on July 23, 1968. 'The element of violence in terrorism often seemed secondary to that of dominating newspaper headlines and television coverage', observed Shpiro (2002, p. 80), quoting former Sinn Féin leader Gerry Adams' definition of what he called 'terrorism at its best' as 'armed propaganda' (Sharrock 2001). 'Today's lurid speculations turn into tomorrow's headlines, making it hard to dismiss even the most far-fetched scenarios', wrote Jenkins (1999, p. iii-iv). Made-for-TV attacks were designed to 'play well' at prime time (Bell 1978, p. 47). The media responded 'with almost unbridled eagerness' (Hoffman 2007, p. 10), to the extent that in Beirut the main American networks became known as the 'Amal Broadcasting Company' (ABC) and the 'Nabih Berri Company (NBC) (Hoffman 2006, pp. 176-177). So important did 'spin' become that some fighters even began to display 'a TV-orientated dress sense' to appeal more to the cameras (Segaller 1987, p. 179). Here was what Denning (1999, pp. 9-10, pp. 101-129) first termed 'perception management', evolving as terrorists seized the new opportunities of scale offered by the emerging information technology. Two things became clear. First: access to the infrastructure of communication was intimately related to power (Crelinsten 1987, p. 443). Second: information technology, of its nature, never stands still. This meant that terrorists who could seize the apparatus of communication and achieve 'autonomous communication' (Conway 2005, p. 9) had an unprecedented technological and propagandistic edge. It also meant that as technology continued to evolve, first-user advantage was invaluable, particularly when the new iteration was disruptive (Burkhardt and Brass 1990, p. 107), packed with transformative impact. It had, in fact, always been thus, but what had changed with the world of information technology was first, electrification, then digitisation, and, as a result of both, scale:

Before technology made possible the amplification and multiplication of speech, the maximum number of people who could be reached simultaneously was determined by the range of the human voice and was around 20,000. In the nineteenth century, within one lifetime, the size of an audience was expanded twenty-five to fifty times. In 1938, the *New York Sun* published a record 39,000 copies. In 1869, on the occasion of President McKinley's election, two US papers, belonging to Pulitzer and Hearst, for the first time printed a million copies. (Schmid and De Graaf 1982, p. 10)

As the Lod Airport attack left 26 people dead in May 1972, and just three months later the assault by Palestinian Black September guerrillas on Israeli athletes at the Munich Olympics killed 12 more (Reeve 2000), researchers at RAND began to examine this new phenomenon. By now television, a powerful new amplification system for international terrorism, had earned the gory epithet, “terrorvision” (Segaller 1987, p. 197).

The terrorism-technology nexus and the internet

The RAND team began by constructing a chronology of terrorist incidents to place an empirical foundation beneath their research. They were faced with the perennial analytical problem: ‘how do we assess the threat of terrorist events that have not occurred?’ (Jenkins 1999, p. ix). The danger was that, in attempting retrospectively to draw coherence out of chaos, they might attribute to the terrorists a level of strategic thinking they had not possessed. They had two key insights (Jenkins 1999, pp. iii-xiv). The first was that terrorism, in this new form, reflected ‘a unique confluence of political events and technological developments that made it likely to ... become increasingly international’. The second was that ‘terrorism evolves’ (Jenkins 1999, p. iv). Both were valuable in that they underlined the interaction of terrorism and technology and introduced the concept of evolution into the terrorism debate, begging the question of what type of evolution and how it worked. In that context, a crucial miss was that they did not, apparently, delve into the distinction between ‘technology’ and ‘information technology’, content to see it as a continuum. However, ‘disaggregation is necessary for precision in interpreting technology research’ (Rousseau 1979, p. 537). Interrogating this disaggregation might have provided valuable perspectives into the evolution they had identified, specifically the ‘new scale’ (McLuhan 1967, p. 15) introduced by each successive iteration, and the contention that disaggregation reveals the patterns inherent in evolution (McShea 1996). However, they could not have anticipated (i) the exponential speed with which information technology would continue to evolve (Gillings et al. 2016, p. 1) or (ii) that it was being powered not just by innovation at industry level but by the relationship with its users (Arthur 2009), identified here as co-evolution.

The internet, however, would change everything. Its impact brought a gradual realisation that there was more to terrorist use of technology than weapons technology, which – not surprisingly given that terrorists’ greatest threat is violence and the fear of it (Hoffman 2002,

p. 313), and that bargaining power ultimately represents ‘the power to hurt’ (Schelling 1966, p. 2) – had been the main focus on technology in the literature of terrorism studies (Bale and Ackerman 2009; Ball et al. 2009; Maurer 2009; Oppenheimer 2009). In a videotaped interview in 2015, reflecting on his 40 years in counterterrorism, Jenkins (2015), a former Special Forces officer, recalled the priorities of the 1970s and 1980s and the degree to which the RAND researchers had been blindsided, first by their own preconception that the only technology relevant to the study of terrorism was weapons technology; then by the emergence of the internet, and, beyond that, by the capacity of terrorists to exploit it in ways that added a whole range of interrelated dimensions to the threat they posed:

We spent a lot of time looking at weapons: what weapons would terrorists use in the future? The weapons developments at the time were precision-guided munitions, heat-seeking surface-to-air missiles. We were attempting to ask: what is going to replace AK47s? And we missed it. I should have known better because my own dictum is, ‘terrorism is about communication, primarily’. Terrorism is about manipulation of an audience. Terrorism is violence that is choreographed to achieve psychological effects. Terrorism is aimed at the people watching. It’s not about battles or winning battles. So what was the single technology that completely went past us? The internet. The internet has allowed terrorists to reach audiences of global proportions, to spread their propaganda, to recruit followers worldwide, indeed to create online communities of supporters, and even to create new kinds of virtual organizations, networks instead of military formations. That was the most profound development in the terrorist arsenal, I think. Insofar as actual weapons are concerned ... terrorists are still armed with AK47s. (Jenkins 2015)

Jenkins (2006, p. 125) led the way in underlining the distinction between information technology and weapons technology. Despite the premium they placed on communication, he pointed out, terrorists had not always communicated effectively. Their messages could be lost in the drama of an attack. They had no control over how editors at old media outlets presented a story.³³ The benefit of the internet was that it was unmediated. In the virtual Wild West (Bryden 2019), what terrorists posted online in domains they controlled was predominately what their audiences saw. As a result, the much-vaunted ‘symbiotic relationship’ (Wilkinson 2006, p. 145) between terrorists and the media, where the media, in the sense of journalists at various levels, were apparently essential for delivering ‘the oxygen

³³ Hoffmann (2006, p. 198) observes: ‘The terrorist must parley this illumination (publicity) into a more effective vehicle of elucidation (propaganda).’

of publicity' (Thatcher 1985) to amplify terrorist atrocities, became a moot point. Save for the question of relative scale, the internet allowed the same type of 'autonomous communication' (Conway 2005, p. 9) achieved by Hezbollah in Lebanon, for example, through the use of its own satellite television station, Al-Manar, until it was banned by the US in 2004 and a number of European countries then followed. 'For terrorists', Jenkins decided, the internet rendered indisputable the fact that 'the most significant technology is not weapons but direct communication with their multiple audiences'. Indeed, as Hoffman (2006, p. 225) pointed out, the internet allowed terrorist groups to maintain multiple sites in different languages with different messages tailored to those multiple audiences. The truth itself was becoming disaggregated, and the internet and its offshoots were the doorway to that disaggregation. As Hoffman (2006, p. 225) observed, quoting US Senator Hiram Johnson: 'the first casualty when war comes is truth'.

The spread of networked terrorism

Just as WWII and its aftermath had supercharged the development of information technology, so the rapid, unforeseen and unexpectedly peaceful end of the Cold War transformed the geopolitical landscape in which terrorism was played out. Once America's 'unipolar moment' (Krauthammer 1990-1991) had passed, it led to a new multi-polar world of inter-state relations (Grant and Valasek 2007; Garton Ash 2006); a period of strategic withdrawal by European nations from colonies in the Far East, the Middle East, and Africa (Hoffman 2006, pp. 43-62); a new economic environment in which the 'imperialist expansion' of free-market capitalism, driven by the spread of Western liberalism, became the norm across much of the globe (Kukoč 2009; Doyle 1986, p. 1151); and a seismic shock to American hegemony, creating 'trauma in the foreign policy and national security community both in and out of government', generating new 'threats and challenges it was largely unprepared to meet' (The 9/11 Commission Report 2004, p. 143).

From the point of view of terrorism, the end the competing Cold War power blocs led to a decline in what would come to be seen as the 'traditional' terrorist groups of the 1960s and 1970s, such as the PLO, the Popular Front for the Liberation of Palestine-General Command, the Provisional IRA, the Red Brigades and the Red Army Faction. These were hierarchical groups who had been pyramidal in organisational design, centrally controlled, often state-

sponsored (mainly by the Soviet Union), with nationalist or Marxist agendas. In the absence of state backing, what emerged in their place were innovative so-called 'new-generation' groups, who were networked, non-hierarchical, flat or 'flatarchical'³⁴ (Morgan 2015) and therefore more versatile, efficient and effective (Don et al. 2007, p. xvi). Thrown back on their own resources, they became 'self-provisioning' (Duffield 2002, p. 157) and worked in teams with a high degree of autonomy. Their networked design gave them 'inherent flexibility, adaptiveness, and the ability to capitalize on the talents of all their members' (Zanini and Edwards 2001, pp. 31-32), as well as on the opportunities offered by the information revolution (Arquilla and Ronfeldt 2001, p. 1), particularly the internet, 'perhaps the most transformative invention since Gutenberg' (Healey 2014).

In the underworld of terrorism, Islamist networks were regarded as being at 'the cutting edge of organizational networking' (Zanini and Edwards 2001, p. 29). They were plugged into international networks of family and supporters, although, of course, as Schmid (2017, pp. 6-8) points out, 'the bandwidth of interpretations of Islam' within the Muslim community or *ummah* includes conservative and pluralist Muslims as well as Sunni Salafist jihadists and a larger circle of 'Islamist Muslims'. In addition to the benefits of such networking, the leadership of Al-Qaeda, in particular, seemed to have 'intuitively grasped' the communicative power of the internet from the start and to have set out to harness it strategically and tactically (Hoffman 2006b, p. 5), although it is worth noting here that from a complexity perspective this drive is now explained more logically by the competitive imperative of co-evolution. Of the four original al-Qaeda operational committees, one was specifically tasked with media and publicity.³⁵ Egyptian computer experts who had fought beside Bin Laden against the Soviets in Afghanistan during the 1980s were recruited to create the network of websites, bulletin boards and email servers that allowed it to function from its 'virtual sanctuary' after fleeing to the tribal areas of Pakistan in October 2001 (Hoffman 2006c, p. 6). Noted one unnamed US government expert in relation to radical Islamist websites at the time: 'Never in history has there been an opportunity where propaganda is so effective' (Hoffman

³⁴ A mixture of flat and hierarchical. 'Organisations with this type of structure are very dynamic in nature and can be thought of a bit more like an amoeba, without a constant structure' (Morgan 2015).

³⁵ The other three were: military operations, finance and business, and fatwa and Islamic study (Gunaratna 2002, p. 57).

2006c, p. 3).³⁶ Terms that had previously applied only to the technology now applied to these networks as well, as if through a new form of symbiosis. Unlike their command-and-control predecessors, they behaved, observed Zanini and Edwards (2001, p. 29), ‘in an internetted manner, without a precise central command’, exactly as the West was to experience with a vengeance on 9/11, ‘the deadliest attacks in the annals of terrorism and the cause of the greatest bloodshed on American soil since the Civil War’ (Jenkins and Godges 2011, p. 1).

Despite the fundamental changes the internet was sparking, it is important to remember that without the benefit of hindsight it was difficult to contextualise this rapid change in so many still apparently unrelated areas. For example, there was nothing inevitable about the evolutionary path of the internet. It was not a linear progression from one grand idea to the next. It was shaped ‘not just by critical technical decisions ... but by accident and by economic, social and cultural forces’ (Naughton 2016, p. 6). It was also the case that by the turn of the millennium internet technology was not as new as it seemed to many mainstream consumers. Design work had started in 1973. It became operational in January 1983. Even then it remained the preserve of a technological and research elite. From the early 1990s, it began to percolate into mainstream society, but gradually. Because of those rarefied beginnings, it took another decade or so before it was recognised as a ‘general purpose technology’ (Bresnahan 2010, p. 764), something without which – like mains electricity or water – society could not function. As Mark Weiser (1991), who coined the term ‘ubiquitous computing’, observed: ‘The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.’ So although the internet over that period from the 1970s on became a global engine of change ‘extensively integrated into the economy, the military and society as a whole’ (Conway 2003, p. 15) in ways the public often did not realise, there were few who fully understood its complex architecture or that it was not a unitary network but ‘a network of computer networks’. Industrial society, observed Naughton (2016, p. 5), in a paper tracking its evolution, found itself ‘in the strange position of being utterly dependent on a technological system’ that was both hugely disruptive and poorly understood. Such dependence was – and continues to be – a recipe for vulnerability.

³⁶ This quote is cited by Hoffman (2006c, p. 3) from a seminar entitled ‘Militant Islamic Political Activism on the Worldwide Web’ held at RAND’s Washington office on December 19, 2000.

This was the deeply unpredictable context in which the information revolution was ‘altering the nature of conflict across the spectrum’ (Arquilla and Ronfeldt 2001, p. 1). In terms of the developmental sequencing of network structures over time (Servan-Schreiber et al. 1989), for instance – or what could be described as the grammar of networks – Granovetter (1973, pp. 1377-1378) showed that in a complex world, strong ties could sometimes, paradoxically, lead to fragmentation, whereas weak ties could prove more resilient over time and lead to more effective integration. As a result, examining only the *strength* of ties ignored important issues to do with performance. Applied to terrorism (Basu 2014; Kennedy and Weimann 2011; Hoffman 2006b), this paradox was exemplified by a marked improvement in Al-Qaeda’s operational capabilities despite its rushed dispersal in response to the post-9/11 US military campaign in Afghanistan. Under pressure to survive and compete, networked terrorism was learning intuitively ‘the strength of weak ties’.

The emergence of ‘information-age threats’

This story of co-evolution – the broadly contemporaneous emergence of a new type of networked terrorist using a new type of networked technology, both of them deeply underestimated and neither of them fully understood – led to a switch from ‘industrial-age threats’ to ‘information-age threats’ (Arquilla and Ronfeldt 2001, p. 2). These ‘information age threats’ arose from the fact that, as had become clear with post-Cold War terrorism (Goolsby 2006), the information revolution favoured network forms of organisation over hierarchical forms (Castells 2004, pp. 3-4).³⁷ As a result, power was migrating towards non-state actors who could form themselves into multi-organisational networks more easily than unwieldy hierarchical state actors could. A good example of this was Hezbollah in Lebanon, with one foot in the social-political camp and the other in the militaristic-terrorist camp.³⁸ This meant that in conflict whoever mastered networking and controlled information stood to gain considerable advantage.³⁹ With the switch to networked structures too came a change in the concept of leadership, where strategic leadership was replaced by strategy-focused leadership. This was where the priority of leaders was to add social capital to the idea of

³⁷ ‘Networks instead of military formations ...’ as Jenkins (2015) put it.

³⁸ See Chapter Four.

³⁹ The Zapatista rebellion in the Mexican state of Chiapas in 1994 was a good example of ‘social netwar’ (Collins 2010; Martinez-Torres 2001; Ronfeldt et al. 1998).

leadership by connecting people, work processes and technology into 'communities' and enabling those communities, thereby creating organisations that were themselves focused primarily on strategy (Tarsiero 2006, pp. 208-209) and therefore more effectively goal orientated, as was notably the case with Osama bin Laden and Al-Qaeda during preparations for 9/11 (Moghadam 2013, p. 27).

The information-age threats posed by such groups were, this thesis argues, the manifestation of the much-debated 'new terrorism' whose existence had been widely hypothesised but whose key points had eluded agreement. Those who believed in this phenomenon (Hoffman 2006; Lacquer 2006b, 1999; Giddens 2004; Morgan 2004; Benjamin and Simon 2003; Khosrokhavar 2003; Bremer 2001; Lesser et al., 1999) saw it as symptomatic of the new information age rather than the industrial age, driven by religious fanaticism rather than any ideological desire for political or social change, with catastrophic intent rather than in pursuit of a place at the negotiating table. The final report of the 9/11 Commission even named its second chapter, 'The Foundation of the New Terrorism' (The 9/11 Commission Report 2004, p. 64). Others, however, were sceptical (Spencer 2006; Tucker 2001; Roy 2004, pp. 41-54; Duyvesteyn 2004; Copeland 2002). Burnett and Whyte (2005, p. 15) took their criticism almost to the point of conspiracy theory, observing that 'some elite groups' would inevitably make 'a great deal of political and social capital' out of the 'violent and socially corrosive' war on terror. They were particularly critical of the RAND Corporation which they described as 'the key institution in the development of "the new terrorism" as an ideological formation', and of what they termed 'the RAND-St. Andrews nexus' (2005, p. 8). In similar vein, in an opinion piece for *The Independent*, Aldrich (2005) described how 9/11 had led to what were, in his opinion, Draconian laws, the creation of new intelligence agencies, the expansion of MI5 to almost twice its Cold War size, and a 'surge' in intelligence assets focused on fresh targets, only to find that 'the new terrorism is not all that new'. Crenshaw (2007) was equally sceptical but more measured, examining 'the logical and empirical foundations of the "new terrorism" argument', finding it 'weak on both grounds' (2007, pp. 2-3), and concluding: 'There is no generic "new terrorist"' (2007, p. 30). Instead, she pointed out, terrorism was 'highly contingent and reactive'. Its development exhibited

‘evolutionary progression, as groups learn from their own experiences and those of others’ (2007, p. 32). She identified the broad sweep of globalisation, including the internet, as part of a cascade of changes empowering non-state actors:

Many of these shifts may be due to a changing environment, largely processes associated with what is termed globalization, in particular, such as advances in communications, access to weapons and explosives, and individual mobility ... The internet, for example, has proved an important resource for terrorists. It is a transnational means of communication, recruitment, indoctrination, instruction, propaganda, and fund-raising that largely escapes government control. (Crenshaw 2007, p. 31)

Crenshaw was correct in her diagnosis but wrong in her conclusion. Like Jenkins (2015), she identified the importance of the internet, but again, understandably – as Jenkins admitted he himself had done – underestimated the radical impact it was having, particularly the way in which it was changing the landscape of terrorism by empowering networked organisations (Castells 2004, pp. 3-4) such as the new post-Cold War breed of jihadist terrorist. By looking at the question from the point of view of complexity theory, she might have seen that ‘the sudden acceleration of the historical tempo and the abstraction of power in a web of computers’ (Castells 1997, p. 69) was the very definition of how globalisation and the information revolution were co-evolving and changing the nature of society and its actors, including those who challenged it using terrorism. To that extent, this was a story of enablement of a certain type of networked terrorism by the information technology it adopted, rather than simply the emergence *ex nihilo* of a new type of terrorist driven by religious fundamentalism. The complexity of the environment in which this took place, the myriad interactions which led to this outcome, and the pattern of emergent change this process set in train meant that Crenshaw was absolutely correct on one point: there was indeed ‘no generic “new terrorist”’. As ever, there were terrorists of greater or lesser ‘sophistication’, some of whom might at times coalesce into networks that could, for instance, be described as complex adaptive systems. However, there *was* a generic new *terrorism*. Its evolution was inextricably linked to the increasing complexity of information technology, specifically the non-linear development of the internet as a platform where consumers could ‘directly create meaning’ (Fenton 2012, p. 141). They did this not just in the form of user-generated content but to the extent that just as technology changes its users, those users change the technology as well (Arthur 2009; Naughton 2016, p. 6), creating new meaning by

virtue of that interaction and the operational changes to which it leads. This was as true of terrorists as of any other user-group, though to the extent that (i) terrorists' intentions were by definition malign, and (ii) some terrorist organisations had organizational structures that allowed them to be described as complex adaptive systems (Hayden 2013, 2006), the effect of interaction in those cases was always likely to be deeply hazardous. Broadly speaking, however, this was an example of 'risk' as 'a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself' (Beck 1992, p. 21). Or as McLuhan and Fiore (1968, p. 4) saw it, electronic media were part of 'the electrical retribalization of the West' where users of information technology were being returned to their 'pre-print, pre-literate, "tribal" balance' (McLuhan and Fiore 2001, p. 119), something now well established by the behaviour of online communications platforms such as Twitter. Arguably, what both McLuhan and Beck were inching towards in their separate ways was a common description of information technology as a complex adaptive system, self-generating, interactive, unpredictable, and propelled by co-evolution with its myriad users to drive social change in what was already morphing into 'network society' (Castells 2004, p. 3). This was a society whose very social structure was made up of networks driven by communications technology.

Information: lifeblood of a networked world

The critical importance of information – 'the new lifeblood of the international system (Conway 2003, p. 1) – became evident first in individual disciplines, mainly in the life sciences: in physics (Dittrich 2015), in evolutionary biology (Adami 2012), and particularly in genomics (Swindells et al. 2002) where the sequencing of the human genome gave an entirely new perspective on the process of adaptive evolution (Meneely et al., 2017), particularly the realization that the information stored in each biological organism's genome was used not just to maintain and control that organism but 'to generate the organism as well' (Adami 2010, p. 49), a process with striking parallels to autopoiesis, the concept of self-generation at the heart of complexity theory. This new recognition of the importance of information made clear that the internet too was 'an information infrastructure' (Leiner et al. 1997) without borders, which was expanding and continues to expand 'along several dimensions, such as scale, performance and higher-level functionality'. Previously unrelated areas were being

brought together by ‘the overarching power of code’ (Dillon 2002, p. 2), revealing, increasingly in scientifically verifiable terms, a world that was not just connected but interactive and ‘hyperconnected’ (WEF 2013; WEF 2013a). This led to the realization that information was ‘the prime mover’ in every aspect of human affairs and ‘the basic constituent of all matter’ (Dillon 2002, p. 2), human beings, and therefore terrorists, very much included (Gillings et al. 2016).

What was being described was essentially the world of biopolitics, the ‘small p’ politics of the infinite number of networked systems – all driven by information/data (Kelly 1994, p. 193) – that humankind has developed, by accident or increasingly by design, to manage its existence. Biopolitics has its roots in the thinking of Michel Foucault (1997 Nilsson and Wallenstein 2013) on modern interpretations of knowledge and power. It was the second of ‘the two great problematisations of security’ (Dillon and Lobo-Guerrero 2008, p. 264)⁴⁰, the other being geopolitics which is based around post-Westphalian sovereign territoriality (Kayaoglu 2010). In one sentence, biopolitics comprised a ‘complex array of changing mechanisms concerned with regulating the contingent economy of species life’ (Dillon and Lobo-Guerrero 2008, p. 268). According to this logic, the pervasiveness of information brought about ‘the weaponization of everything’ (Mousavizadeh 2015), potentially at least:

[B]iopolitical intercourse simultaneously both sustains and undermines itself. Air travel circulates disease as well as tourists, commerce and business. Similarly, the international financial system may be used to sustain terrorist activities as well as industrial and commercial growth. Complex national and international infrastructures vital to sustaining the very ebb and flow of biopolitical intercourse are the same mechanisms through which life also threatens itself ... It is commonly recognized now that they can be a direct function also of the very complex dynamics of the systems themselves. The war on terror has intensified and amplified these characteristic features of the biopolitics of security, but it did not initiate or invent them. (Dillon and Lobo-Guerrero 2008, p. 269)

This dawning realization that society’s very understanding of ‘life’ itself was being rapidly and profoundly transformed (Dillon and Lobo-Guerrero 2008, p. 270) by the power of information technology prompted a new paradigm for American grand strategy, known as ‘noopolitik’⁴¹

⁴⁰ In the sense of Louis Althusser’s concept of ‘problematic’ as ‘the ideological or theoretical framework without which a concept cannot exist and cannot be studied’ (Kelly 2018; Macey 1993, p. 25; Kelly 1978).

⁴¹ For Plato, ‘noocracy’ – a combination of *noos* (intellect or mind) and *kratos* (power) – was a notional social and political system to be run by professionally trained ‘élites’ (Kováč 2004, p. 7).

(Arquilla and Ronfeldt 1999), reflecting the growing importance of knowledge as a source of power. With that came a cultural pivot to network-centric thinking, where 'information, speed, self-synchronization and flexibility' were at a premium, 'just as they are in the global economy' (Dillon 2002, p. 2). In counterterrorism, 'the emergence of interconnected computer networks' represented 'the biggest post-Cold War paradigm shift in tactical intelligence collection' (Fitsanakis and Bolden 2012, p. 28). It also marked the advent of 'netwar', in which the protagonists use 'network forms of organization, and related doctrines, strategies, and technologies attuned to the information age' (Arquilla et al. 1999, p. 47).

The shock of 9/11: Understanding a new and complex opponent

Who exactly was the enemy in this network-centric world in which information had become 'the new metaphysic of power' (Dillon 2002, p. 3)? When they came, the 9/11 attacks were aimed at the very heart of the West's 24/7 information society, and in the aftermath, Al-Qaeda leader Osama Bin Laden became 'a simulacrum of the infinity of danger to which network society is exposed' (Dillon 2002, p. 5):

The destruction of the World Trade Centre on real time network TV was a strategic surprise attack on an even more complex network, global network society itself, of which the US is the epicentre. Knowledge-based, globally linked through *complex adaptive connections* of every description, the terrorists exploited the very strategic strength of network society, its openness and connectivity, to send violent shock waves throughout the capillaries that channel its flows of image, information, technology, people and capital. (Dillon 2002, p. 1, italics in original)

Given the almost epic proportions of that description, it is perhaps little surprise that terrorism quickly morphed into 'a new kind of war without end' (Dillon 2002, p. 5), characterised by Simon and Benjamin (2001) as 'The Terror', with echoes of the '*grande terreur*' of the French Revolution (Laqueur 2006, pp. 23-24). The modern-day Terror had begun, they maintained, in 1993, with the first attempt to destroy the World Trade Centre in New York. It was 'terrorism motivated either in whole or in part by a religious imperative, where violence is regarded by its practitioners as a divine duty or sacramental act' (Hoffman 2006, p. 83). There followed a host of other attacks and attempted attacks: the conspiracy to destroy 11 jumbo jets over the Pacific in 1995, the sarin gas attack in Tokyo the same year, the Oklahoma City bombing in 1996, the East Africa embassy bombings in 1998, plans for

simultaneous attacks in the US and Jordan around the time of the millennium celebrations, and the bombing of the *USS Cole* in October 2000. Then, the following year, came 9/11. As former CIA director, Jim Woolsey, observed: 'Today's terrorists don't want a seat at the table, they want to destroy the table and everyone sitting at it' (Morgan 2004, pp. 30-31). September 11, said Beck (2002, p. 39) represented 'the complete collapse of language' because 'ever since that moment, we've been living and thinking and acting using concepts that are incapable of grasping what happened then.' The attacks, said Jenkins (2002, p. 6), 'destroyed America's sense of invulnerability and illustrated the limits of its intelligence infrastructure'. They 'shattered the pre-existing, prevailing sense of personal, national and international security' (Kegley 2003, p.1).

In such an atmosphere of psychological fragility, it became clear that the evolution of information technology from the pre-internet world to the internet-enabled world had transformed not just the way terrorists communicated and controlled their messaging, but the way in which they strategised and attacked as well. This was a new level of conflict that demanded not just a sophisticated response but a new level of understanding of the attackers and how they functioned. That new level of understanding was increasingly provided by complexity theory, an overarching view of the world as non-linear, interactive, emergent, and inherently unpredictable (Holland 2014, 1995, 1992b, 1992a, 1975; Kauffman 1993, 1992, 1991b, 1991a; Mitchell 2009, 2006, 1995) rather than as previously thought, linear, mechanistic, reducible to the sum of its parts (Gerrits 2008, p. 11). In essence, it was a development of systems thinking enabled by the information revolution and the rapid evolution of the computer, 'the instrument of the sciences of complexity' (Pagels 1989, p. 36). As noted in the introduction, complexity theory had thus far been used mainly on the margins of terrorism studies to model covert terrorist networks with the aim of disruption (Tsvetovat and Carley 2005; Carley et al. 2004, 2003; Carley 2002; Carley, Lee and Krackhardt 2002),⁴² though it had been applied by Moffat (2003) to the related field of network-centric warfare. Using publicly available data, Krebs (2002) notably mapped the network centred around the 19 dead September 11 hijackers. Fellman et al. (2010, p. 6) concluded that 'terrorist networks are complex', not unlike the type of structures often typically encountered in conflict in that

⁴² It largely replaced old-style link analysis (Harper and Harris 1975) used by law enforcement agencies.

they possessed ‘multiple, irreducible levels of complexity and ambiguity’. Hayden (2013) focused on terrorist networks as complex adaptive systems, dynamic systems that adapt and change as a result of interaction internally and with their environments.⁴³ She identified specific terrorist groups as particular types of network, showing that their network designation affected the degree to which they could adapt and innovate and thus the degree to which they could be described as complex adaptive systems. An important element of her analysis was that because terrorist networks were constantly changing, their designation as complex adaptive systems was not constant; at times, some groups could be described as such, at other times not (Hayden 2013, p. 19). Mesjasz (2015, p. 38; 2008) noted that complex adaptive systems were increasingly seen as ‘the most promising tool of modelling for broadly defined social phenomena and social systems’, including terrorism. As Irene Sanders, founder of the Washington Centre for Complexity and Public Policy, observed in an article for *The Washington Post* published in the aftermath of the attacks under the highly apposite headline, ‘To Fight Terror, We Can’t Think Straight’:

The enemy we face is a loose coalition of semi-independent terrorist cells, each with a well-defined mission and a high degree of adaptability and flexibility in carrying out that mission. Al Qaeda does not rely on immediate direction from a central authority yet still maintains effective co-ordination ... and hence has been far less susceptible to intrusion or destruction. It adapts its methods to accomplish its goals. (Sanders 2002)

The 9/11 attacks still begged one key question, however. Why had terrorists suddenly been empowered to this extent now, even accepting the political ‘trauma’ after the Cold War, the speed of technological change, and the emergence of a new type of networked terrorist with international reach? The answer was the exogenous shock to the information system in the form of the internet, not so much in terms of its difference from previous technologies but – exactly as McLuhan (1967, p. 15) had predicted⁴⁴ – in terms of its scale as a new technology. As Castells (2004, pp. 2-3) had long argued, networks were not specific to twenty-first century societies. They had been the foundational structures of many advanced civilizations over thousands of years (2004, pp. 3-4). Even so, they had never achieved the dominance achieved

⁴³ For more on complexity theory, see Chapter Two.

⁴⁴ ‘[T]he personal and social consequences of any medium – that is, of any extension of ourselves – result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology’ (McLuhan 1967, p. 15).

by hierarchical bureaucracies. Why? His hypothesis, said Castells, was that there were limits to their ability to prevail, limits which, as he put it, 'were fundamentally linked to available technology' (2004, p.3). The problem for networks was that 'beyond a certain threshold of size, complexity, and volume of exchange, they become less efficient than vertically-organized, command and control structures, **under the conditions of pre-electronic communication technology**'(Castells 2004, pp. 3-4, bold emphasis in original; Mokyr 1992). In other words, they needed technological change of sufficient disruptive capacity to enable their unique networked qualities to kick in and diffuse. The internet – and to a lesser extent satellite technology and again social media – provided that disruptive capacity.

Social media: Terrorists' 'open social utility'

Social media emerged at around the turn of the millennium while Al-Qaeda was reconfiguring itself in Pakistan after 9/11 and the world was pondering how and when terrorism might deploy in cyberspace. They began in the form of blogging and initially seemed little more than novel offshoots of the 'usernets' of the late 1970s (WDD 2009), with no centralised servers or dedicated administrators. They began to develop more rapidly in 2006 with the arrival in earnest of Facebook, Twitter and YouTube. Social media were web-based, mobile-first technologies that turned communication into an interactive dialogue (Cohn 2011). In technical terms, they were Web 2.0 applications, websites based solely on interactive user-generated content (Dean et al. 2012, p. 4; Kisselburgh et al. 2010; Sharma 2008). The production, sharing, and viewing of that content led frequently to collaboration among users based on common interests, political ideologies, or often something as simple as a shared geographical location (Wooley et al. 2010). In that sense, with 2.8 billion users at the end of 2018, social media enabled and amplified social networking, giving it global reach and the capacity to fragment into an endless number of categories. Mark Zuckerberg saw Facebook as an 'open social utility' (Murphy 2020). He was correct that in marketing terms social media were something new: a cheap and effective tool of mass communication, and, in particular, a highly effective method of targeting specific demographics (Hindman 2018; Dean et al. 2012, p. 5; Earl and Kimport 2011, pp. 63-120). This was the lesson of social media that terrorist users learned even more rapidly than they had learned to adopt the internet. Social media, essentially 'made of' interaction, its users comprising an ever-expanding non-linear

constellation of nodes with no discernible patterns of use, constantly changing and therefore totally unpredictable, amounted to a whole new array of complex weapons for digital-native terrorist networkers, as Islamic State would show to lethal effect.

Here again, scale and speed came into play. Having been confined initially to students, Facebook opened to all comers in September 2006. By January 2009, it had 175 million users, rising to 500 million by July 2010, just 18 months later. By January 2018, that figure had risen to 2.2 billion users (Facebook 2018; Constine 2017). Twitter was launched in March 2006. The following year, an average of 5,000 tweets was posted every day. In 2008, that number was 300,000 a day, rising to 340 million tweets a day by 100 million users in 2010. On November 8, 2016, the day of the US presidential election that returned Donald Trump, Twitter was the largest single source of breaking news, with 40 million election-related tweets sent by 10 pm, far exceeding the 31 million sent on election day 2012 (Isaac and Ember 2016; Beaumont 2010). The rush was not just to Facebook and Twitter. By January 2009, every minute of every day 10 hours of fresh content was being uploaded to the video-sharing platform YouTube, while Flickr users were already sharing a total of more than three billion photographs. By the second quarter of 2008, such was the stampede to the new technology that 75 percent of internet-surfers used social media in one form or another, up from an already-impressive 56 percent in 2007, according to US analysts Forrester Research (Kaplan and Haenlein 2010, p. 59). By McLuhan's measure of the 'new scale' introduced into users' affairs by this evolving technology (McLuhan 1967, p. 15), social media were, as the internet had been, transformative. There were initial concerns among terrorist networks about the operational security of social media on the grounds that 'user-generated content imperils message control' and that 'social networking renders jihadists vulnerable to detection, surveillance, and arrests' (Kimmage 2010, p. 15). On both counts, they were correct (Holden 2017; Price and Al-'Ubaydi 2017; Weimann 2010, p. 49). That caution, however, was short-lived. By April 2006, former FBI consultant Evan Kohlmann reported that 'more than 90 percent of terrorist activity on the Internet now takes place using social media networking tools' (Noguchi 2006). This was to some extent to evade detection, but primarily because their audience had already followed the trend to social media.

Each of the social media had a distinct terrorist purpose (Dean et al. 2012, pp. 5-10). Facebook was used primarily for recruitment (Department of Homeland Security 2010; Torok 2010),

deploying the 'groups' function to attract sympathisers from all over the world without any significant threat to the organization. From the group, potential recruits were then directed to the organization's website or to forums used for indoctrination and training (al-Shishani 2010; Weimann 2010). Twitter, by contrast, was used for instant messaging during the 2008 Mumbai attacks by Lashkar-e-Taiba, which left 164 people dead (O'Rourke 2010; Rabasa et al. 2009; Leggio 2008). Interviews with the sole surviving attacker, combined with telephone intercepts, showed that the terrorists' controllers in Pakistan were able to provide them with a constant flow of information from public Twitter posts, including tactical information about Indian counter-terrorism units planning an assault on the hotel at the centre of the attacks (Dean et al. 2012, p. 8). It was similarly used by al-Shabaab during the Westgate attack in Nairobi in 2013 (Mair 2016). Its immediacy meant it emerged at its height as 'terrorists' favourite Internet service' (Weimann 2014, p. 8). Because of the attractiveness of video as a means of communication, YouTube also became immediately popular, featuring, for instance, bomb-making videos and videos demonstrating the use and field-stripping of an AK47 (Dean, Bell and Newman 2012, pp. 9-10; Department of Homeland Security 2010). In terms of proselytizing, Yemeni-American imam Anwar al-Awlaki⁴⁵ posted more than 5,000 videos carrying extremist messages on YouTube alone, while he was also active on Facebook (Meleagrou-Hitchens 2011; Barclay 2010; Madhani 2010; Torok 2010; Shephard 2009; Smith 2009). All of these operational activities would have been incalculably more dangerous, more time consuming, and more demanding on manpower prior to social media. In the meantime, jihadists were moving on, migrating to private channels on the encrypted app Instagram to avoid detection (Holden 2017). Autonomous communication (Conway 2005, p. 9), the holy grail for terrorists in their exploitation of media, remained as powerful an incentive as ever.

The contribution of this thesis: pre-complexity terrorism meets co-evolution

In macro terms, as noted in the introduction, the contribution of this thesis to the sub-discipline of terrorism studies is that it looks afresh, from the point of view of complexity theory, at the traditional narrative of how networked terrorism has interacted in mutually propulsive fashion with information technology, and having done so, identifies a mechanism

⁴⁵ In Yemen, al-Awlaki became the first US citizen killed by a US drone on September 30, 2011 (BBC News 2011).

by which the two interact through co-evolution, a key element of complexity theory. In micro terms, the point of connection between this literature review and what the thesis adds to the historical narrative lies in the immediate aftermath of 9/11 when a myriad different questions were being asked about the capacity of Al-Qaeda to strike such a devastating blow. A myriad questions were being asked, yet their focus was unclear. The focus of those questions was unclear not because of the psychological impact of the attack, although that did contribute to an air of fragility in Western capitals. It was unclear because the United States and its allies remained – despite having embraced an information-driven geopolitical strategy of ‘noopolitik’ well before the turn of the millennium (Arquilla and Ronfeldt 1999) – intellectually wedded, particularly at political level, to pre-complexity thinking. In addition, they had consistently underestimated Al-Qaeda as opponents and continued to do so despite the death toll. What was gradually becoming clear was that the pursuit of Al-Qaeda in Afghanistan had forced its leadership to flee to neighbouring Pakistan where it set up a ‘virtual sanctuary’ (Ranstorp 2007) and continued the transition to a diffuse and leaderless network that had begun when it first adopted the internet. The tilt had occurred where the users had begun to mimic the architecture of the technology. To an observer looking on from a distance, this was the point at which it became clear that a hyperconnected Al-Qaeda no longer needed old media to amplify its message and reach potential recruits. The internet was the message and in the case of Al-Qaeda it provided free unlimited global access to the relatives, friends and sympathisers of the ummah.

Once the internet made journalists and traditional media irrelevant, the hollowness of the traditional view of the ‘symbiotic relationship’ (Wilkinson 2006, p. 145) between terrorism and the media became apparent. The challenge – taken up in this thesis – then became to identify the mechanism by which terrorism interacted directly with information technology. Logically, following the example of Al-Qaeda’s adoption of the internet, there had to be three elements: a high-performing terrorist network; a new iteration of information technology being leveraged by those terrorists, and evidence of a significant force multiplier effect (Hurley 2005) for the terrorists as a result of their interaction. The search for other possible pairings led to Hezbollah and its switch to satellite technology, and, twenty years later, Islamic State and its flamboyant adoption of social media. It was Hayden (2013, 2006) who identified some high-performing terrorist groups, with particular organisational structures which

rendered them more agile and innovative, as complex adaptive systems. Kaufmann (1993, p. 237) revealed that a key element of complex adaptive systems was that they ‘co-evolved’ in partnerships they found to be mutually beneficial. It was this co-evolution that maximised evolutionary thrust and ‘significantly augmented performance’ (Holland 1992b, p. 11). There was one other element that made the co-evolutionary mechanism work. It was the fact that – as Castells 2004, pp. 203 noted – networked systems needed technological change of sufficient disruptive capacity to enable their unique networked qualities to kick in and diffuse. While that had not been possible ‘under the conditions of pre-electronic communication technology’, the internet, and to a lesser extent satellite technology and later again social media, provided that disruptive capacity.

The thesis adds a historical perspective to the search for the co-evolutionary mechanism by tracing the evolution of the information technology it examines and showing that the three instances, satellite broadcasting, the internet, and social media, even apart from their co-evolutionary partners, form one coherent trajectory over time. This, in turn, confirms the choice of the terrorist groups as linked in each case through co-evolution. As Chapter Four will show in more detail, satellites have three types of communications function: telecommunications, broadcasting, and data transmission, all of which are varieties of electronic information diffusion (NASA 2020; Orbital Today 2020; Maini and Agrawal 2014). The progression from terrestrial to satellite technology meant a significant increase in speed and power, so that data was now ‘transferred in gigabytes per second rather than megabits per second’.⁴⁶ At the same time, the breaking down of barriers between terrestrial and satellite technology increased interoperability, scale, and therefore force multiplier effect. That transformed Hezbollah’s global presence. In the case of Al-Qaeda and the internet, examined in Chapter Five, the process is similar. The internet was originally developed as a system that would allow the US military to link satellite systems and to transmit information to and from the front lines of distant conflict. Again, enabling satellite systems to work together increased interoperability, scale and force multiplier effect. So too with Islamic State in Chapter Six and its early adoption of internet-based social media, which allowed users to form microstructures (Knorr Cetina 2005, p. 216), in the sense of social networks who could

⁴⁶ One gigabyte (GB) equals one billion bytes, while one megabyte (MG) equals one million bytes (NIST 1998).

generate their own new material and feed it into the system, multiplying its reach and taking ownership of the process far more than in the case of the internet. The fact that hardware was gradually disappearing as part of this trajectory and being replaced by 'socio-technical terminology' such as communications protocols, platforms and networks (Lash 2003, p. 54), was also a reflection of substantially increased interoperability and complexity, as the new information technology was 'diffused throughout the entire realm of human activity by growing miniaturisation', as anticipated by Castells (2004, p. 9).

There is also a contribution to the discipline in terms of the rudimentary exploration of the architecture of the co-evolutionary mechanism that has taken shape here. Researchers 'can only discover, describe and explain mechanisms through the construction of models, and these models are invariably partial, abstract, idealized, and plural' (Glennan et al. 2021, p. 142). In that context, a helpful lesson to be learned from complexity theory is that there are two ways in which complex adaptive systems analysis and social science research can intersect productively: by thinking in terms of 'hard' and 'soft' complexity, the former developed through the use of computerized mathematical modelling, and the latter through the use of qualitative concepts of complexity found in areas such as cybernetics, systems thinking, sociology and psychology (Mesjasz 2015, pp. 40-42), and in the case in hand, molecular biology. In terms of soft complexity, cybernetics has studied the control of different systems independently of their substrates (Wiener 1948). This has allowed researchers to use the same terminology to describe different phenomena, such as electronic circuitry and neuronal circuitry, allowing the transfer of solutions from one domain to the other (Gershenson 2014, p. 1). For instance, understanding adaptive behaviour in animals contributed to the capacity to build adaptive machines (Walter 1951, 1950). It is a process with echoes of what Luhmann (1987, p. 260) calls the capacity to 'control heterogeneities through concepts'. In the case of this co-evolutionary mechanism, it is a typical information system with a three-stage input-process-output design (Clancy and Brown 2008). Although even this level of molecular biology is significantly outside the scope of this thesis, it is informative to note for reasons of comparison that those three basic elements closely mimic the relationship between DNA, RNA and proteins, and particularly the process by which genetic information moves between them (Isaacson 2021, pp. 43-44; Crick 1972). That relationship can be described simply and accurately as: DNA makes RNA, which in turn makes

proteins. However, it is not, as it seems, a straight information transfer. In the DNA-RNA-protein relationship, it is DNA which contains the genetic code. That DNA is 'transcribed' into RNA. It is RNA which then catalyses or 'translates' that code into proteins as instructed by the coded information. It is the proteins which are the expression of the overall process, the building blocks of life, as they are often called. Similarly, in the case of the co-evolutionary mechanism identified here, the new information technology provides the new code that will be used by the terrorists to strike in a new and unexpected way. It is transferred to the terrorists through interaction. Having been transferred, the terrorists then act as catalysts to translate the code into action. It is the architecture of the new information technology which will determine the manner in which the relationship between the terrorists and the technology is expressed in the force multiplier effect. 'The process of translation can be seen as the decoding of instructions' (Clancy and Brown 2008). In the case of Hezbollah and satellite broadcasting, it allowed Hezbollah to broadcast propaganda on the progress of the 2006 war directly to the homes of Israelis, despite repeated Israeli attempts to block its transmitters (Jorisch 2004c, 2004b, 2004a). This was simply the impact of an increased satellite footprint. In the case of Al-Qaeda and the internet, the internet was global, many to many, acknowledging no boundaries and this was the outline of the benefit it delivered for Al-Qaeda, allowing it to communicate globally and covertly from behind a computer, and to 'cyberplan' (Thomas 2003) as if invisible in the run-up to 9/11. More striking in the case of Islamic State and social media was the spate of lone attacks, predominantly in Europe, from 2014 until 2018 (Nesser 2019, p. 15), by attackers with marginal links to the core organisation. This reflects the reflexive capacity of social media to allow individuals to feed back into its operating system and influence the organisation and its direction, an extraordinary new level of autonomy. An examination of the three case studies also indicates that, in line with the change in power balance (Burkhardt and Brass, 1990, p. 105) that typically accompanies the 'exogenous shock' (Barley 1986, p. 80) caused by adoption of new technology, it is the terrorists who initially control the innovative new manner in which the technology is applied, for example in the case of pre-9/11 cyberplanning by Al-Qaeda (Thomas 2003), until a tilt occurs after which the technology begins to influence the operational 'shape' of the terrorist network as a result of becoming more diffuse,, in the case of Al-Qaeda underpinning it as leaderless and global at once, and in the case of Islamic State, empowering individual followers to attack on behalf of the network as a whole.

Finally, the thesis also contributes by showing how, in the detail of its structure, the co-evolutionary mechanism also sits comfortably with terrorism as a social system as defined by Luhmann (1995, 1987, 1986), who, uniquely in sociology, promotes communication to the dominant position in the pantheon of life systems, reflecting the central position it also occupies in terrorism studies (Jenkins 2015; Nacos 2007, p.14; Hoffman 2006, p. 198), while relegating human actors to the role of catalysts. This is reflected by the fact that in the co-evolutionary DNA-RNA-protein mechanism, RNA acts as a catalyst which allows the code contained in DNA to be translated into proteins. Similarly, in the co-evolutionary mechanism, the architectural design of each new iteration of information technology is catalysed by its terrorist users. However, just as Luhmann (Lenartowicz et al. 2016, p. 2) would have it, it is the communication itself and not its terrorist catalyst that matters. There is, says Stichweh (2000, p. 8), a relatively direct lineage ‘from the early information and communication theories of the late 1940s and 1950s to the adoption of communication in sociological theory, and especially in Niklas Luhmann’. That lineage is acknowledged and traced to some modest extent in this thesis, right up to the threat of information terrorism posed by the potential hijacking of genome editing (Kosal 2020; Regalado 2016).

Conclusion

The novel co-evolutionary mechanism by which a succession of networked terrorists have leveraged new iterations of information technology to lethal effect is identified in this thesis and its structure examined from the viewpoint of complexity theory. This literature review has uncovered the evolutionary trajectory of information technology, from quantum mechanics in or around 1915 to genome editing in or around 2015, that has relentlessly challenged the prevailing assumptions about life, identified it as complex in the sense of interactive, non-linear, and unpredictable, and shown how it co-evolves with networked terrorists who exploit it for their mutual benefit. The two connect seamlessly in a narrative of complex change, signposting a future driven by the same terrorist imperatives of greater technological interoperability, enhanced scale and reach, and increased communicative autonomy, although the identity of the terrorists involved will inevitably change (Kriner 2022; Newhouse 2021; Regalado 2016) as information terrorism evolves beyond the networked jihadism of the post-Cold War period. Some believe this may be ‘the beginning of posthuman

history' (Fukuyama 2002, pp. 216-218). Perhaps with it may come the same tilting of the power balance that comes with every new iteration of information technology, but on a larger scale: the beginning of posthuman terrorism?

CHAPTER TWO

The theoretical route to co-evolution: Networked terrorism and information technology as complex adaptive systems in pursuit of 'significantly augmented performance'

Introduction

Interaction has always been fundamental to systems. The English word 'system' has its root in the Greek term 'sustema', meaning 'reunion, conjunction or assembly' (François 1999, pp. 203). The concept dates to the seventeenth century when Descartes, in *Discours de la Méthode*, introduced the idea of 'a co-ordinated set of rules to be used to reach coherent certainty'. By the end of the eighteenth century, those rules were firmly established as 'a constructed set of practices and methods usable to study the real world'. The related idea of regulatory systems or cybernetics first appeared in the work of the physicist Ampere in 1843 (Vallée 1993). In the last years of the same century, however, the mathematician, Poincaré, showed that systems were not invariably stable entities. They could be, and frequently were, unstable. That would lead to chaos theory (Oestreicher 2007), and later, to non-linear dynamics (Strogatz 1994). It was 'one of the very first steps towards the establishment of a new type of qualitative mathematics appropriate for the study of complex systems' (François 1999, p. 205), systems – it became clear – whose constituent parts interacted in non-linear and therefore unpredictable fashion, on innumerable different spatial and temporal levels, to generate system behaviour. Because the study of those complex systems is interdisciplinary, drawing on fields as diverse as evolutionary biology, game theory, catastrophe theory, dynamical systems theory, and cybernetics, for its core concepts (Goldstein 1999), 'complexity science' is regarded as the appropriate term for this group of theories. However, the term 'complexity theory' is also widely used (Gerrits 2008, p. 11).

For Descartes, Newton and the other founders of modern scientific method, reductionism, the idea that everything could be explained by physics once it was reduced to its constituent parts – in conceptual terms essentially the opposite of non-linear complexity – was the key to understanding the world as mankind encountered it. They saw change as 'mechanical', in the sense that 'causality is fixed and that developments are stable, time-reversible and replicable' (Gerrits 2008, p. 11). In the first decades of the twentieth century, however, physics was

revolutionized by the discoveries of relativity and quantum mechanics, marking ‘the demise of the reductionist dream’ (Mitchell 2009, p. x). Scientists were coming to realize that reductionism could not explain the *adaptive* nature of many systems (Byrne 1998), from ant colonies to the human brain. In thermodynamics, moreover, it emerged that all complex natural processes were, indeed, irreversible (Lucia 2009; Prigogine and Stengers 1984). This pivot away from reductionism represented a schism in thinking that was widened by the power of modern computing to model the previously unthinkable⁴⁷: non-linearity (Pagels 1989, p. 36). To this day, that mismatch – between non-linear problems and linear solutions – often ‘stands in the way of understanding the real nature of the grand challenges we face and of taking appropriate action in response to a crisis’, warned a panel of world-leading academic experts⁴⁸ in complexity science in 2013. After more than 400 years of intellectual dominance, they said, linear thinking – the idea that each effect has a roughly proportionate cause – was not just out of date as an approach to complex problems, but was incorrect and potentially ‘dangerous’. ‘Complexity theory’, on the other hand, ‘has revealed many deep similarities between superficially unrelated systems and processes’ (Paperin et al. 2011, p. 609). It does not attempt to replace the canon of knowledge that already exists but provides a new way of looking at it that has the potential to explain countless underlying connections whose existence is already hypothesised, if not always fully understood.

Against that background, and given its complex multi-faceted nature, putative solutions to the problem of terrorism ‘based on single factors’ are ‘destined to fail’, maintain Schoenenberger et al. (2014, p. 16). On that basis, argues Mesjasz (2015, p. 65), more attention should be given in terrorism research ‘to the epistemological foundations and qualitative interpretations of complexity than has been done in the past.’ With that exhortation in mind, this chapter will (i) trace the historical roots of complexity science; (ii) examine how complex adaptive systems work, with observations as to how concepts from complexity theory match or illuminate issues in the study of terrorism ; (iii) pay particular attention to genetic algorithms as the competitive processes that drive the ‘emergence’ of

⁴⁷ The saying by British statistician George Box is worth keeping in mind in relation to even the most advanced modelling using supercomputers: ‘All models are wrong but some are useful’ (Box 1979).

⁴⁸ The membership of the expert academic panel, some of whom are referenced in this thesis, can be found at WEF 2013a, p. 8. Available from: http://www3.weforum.org/docs/WEF_GAC_PerspectivesHyperconnectedWorld_ExecutiveSummary_2013.pdf

complex adaptive systems; (iv) show how genetic algorithms lead to co-evolution; (v) locate both terrorism and information technology as complex adaptive systems that co-evolve; (vi) argue that both are also social systems as defined by German sociologist Niklas Luhmann, and that this explains the central position of communication in both; and (vii) consider what this means for the interaction of terrorist networks and information technology, particularly where the technology is undergoing large-scale structural change that illustrates the co-evolutionary mechanism at its most impactful:

New environments inflict considerable pain on the perceiver ... When print was new in the sixteenth century, Hieronymus Bosch painted the new confusion of spaces resulting from the Gutenberg technology invasion of the old tactile world of medieval iconography. His 'horror' pictures are a faithful artistic report of the pain and misery that result from a new technology. (McLuhan and Fiore 1968, p. 7)

The historical roots of complexity science

Modern complexity theory has its roots in the switch from hierarchical thinking to network-centric thinking prompted by the rapid acceleration of the information revolution from the invention of the first computers in the mid-1940s onwards (Drucker 1999). That switch brought with it a change from 'machine bureaucracy' (Weber 2009; Taylor 1911), which regarded systems as standardized, reductionist and closed, to more 'emergent' forms of organizational thinking which said that systems had to be flexible, open, innovative, and responsive in order to survive and prosper, especially in what had become a fast-growing, ultra-competitive, globalized, market economy (Rosińska-Bukowska 2013; Grobman 2005; McElroy 2000). This period was characterized by a string of complex innovations, from mainframe computers, atomic energy and space exploration to commercial air travel, cheap white goods, and television (Schwartz and Leyden 1997). Whereas machine bureaucracy used as its paradigm 'the view of a clockwork universe that was prevalent for much of the 18th and 19th centuries' (Grobman 2005, p. 355), the new age quickly came to reflect the counterintuitive realisation that 'to be effective, an organization must possess attributes that are simultaneously contradictory, even mutually exclusive' (Cameron 1986, p. 545). So complexity was paradoxical (Obolensky 2014). Organizations could be 'both centralized and decentralized, both general and specialist, have stability and adaptability, and [be] diversified

while “sticking to their knitting” (Grobman 2005, p. 359). Observed Goldenfeld and Kadanoff (1999, p. 87): ‘Complexity means that we have structure with variations’.

The founding of the multi-disciplinary Santa Fe Institute in 1984, in tandem with the growing power of computing, gave the discipline its first coherent identity, although, in actual fact, biology had ‘for all its modern history been the science of living complexity’, notes Claus Emmeche (1997, p. 5). ‘It is an old idea’, he observes, ‘that life, or living systems, are characterized as being organized, i.e. more complex than inorganic systems in Nature’. Jean-Baptiste Lamarck, who coined the term ‘biology’ in 1802, was the first scientist to propose and actually ‘temporalize’ the idea of a ‘chain of being’, as part of which ‘the more complex could have originated from the less complex’ (Emmeche 1997, p. 5). This led over time to the proposition that complex living systems, such as a cell, might have two complementary modes: one constituting ‘the physical-chemical workings of the cell’s components’, and the other ‘more like a linguistic or informational mode where information is selected, stored, and interpreted by the cell’s physical actions’ (Pattee 1979, 1977). There was, says Emmeche (1997, p. 6), an ‘intuitive sense of complexity as something characteristic of living organization’, a sense first noted by Kant (1951 [1790], p. 222) in his *Critique of Judgment*.

More contemporary views of complexity – noting its Latin root *plexus*, meaning intertwined (Gell-Mann 2002, p. 17) – saw it as arising from the interaction between ‘elements within a system or organization and between a system and its environment’ (Mitleton-Kelly 2000, p. 2). Human systems were often referred to as complex social systems, to distinguish them from other complex systems. This was where complexity – like technology and information – gradually became disaggregated. This disaggregation led McShea (1996, p. 479) in his analysis of metazoan complexity and whether or not it shows ‘a pervasive evolutionary trend’, to observe that ‘the more differentiated a system is, the more complex it is’. In the life sciences, in particular – but also in areas such as business theory (McKelvey 2002, 1999) – it became clear that complexity was more than simply a metaphor for the way the world worked. It reflected the reality of nature and its myriad changing biological systems (Downing 2015; Baetu et al. 2013), and increasingly the reality of its information technology-led systems as well. These, it transpired, were also evolving over time. As De Landa (1997, p. 13) put it: ‘Science, too, has acquired a historical consciousness’.

Once identified, the degree to which complexity provided a template that explained the workings of systems gradually became clear. Used in connection with science alone, Emmeche (1997, pp. 43-46) identified five different types of usage: (i) descriptive complexity, where several different methods were necessary to describe a phenomenon in a reasonably complete way; (ii) ontological complexity, which examined the complexity of real objects, systems and processes – such as a living cell, the brain, clusters of galaxies, or society – phenomena ‘located equally far from the totally ordered and predictable, on the one hand, and the completely random and disordered on the other’; (iii) complex adaptive systems, often incorporating attempts to measure their degrees of complexity, based, for instance, on logical depth (Bennett 1988), hierarchical structure (Huberman and Hogg 1985; Simon 1962), algorithmic complexity (Chaitin 1974), or measures related to Shannon’s concept of ‘information entropy’ (Soni and Goodman 2018, pp. 161-164; Grassberger 1986), where an increase in information means a reduction in uncertainty; (iv) the suggestion that science is on the cusp of ‘a major transition from a classic, simplifying paradigm to a new “complexity paradigm”’, particularly the idea that a ‘new focus on self-synthesising wholes is becoming a central part of a new scientific mode of thinking’ (to replace reductionism, in effect); and (v) the view of complexity in the social sciences, as exemplified by Luhmann (1987).

Even having parsed the idea of complexity in science, it remains extremely difficult to compare the complexity of different entities. A bacterium may be far more complex in its behavioural repertoire than any individual cell in a higher organism, no matter how complex that organism may be at supra-cellular level (Castrodeza 1978). For this reason, complexity is ‘not something to be perceived directly’ (Emmeche 1997, p. 7). It is, rather, ‘a conceptualization of certain structures into particular patterns or components in order to carry out appropriate comparisons’, a conceptualization which can, in principle, be made ‘innumerable ways’ (Castrodeza 1978, p. 470). That conceptualization is possible because what all complex adaptive systems have in common is that they are networks of information (Kelly 1994, p. 193), and networks – especially the internal connection between their topology and their behaviour (Chen et al. 2015, p. 5) – are the foundations of complexity science, having emerged from random graph theory as representations of the relationships between discrete objects (Erdős and Rényi 1959). At the outer reaches of research into the co-evolution of systems and information, eminent quantum physicist Paul Davies (2019b) defines ‘life’ as

‘how information couples with matter’. That definition, he says (Davies 2019a), leads directly to two fundamental questions in twenty-first century science: ‘How that happens ... and how information gains leverage over matter.’

Complex adaptive systems

At the heart of complexity theory are complex adaptive systems (Downing 2015; Mesjasz 2015; Holland 2014, 1995, 1994, 1992b, 1992a; Rupert et al. 2008; Mitchell 2006; Bar-Yam 2004, 1997; Axelrod and Cohen 1999; Gell-Mann 1994; Kauffman 1993, 1992, 1991a; Langton 1992; Gleick 1987; Prigogine and Stengers 1984). They form part of the biopolitical world view, the perception that the world comprises ‘a complex array of changing mechanisms concerned with regulating the contingent economy of species life’ (Dillon and Lobo-Guerrero 2008, p. 268). The intellectual grandeur of that view, which conflates an understanding of complexity with an improved likelihood of grasping the principles underlying life itself (Hawking 2000; Pagels 1988), was underlined by Nobel physics laureate Murray Gell-Mann:

I favor a comprehensive point of view according to which the operation of CAS encompasses such diverse processes as the prebiotic chemical reactions that produced life on Earth, biological evolution itself, the functioning of individual organisms and ecological communities, the operation of biological subsystems, such as mammalian immune systems or human brains, aspects of human cultural evolution, and adaptive functioning of computer hardware and software. Such a point of view leads to attempts to understand the general principles that underlie all such systems as well as the crucial differences among them. (Gell-Mann 1994, p. 19)

As with terrorism, there is no single definition of a complex adaptive system (Mesjasz 2015, p. 38; Downing 2013, p. 2; Rupert et al. 2008, p. 133). Fundamentally, they are networks of interaction. There are a multitude of working definitions, such as (i) systems that ‘change and reorganize their component parts to adapt themselves to the problems posed by their surroundings’ (Holland 1992a, p. 18); (ii) ‘a large network of relatively simple components with no central control, in which emergent complex behavior is exhibited’ (Mitchell 2006, p. 1196); (iii) ‘dynamic systems able to adapt and change within, or as part of, a changing environment’ (Mitleton-Kelly 2000, p. 2); or (iv) ‘a system of individual agents who have the freedom to act in ways that are not always predictable and whose actions are interconnected such that one agent’s action changes the context for other agents’ (Plsek 1997, p. 2).

Holland (1992a, p. 19) identified three qualities that make systems both complex and adaptive: evolution, aggregate behaviour, and anticipation. In relation to evolution, they change and reorganize their component parts to adapt to the problems posed by their surroundings. Individual parts 'evolve in Darwinian fashion' in an effort to improve their capacity to survive in their interactions with those around them. 'This ability of the parts to adapt or learn is the pivotal characteristic of complex adaptive systems' (Holland 1992a, p. 19). Because each organism and each of its elements is constantly evolving, complex adaptive systems amount, quite literally, to more than the sum of their parts, and so they show the second characteristic, 'aggregate behaviour'. Because this behaviour is representative of the complex organism as a whole, it is this that analysts typically aim to understand, and, sometimes – as in the case of counterterrorism (Hayden 2013; Ilachinsky 2005; Tsvetovat and Carley 2005; Carley et al. 2003; Carley 2002; Carley et al. 2002; Krebs 2002) – to modify or disrupt. This leads to the third characteristic: their ability to anticipate, in a fashion not too different from Pavlovian conditioning, where, 'If the bell rings, then food will appear' (Holland 1992a, p. 20). In seeking to adapt to changing circumstances, explains Holland, 'the parts can be thought of as developing rules that anticipate the consequences of certain responses', so that as Heylighen et al. (2017, p. 10) observe: 'After a while, the anticipation of a reward starts to function like a reward in itself'. Even with simple Pavlovian conditioning, however, the effects are quite complex when large numbers of parts are being conditioned in different ways, especially when the way they are being conditioned depends on the interaction of other parts. The result is that each part is, in effect, 'embedded in perpetually novel surroundings' (Holland 1992a, p. 20). This is important because in examining individual system parts in general, researchers typically focus on the optimal 'end points' of those parts, whereas, in reality, complex adaptive systems 'never get there' (Holland 1992a, p. 20). 'They continue to evolve, and they steadily exhibit new forms of emergent behaviour'. This is consistent with the view that to understand complex adaptive systems one must act counterintuitively and adopt a holistic approach rather than a reductionist one (Ahmed et al. 2008, p. 2) because 'this super-additivity is the hallmark of a non-linear system' (Downing 2015, p. 2).

There are important implications here for the study of terrorism. The first is that because 'typically, complex systems defy the prediction of global behaviour from cursory analyses of

components and their interactions' (Downing 2013, p. 2), attempts to examine learning or innovation in the context of terrorism encounter the problem of 'explanatory incompressibility' (Bedau 2008, pp. 443-459), where the only way to avoid 'surprises' is 'to observe the system itself or run very large-scale simulations' (Downing 2015, p. 2). The second is that the idea of perpetual emergence echoes the view that there is, essentially, no end-point to the challenges facing counterterrorism. Terrorism is 'not about battles or winning battles' (Jenkins 2015a). Winning simply does not apply. Terrorism will continue to evolve, adapt, and adjust, and the challenge facing counterterrorism is 'never-ending' (Hoffman 2002, p. 314). A third is that because in non-linear systems there is no proportionality between cause and effect, small 'perturbations' can result in 'massive changes to the system', and this makes behaviour challenging to anticipate where the system is closed to its environment, such as in terrorist organisations (Hayden 2013, p. 2). The result can be unanticipated and disproportionate shocks such as 9/11.

Genetic algorithms: the key to co-evolution

How does aggregate behaviour 'emerge' from the interaction of a complex adaptive system's parts? If a complex adaptive system is to evolve to deal with new situations, existing rules will not suffice: it has to create new rules. It does this through 'credit assignment' which rewards rules in proportion to the degree to which they strengthen its performance or vice versa. This also gives the system something *towards which* to evolve. This is a subtle process 'because it is important that the discovery process generate *plausible* rules, rules that are not wrong on the basis of past experience' (Holland 1992a, pp. 23-24, author's italics). The way complex adaptive systems ensure that newly invented rules are plausible is that the 'building blocks' from which those rules are built are a 'recombination' of new blocks and existing ones. This is reminiscent of the fact that there are numerous steps in technological development and that innovation frequently involves a reworking of existing products (Sinofsky 2014). Similarly, as Crenshaw (2010, p. 45) notes in relation to innovation in terrorism: 'Theories of social movements agree that innovations are not completely new; they occur at the margins or periphery of existing repertoires or familiar practices'. Rule discovery procedures of this kind are identified and described by Holland (1992a, p. 24; 1975, pp. 89-140) as 'genetic algorithms' (GAs). These are algorithms whose design is drawn from computer simulations

that mimic the processes of biological evolution in order to solve problems and model solutions (Mitchell 1995, p. 1). Holland's 'schema theorem' (Holland 1992b) and related 'building block hypothesis' (Goldberg 1989) provide the theoretical basis for the design of efficient GAs:

A genetic algorithm 'learns' automatically by biasing future generations of rules toward *combinations* of above-average building blocks (as, in genetics, coadapted sets of genes appear ever more frequently in successive generations). It can be proved that genetic algorithms find and recombine useful building blocks. They have counterparts in each of the known complex adaptive systems. Of course, many of the new rules generated by this process are nonsense, but nonsense rules do not promote 'good' behaviour and are systematically weeded out. (Holland 1992, p. 24, author's italics)

Applied to terrorism, it seems reasonable to take this learning by genetic algorithms as suggesting that terrorist networks choose among the many capacities/tools they use, and assign credit to those that have contributed to improving their performance over time or at critical junctures. On the evidence of Jenkins (2015a), Hoffman (2006, pp. 173-228), Jackson (2009, 2001), Oppenheimer (2009), and many others, that would make technology a stronger, more influential element in the overall make-up of a terrorist organization that uses it effectively, less influential where it is used less, and unimportant where it is considered not at all. Successful adoption of a new information technology by a terrorist organization therefore 'biases' its future development in favour of co-evolution, which, in turn, is 'how aggregate behaviour *emerges* from the interaction of the parts' (Holland 1992a, p. 20, author's italics).

Genetic algorithms and their function as a natural selection process having been identified by Holland (1992a), Kauffman (1993, 1992, 1991a) took the next step in the development of complexity theory by linking each organism's genetic structure to its own internal adaptive process. He conceptualized evolution as 'a process of search over fitness landscapes', where organisms are perpetually in pursuit of 'superior levels of biological fitness'. Once they achieve that next level of fitness, they are ripe for selection by generic algorithms:

Kauffman contributes to our understanding of evolution by linking this adaptive process to the genetic structure of the organism. Specifically, interdependence between an organism's genes generates the topography of the landscapes in Kauffman's model. Because the topography of the landscape

determines the likelihood of fruitful search, this connects the interdependence of the individual genes to the adaptive ability of the organism as a whole. (Fleming and Sorenson 2001, p. 1019)

Geneticist Sewall Wright (1932) first used the idea of 'fitness landscapes' as a tool for understanding the distribution of genes in the population of a species (Fleming and Sorenson 2001, p. 1021). Kauffman's NK Boolean dynamic fitness landscape is set out in robust mathematical terms in his book, *The Origins of Order* (1993). Kauffman explained his fitness landscape as 'a mountainous terrain showing the location of the global maximum (highest peak) and global minimum (lowest valley)', where the height of a feature is a measure of its fitness. What is most innovative about this model, as noted by Fleming and Sorenson (2001, p. 1020), is that Kauffman links the topography of the fitness landscape to the structure of the underlying components. He does this by developing a Boolean simulation model (Wang et al. 2012) that varies along two parameters: N , the number of components comprising the whole, and K , the degree of interdependence between these components. In this way, he defines an organism as 'a binary string of N components' (Fleming and Sorenson 2002, p. 1021). Using this model, Kauffman demonstrates that K primarily determines the topography of the competitive landscape (Kauffman 1993, p. 42; Weinberger 1991). What Kauffman has achieved is 'a dynamic rather than a static model' (Fellman and Post 2010, p. 5) to measure fitness for co-evolution. That very architecture of the fitness landscape itself 'describes co-evolution' (Chan 2001, p. 4).

Given this constant drive to compete in the fitness landscape and their constant state of emergence, it is not surprising that complex adaptive systems are frequently described as 'exhibiting a mixture of order and disorder'. This tells us that 'an understanding of complexity requires one of chaos as well' (Downing 2015, p. 5). The liminal space between the twin poles of complexity and chaos is known as 'the edge of chaos'. This is where the agents that comprise a complex system are under greatest pressure to adapt. To optimize their chances, these agents often 'co-evolve to ensure survival in the new environment' (Rupert et al. 2008, p. 134; Choi et al. 2001, pp. 352-353). This co-evolutionary process can be seen as a combination of (i) a random search by an agent over its unique 'fitness landscape' in an effort to improve its evolutionary positioning, and (ii) the exploitation of a promising agent aimed at reinforcing an organism's more-promising evolutionary tracks, thus allowing adaptation (Rupert et al. 2008, p. 134).

This underlines co-evolution as a strategy where two agents ‘together significantly augment the performance’ (Holland 1992b, p. 11) of the organism as a whole:

Organisms, economic entities, nations, do not evolve, they *coevolve*. Almost miraculously, coevolving systems, too, mutually achieve the poised edge of chaos ... The automobile replaced the horse. With the automobile came paved roads, gas stations, hence a petroleum industry and war in the Gulf, traffic lights, traffic courts, and motels. With the horse went stables, the smithy, and the pony express. New goods and services alter the economic landscape. (Kauffman 1991a, p. 6, italics in original)

How co-evolution becomes a force multiplier for terrorism

The term ‘co-evolution’ was first used by biologists Ehrlich and Raven (1964) to describe a change in a biological entity triggered by a change in a related entity, where each exerts influence and pressure over the other, affecting the evolutionary trajectories of both (Yip et al. 2008). This is a fundamentally complex concept focusing on interaction and the sequence of non-linear change it sets in train. In terms of co-evolution involving information technology, it recalls the view in the 1990s, as the overwhelming scale of the information revolution in the West became apparent (Nye 2014), that while technological change was normally incremental, punctuated by discontinuities that represented significant breakthroughs in established process (Anderson and Tushman 1990; Tushman and Anderson 1986), radical new technologies or ‘competence destroying discontinuities’ (Tushman and Anderson 1986, p. 442) were regarded as ‘exogenous shocks’ (Barley 1986, p. 80) which led to major change in the distribution of power and control (Chandler 1977) and increased ‘uncertainty’.⁴⁹ ‘Those who get the upper hand in the game are those who control most of the crucial uncertainties’ (Crozier and Friedberg 1980, p. 34). That was why early adopters of new information technologies – such as the three terrorist networks used as case studies in this thesis, Hezbollah, Al-Qaeda and Islamic State – had what was tantamount to ‘a recipe for increased network centrality and power’ (Burkhardt and Brass 1990, p. 107). They were identified as experts and sought out by others (Crenshaw 2008, p. 26), and, given their structural identities as core-periphery networks (Hayden 2013, p. 8), the diffusion of that new expertise was likely to be rapid and extensive, as was particularly the case with Al-Qaeda and Islamic State. This

⁴⁹ Uncertainty is defined as ‘the difference between the amount of information required to complete a task and the amount of information already possessed’ (Galbraith 1977, pp. 36-37).

is a striking reminder too of the impact of the internet as epoch-making technology that was cheap and accessible⁵⁰ and so rapidly became ‘the instrument of a political power shift’ (Conway 2005, p. 6).

That reciprocity identified by Ehrlich and Raven (1964) remains the key element of co-evolutionary relationships stressed by all definitions today (Mitleton-Kelly and Davy 2013, p. 43). Beyond that, there are differences in emphasis: while biology focuses on selection and competition, the social sciences tend to focus instead on adaptation and change. In their review of the literature on co-evolution, Mitleton-Kelly and Davy (2013) look at the concept in five settings: the social sciences, economics, socio-technical systems, human culture and cognition, and human ecology and ecological economics. Socio-technical systems (2013, pp. 48-50) are most pertinent here, focusing on the ‘mutually constitutive role’ of information systems in shaping organisations and of organisations in shaping information systems (Kim and Kaplan 2006, p. 37). They also identify ‘continual change’ as a fundamental factor in the co-evolution of socio-technical systems (Benbya and McKelvey 2006b; 2006a; Mitleton-Kelly 2013; Mitleton-Kelly 2011). That new emphasis on change and ‘change management’ (Newton 2019) and the consequent pivot towards complexity in management thinking identified by McKelvey marked a significant change in attitude in the discipline (Kim and Kaplan 2006, p. 36). Previous analysis had typically focused on how new systems should be implemented, on employee resistance to change, and, frequently, on the misalignment between the organization’s needs and the solution. The problem with that reductionist view was that it ignored ‘the co-evolutionary phenomena that drive both in new and largely unanticipated directions’. That brought a gradual realization that information system alignment was not a single event but a complex process of continuous adaptation and change. It was, in fact, ‘a co-evolutionary process’ (Mitleton-Kelly and Davy 2013, p. 48).

This new recognition of the ‘deep interconnectedness of the technological and the social’ (Axtell 2004, p. 2) led to the conclusion that, for successful corporations, traditional top-down engineering would be ‘inadequately static’ and that ‘managers should see information system design projects as “complex adaptive systems” in order to deal with evolutionary complexity’ (Mitleton-Kelly and Davy 2013, p. 48; Benbya and McKelvey 2006b). The co-evolution of

⁵⁰ As CRISPR gene editing technology is today.

terrorism and information technology can be seen as another example of such ‘deep interconnectedness’. The willingness of Osama bin Laden, for example, to welcome a project as radical as the 9/11 attacks, brought to him in its raw state by Khalid Sheikh Mohammed, was a striking example of the enabling function of complex leadership (Moghadam 2013, pp. 21-23). McKelvey (2002, p. 3) identifies six types of co-evolution, two of which seem apposite to terrorism: (i) *predator-versus-prey co-evolution*, where sustained countermeasures lead to a sustained terrorist response and a sustained terrorist response leads to increased countermeasures; and (ii) *co-evolution between a change rate and its environment*, where the more information technology develops, the more people develop IT skills, and the more people (including terrorists) develop these skills, the more rapidly the technology develops. Co-evolution, this thesis argues, is the ‘recurrent causal architecture’ (Downing 2015, p. 7) which enables terrorist networks to exploit information technology to their mutual benefit as a force-multiplier.

It is also worth noting that the gradual acceptance of the idea of ‘continual change’⁵¹ in socio-technical systems can be regarded as linking to ‘phase transitions’ in complexity theory (Langton 1990; Solé 2011), changes in the internal symmetry of technology in the form of transitions between alternate states, usually in pursuit of optimization. Phase transitions are ubiquitous and constant, vary in scale, and appear fundamentally connected to collective computation, the ability of biological systems to create their own macroscopic worlds (Flack 2017). ‘There is considerable evidence that computation is done in complex systems on the so-called “edge of chaos”’ (Har Shemesh 2017, p. 24). An example of this is the way in which coherent behaviour results from the firing decisions of billions of neurons in the brain (Flack 2017). This has significant implications for understanding the role of information in nature, particularly (i) the idea that collective computation may be linked to the ability of a complex adaptive system to store, transmit and modify information (Langton 1990, p. 13), and (ii) the proposition that evolution amounts to the process by which life has gained ‘local control over a successively greater number of environmental parameters affecting its ability to maintain itself at a critical balance point between order and chaos’ (Langton 1990, p. 13). For the study of terrorism, it may, for example, position collective computation as the active element

⁵¹ Or a ‘historical consciousness’, as suggested by De Landa (1997, p. 13).

behind the co-evolutionary mechanism by which terrorists identify and ever more confidently embrace the next emerging information technology as not alone mutually beneficial, but as likely to be even more mutually beneficial than the last.

Terrorism and information technology as complex adaptive systems

Having underlined the importance of the switch from linear to non-linear thinking (WEF 2013a) and traced the roots and workings of complexity theory up to the point where evolution morphs into co-evolution, the aim now is to identify both terrorism and information technology as complex adaptive systems, and to describe how they co-evolve in a manner that is mutually beneficial in that it magnifies the threat they pose together.

Terrorism as a complex adaptive system

The challenges posed by ‘terrorism in a complex global society’ are characterized by Mesjasz (2015, p. 52) as the ‘New Security Dilemma’, a term taken from the paper, ‘Terrorism and the New Security Dilemma’, written in 2005 by Philip Cerny. In taking his lead from Cerny, Mesjasz (2015, pp. 51-52) has two aims: to recognize, as Cerny did, ‘that there is a new problem and that it calls compellingly for a new kind of solution’, but more than that, to identify the core elements of Cerny’s new security dilemma as essentially the same elements that would today, with an improved understanding of complexity theory, lead to terrorism – just one of the elements at the heart of Cerny’s security dilemma – being described as a complex adaptive system. Why is Cerny’s analysis so apposite to complexity thinking? Because, says Mesjasz, Cerny’s view reflects a shift in focus from state security to the security of other referent objects, including individuals. In other words, it represents a shift from the geopolitical to the biopolitical. In making that shift, he argues, Cerny created a new security theory with roots in both Foucault and McLuhan, the former in terms of a biopolitical view of police and policing that focused more on public health, social welfare and regulating the marketplace than on arresting and jailing criminals (Johnson 2014; Foucault 1977), and the latter in terms of the postmodernist fragmentation of cultures and societies reflected in McLuhan’s ‘global village’ (McLuhan and Powers 1992). In that context, Cerny (2005, pp. 11-13) identified twenty-first century terrorism as more transnational and diffuse. It involved new ‘networks and patterns of violence’. It featured ‘quasi-random targeting of civilians’. That fragmentation of the

globalised international system he described as ‘neomedievalism’, a world, he says, best described as one of ‘durable disorder’. One might equally see the world Cerny describes as not alone complex and non-linear but as permanently on ‘the edge of chaos’:

We are increasingly in the presence of a plurality of overlapping, competing, and intersecting power structures – institutions, political processes, economic developments, and social transformations – above, below and cutting across states and state systems. States today represent only one level of this power structure, becoming more diffuse, internally split, and enmeshed in wider complex webs of power. This structure is fluid and fungible, feeding back and undergoing continual adjustments and ad hoc responses to a rapidly changing environment. (Cerny 2005, p. 12)

Where does one look for this complexity in the lexicon of twenty-first century terrorism? There are four questions, says Mesjasz (2015, pp. 52-54) that constitute ‘a point of departure in the search for “complexity era” terrorism’: (i) how can terrorism, treated as collective behaviour, be defined in systems terms; (ii) are there new forms of terrorism that are particularly able to affect contemporary complex society; (iii) are there specific features of modern society that make it more vulnerable to terrorism; and (iv) what are the negative consequences of countermeasures addressing this type of terrorism?⁵² The answers may be found, at least partially, Mesjasz (2015, pp. 53-54) contends, in the ‘new’ terrorism (Hoffman 2006; Laqueur 2006b, 1999; Giddens 2004; Morgan 2004; The 9/11 Commission Report 2004, p. 64; Benjamin and Simon 2003; Khosrokhavar 2003; Bremer 2001; Lesser et al. 1999) versus ‘old’ terrorism (Crenshaw 2007; Spencer 2006; Aldrich 2005; Burnett and Whyte 2005; Duyvesteyn 2004; Roy 2004, pp. 41-54; Copeland 2002; Tucker 2001) debate. Useful strands may also be found in attempts at ‘periodizing’ terrorism into ‘waves’, suggests Mesjasz. Among the elements of interest that he identifies – many of which fit together as proposed by this thesis – are the persistent threat of CBRN weapons, the indiscriminate nature of attacks and their religious inspiration, the networked structure of terrorist groups, the impact of the internet, and the proliferation of media, combined with the idea of terrorism as ‘an act of communication’ (Nacos 2007, p. 14). He concludes, however: ‘Several marks of distinction or discontinuity have been proposed’, but ‘nothing has yet really come out of this effort’ (Mesjasz 2015, p. 53).

⁵² All four questions are, arguably, answered in Hayden (2013, 2006) and Beck (2002), which address the non-linear nature of terrorism.

Perhaps a more productive way of looking at the relationship between terrorism and complexity, which illustrates the nature of terrorism as both complex and adaptive, is through the lens of 'risk society' (Beck 2009, 2002, 1992; Giddens 1999), defined as a society that has emerged 'as a consequence of changes in contemporary society on a global scale, which, for the most part, can be summarized in a single word – "modernization"' (Mesjasz 2015, p. 54). From this perspective, the vulnerabilities caused by the interdependence of major elements of the global system are known as 'manufactured risk', where contemporary society is 'forced to accord highest priority to the mega-threats it itself has generated' (Beck 2009, p. 8). Where does terrorism stand in this risk society? While environmental and economic crises may be understood as 'side effects of radicalized modernization' (Beck 2009, p. 15) or unintentional catastrophes, terrorist attacks must, by contrast, be understood as intentional catastrophes. 'More precisely, they conform to the intentional triggering of unintentional side effects' (Beck 2009, p.15). This means that the principle of deliberately exploiting the vulnerability of modern civil society replaces the principle of chance and accident. Terrorists need magnify only 'residual risks' in order for a highly complex hyper-connected world to immediately 'globalize the "felt violence" which paralyses modern society and causes it to freeze with panic' (Beck 2009, p. 15). What is most striking about this scenario, says Beck, is how the anticipation of terrorist attacks is ultimately 'manufactured' in involuntary interaction with the power of Western mass media, Western politics and the Western military. 'To put it pointedly', he contends (2009, p. 15), 'the belief in "global terrorism" springs from an unintended self-endangerment of modern Western society' (Beck 2009, p. 15). That being so, 'security solutions alone cannot be successful' (Ahmed et al. 2018, p. 5). In terms of the negative consequences, the most ironic is certainly that in order to protect their citizens, states increasingly limit civil rights and liberties, with the result that free society is curtailed but the terrorist threat is not diminished (Mesjasz 2015, p. 55). Fundamentally though, at the heart of risk society, are information-age threats, most cogently in this case threats posed by the co-evolution of terrorism and information technology.

While it is one thing to locate terrorism in a world whose functioning can be described and perhaps explained by complexity theory, it is another to say that terrorist networks are, in and of themselves, complex adaptive systems or that a particular terrorist organization is such a system. Having described how complex adaptive systems are constituted, how pervasive

they are, how they function and self-perpetuate, and how they co-evolve with other systems, it may even seem likely on the face of it that terrorism is one such; that it is 'obvious' (Ahmed et al. 2018, p. 3). Often, a perceptive and well-informed description can be almost enough to convince. It is from such persuasive descriptions⁵³ that Ilachinski (2005) derives the proofs he says are essential if terrorist networks such as Al-Qaeda are to be accurately described as complex adaptive systems:

... that they consist of widely dispersed, autonomous cells that obey a decentralized command-and-control hierarchy; their mission operatives are highly adaptive and mobile; their cells are strongly compartmentalized, structurally robust, and largely impervious to (unfocused) local attack; and though the networks, as a whole, are typically covert and amorphous, they can also rapidly coalesce into tightly organized local swarms. This implies that, in principle, terrorist networks, as dynamical systems, ought to be amenable to the same methodological course of study as any other complex adaptive systems (such as natural ecology, a biological immune system, or the human brain). In particular, fundamental insights into the behaviour of terrorist networks – including an understanding of *how they form, how they evolve, how they adapt* (to changing internal and external contexts), and what their innate strengths and vulnerabilities are – may be gleaned by studying the patterns that emerge from a multiagent-based simulation of their dynamics. (Ilachinski 2005, p. 1, author's italics.)

In determining how far the empirical evidence actually leads, Lichtblau et al. (2006, p. ES-1) conclude that there is 'a *prima facie* case that complexity theory in general, and ABM (agent-based modelling) in particular, are probably good methods – maybe even the best – for analysing terrorism and similar phenomena'. In fact, they go further and decide that 'terrorist groups considered *qua systems* are no doubt *adaptive*' (2006, p. ES-1), just as the US Quadrennial Defense Review (2010, p. 6) warned that 'our terrorist adversaries continue to learn and adapt' and Crenshaw (2018) refers to 'jihadis' adaptability and diffusion'. However, Lichtblau et al. (2006, p. ES-1) then hold back and say of such groups, despite the asymmetric threats they pose: 'it is not obvious that they are *complex* in the formal or theoretical sense of that term'. They reach this conclusion even though they concede elsewhere that 'asymmetric adversaries (in particular, transnational terrorist networks) seem to exhibit complex adaptive system (CAS) behavior' (Lichtblau et al. 2006. p. 3).

⁵³ In particular, Irene Sanders' striking description of Al-Qaeda in Chapter One (Sanders 2000).

That question of whether terrorist cells are complex adaptive systems – or, at the very least, whether *some* terrorist networks may legitimately be described as complex adaptive systems – is answered in the affirmative by Passig and Hasgal (2006). For them, a complex adaptive system ‘imitates the survival principles of natural systems’ (2006, p. 3). Terrorist organizations that operate in this way function as interactive networks of independent cells (2006, p. 1). Passig and Hasgal use Dooley’s study of organizational complexity to guide their understanding of what constitutes a complex adaptive system. A common element of all such systems, says Dooley (2004, pp. 1-3), is that they incorporate the dimension of time, which few previous organisational paradigms have done. That is particularly important when studying phenomena involving change⁵⁴ – as this dissertation does – ‘as change can only be defined and studied over time’. This allows complex models to go beyond a ‘mere progression of activities and events’ to explicitly articulate ‘the generative mechanisms responsible for change’, which is precisely the aim of this dissertation. In that sense, Dooley maintains, complex adaptive systems are unique in that they combine ‘a variance theory’ and ‘a process theory’. As a result – precisely as this thesis contends about the potential of examining the interaction of terrorism and information technology from the perspective of complexity theory – ‘complexity science answers both the “how” and “why” of organisational change’ (Dooley 2004, p. 3).

A pioneer of agent-based synthetic warfare, Ilachinsky (2005) reaches a similar conclusion to Passig and Hasgal though by a different route. He reviews the analytical and modelling tools used in the study of dynamic networks and attempts to design ‘a new multi-agent based toolkit’ which ‘uses autonomous, intelligent, agents to represent the components of *coevolving* terrorist and counterterrorist networks’ in order to understand how they work. His three main conclusions are: (i) terrorist organizations are, fundamentally, self-organized, emergent, multicellular organisms; (ii) the topology, behaviour and function of terrorist networks co-evolve with their ‘enemy’, i.e. whoever seeks to disrupt them; and (iii) the best approach to understanding how terrorist networks operate – how they form, grow, evolve and adapt – is one that combines several related disciplines: ‘complex systems theory,

⁵⁴ As noted earlier in this chapter is a business context (McKelvey 2002).

network science, social network analysis, mathematical graph theory, and multi-agent based modelling' (Ilachinsky 2005, p. 9).

The views of Passig and Hasgal and then Ilachinsky are reinforced by Marion and Uhl-Bien (2003). They look, in particular, at 'complex leadership' in Al-Qaeda and argue that, where it applies, both organization and leader are the 'products of interactive dynamics' in that 'leaders do not create the system but rather are created by it through a process of aggregation and emergence' (Marion and Uhl-Bien 2003, pp. 55-56). This can only happen where the idea of complex leadership 'permeates the organization' so that the differences between 'leader' and 'follower' are 'blurred'. The effect of this 'distributed intelligence' is that 'human capital' (Becker 1975) is 'maximally enabled' (Marion and Uhl-Bien 2003, p. 69). That process is aided by 'autocatalysis', the tendency in recursive systems to self-generate catalysts that speed up or enable aggregate behaviour and evolution (Marion and Uhl-Bien 2003, p. 61; Kauffman 1993, 1986). As a result, complex leadership is totally distinct from 'traditional notions of leadership as a formal position of control'. This, they argue, explains the emergence of Osama bin Laden (Hayden 2013, p. 12) in the context of 'a highly adaptive learning organization' (Marion and Uhl-Bien 2003, p. 73).

Hayden (2013) takes the most rounded approach to the question. She notes that treatment of terrorist organizations as complex adaptive systems has become 'routine' in the security community, with 'an abundance of models' focused on understanding their structural strengths and weaknesses 'with the ultimate goal of disruption and defeat' (Hayden 2013, p. 1). Despite this, the evidence suggests that the majority of these organizations 'show surprisingly little of the type of innovation that is often characteristic of CAS'. Not alone that, but while most experts acknowledge the key role that innovation and learning play in providing terrorist organizations with the capacity to adapt, 'there is a paucity of systematic treatment of the topic'. That being so, Hayden (2013, pp. 1-2) sets out to generate criteria for applying the complex adaptive system paradigm to terrorist organizations; to propose a framework for innovation and learning in complex adaptive systems; to bring those two together to model innovation and learning in terrorist organizations, and to examine what evidence exists in support of that model. As to the provenance of her analysis: 'Historical evidence of terrorist organizations and their activities over more than 30 years supports the qualitative predictions of the framework', specifically evidence from the Global Terrorism

Database (2012), and BAAD, a US government platform offering updated, vetted and sourced terrorist narratives.

The most important criterion for applying the complex adaptive system model to a terrorist network is that members must be 'in *regular interactions* that lead to *system behaviour* as a whole' (Hayden 2013, p. 2). Evolution, adaptation, learning and innovation are also important features of complex adaptive systems and can be conceptualized as a system's responses to different types of internal and external feedback (Hayden 2013, p. 4). This feedback is 'self-organizing' in that the system is responding automatically to internal network drivers 'such as competitive goal-seeking', external forces such as counterterrorism, or unexpected shocks (Hayden 2013, pp. 4-6). At the same time, that capacity to learn, innovate, evolve and adapt is also influenced by which of the many types of network structure – for example, random networks, small world networks, core-periphery networks, ring networks, windmill networks and reinforced wheel networks – best describes a given terrorist group. This is because network structures 'influence and constrain the processes of evolution, adaption, innovation and learning through information exchange mechanisms' (Hayden 2013, p. 6). Strategic purpose, leadership, group dynamics, methods, and resources also appear as 'feedback loops' having a positive or negative influence on decisions, depending on circumstances.

Having established that different types of network reflect the make-up of different terrorist groups, the next question is how innovation 'happens' in each case. In this context, an important analytical tool is the Cynefin framework, a conceptual 'sense-making device' (Kurtz and Snowden 2002, p. 462) which combines a means of analysing a system's state, particularly the degree to which it is ordered, with a means of measuring the possibility of innovation based on that system state. Knowing the level of order in a system is a prerequisite to discovering to what degree it is capable of innovation (Snowden and Boone 2007). Once innovation occurs, a process of diffusion takes place that has been 'well characterized', says Hayden (2013, pp. 11-12). Each of the steps involves interaction and information exchange with the external environment, where an agent acquires knowledge of the innovation, followed by a period of actively seeking more information, followed by the decision stage, where the innovation is accepted or rejected based on relative advantage, compatibility, ease of use, the possibility of experimentation, and the visibility of the innovation. This is all familiar territory from the discipline of terrorism studies, particularly terrorist innovation and

technology acquisition (Ranstorp and Normark 2015; Crenshaw 2010; Jackson and Frelinger 2009; Oppenheimer 2009; Dolnik 2007; Clarke 2004; Jackson 2001) and, says Hayden, is all behaviour 'well represented within the framework of self-organizing, goal-seeking, CAS'. As regards the capacity of terrorist organisations to be legitimately described as complex adaptive systems, Hayden (2013, pp. 19-20) leads to six main observations: (i) at some times, some terrorist organizations exhibit complex adaptive system characteristics, depending on the structure of the organization; (ii) the degree to which they can adapt and are likely to exhibit innovative behaviour may change over time in response to system dynamics catalysed by interactions with their environment; (iii) success by covert organizations stimulates countermeasures; (iv) terrorist resilience requires innovation in the face of those countermeasures; (v) two counteracting feedback loops compete with innovation drivers: the first being the need for secrecy, and the second, the need for 'recognized successes', meaning the greater the need for secrecy and the more failure-intolerant the organization, the less likely innovation will be; (vi) organizations most likely to show innovation and learning will be those with core-periphery networks, 'where ideas from outliers can be quickly assessed and assimilated and exogenous shocks can be distributed' (Hayden 2013, p. 20).

Given that importance, core-periphery networks require further examination. They evolve as elements on a periphery join a core to exploit economies of scale, or as a core expands in pursuit of resource exploitation. Political examples are 'bandwagoning' and colonization. Social examples include networks of friends. In the online world, information diffusion and virus propagation exhibit core-periphery structures. All three of the terrorist networks used as case studies in this thesis have distinct core-periphery elements to their development. 'Terrorist organizations that enjoy state sponsorship, such as Hizbollah, are more likely to evolve into core-periphery networks' (Hayden 2013, p. 8). And while Al-Qaeda does not have such state backing, its hierarchical structure and inclination to centralize its strategy, combined with a willingness to delegate and outsource attacks, arguably exhibit qualities of a core-periphery structure. In addition, Goolsby (2006, p. 2) explains how Al-Qaeda 'evolved' by 'co-opting other groups, hijacking their agendas and transforming their ideologies'. Islamic State, which began life as an Al-Qaeda offshoot, finally broke away and co-opted huge numbers of online supporters using social media (Berger 2014). In relation to contagion – the view that 'terrorists learn from the experiences of others ... hence the existence of patterns

of contagion in terrorist incidents' (Crenshaw 2008, p. 26) – it is also worth noting that core-periphery networks have 'much higher transmission rates' (Hayden 2013, p. 8) than some others. This means they are more likely, for example, to adopt an unproven technology, something that would normally require 'multiple social proofs' within the group (Hayden 2013, p. 8). Where such a group adopts a powerful new iteration of information technology, the result can be a rapid and unforeseen force-multiplier effect, as noted earlier by Knorr Cetina (2005, p. 213).

Information technology as a complex adaptive system

If technology can be defined as 'the application of scientific knowledge' for practical purposes, then information technology comprises 'a converging set of technologies in microelectronics, computing (hardware and software), telecommunications, broadcasting, optoelectronics and even genetic engineering', each with its own expanding array of applications (Low 2000, p. 4). The logic of including genetic engineering is that it involves 'the decoding, manipulation, and reprogramming of the information codes of living matter' (Castells 1996, p. 30). As the world has become more complex and dependent on information, information technology has come to be seen simply as 'technology', regarded metaphorically as 'the new lifeblood of the international system' (Conway 2003, p. 1). It plays a profound role in shaping the global risks landscape because of its own myriad internal vulnerabilities, illustrated by its susceptibility to cyberattacks (WEF 2019, p. 7). It is also a fundamental driver of terrorism by virtue of terrorists' exploitation of the internet to increase their global reach (UNODC 2012, p. 1). The purpose of information technology is to make itself available to be used as an operating system. It does this by co-evolving with its creators and anticipating the needs of its users.⁵⁵ 'New technologies are constructed mentally before they are constructed physically' (Arthur 2009, p. 23). That interaction between technology and user involves an exchange of information leading to a change in the power balance between them (Burkhardt and Brass 1990, p. 105), with results that are not always predictable. This clearly depicts information technology as a complex adaptive system. It also underlines an important point made by Crenshaw (2010, p. 2): that in attempting to understand the evolution of terrorist

⁵⁵ Along with evolution and aggregate behaviour, Holland (1992a, p. 19) identified anticipation as one three core characteristics of complex adaptive systems.

organizations, focusing on them 'in isolation addresses the issue of agency but misses the significance of interactions'. Taking interaction into account, information technology 'enables humanity to surpass itself 'and to 'supersede its history' (Davies 2016, p. 81). That broad set of 'humanity' includes the subset of terrorists.

Butler (1998) divides the history of communications technologies into four periods: pre-mechanical, 3000 BCE to 1450 CE; mechanical, 1450 to 1840; electromechanical, 1840 to 1940, and electronic, 1940 to the present. 'Autonomous' might arguably come next. Information technology, however, forms part of the electronic period. The term 'information technology' was first used by Leavitt and Whistler (1958) in an article for *Harvard Business Review* which warned that its impact would lead to dramatic organizational change, which it did. Information Systems are the software and hardware that emerged in support of that organizational change and that today support data-intensive applications (Piccoli and Pigni 2018, p. 28). What information technology and information systems have in common is information, which is why the 'developed' world came to be described as 'information society' (Crawford 1983), based on knowledge rather than on the residual mechanics of industrial society. This is also why, in the theory of terrorism and specifically in the literature on destabilizing terrorist networks, a key indicator of success is where 'the rate of information flow through the network has been seriously reduced, possibly to zero' (Carley et al. 2002, p. 84).

Out of that technologically transformed information society emerged the internet, opening up 'a seemingly infinite variety of new forms of interaction' (Heylighen and Lenartowicz 2017, p. 1) at such staggering speed that discerning stable trends became more and more difficult (Heylighen 2016). Information society became 'network society' (Castells 2010, 2007, 2004, 1996). To come to terms with this 'tangle of uncertain, complex and ambiguous' developments, the idea of a 'global brain' (Vidal 2015; Bernstein et al. 2012; Russell 1995) was developed, initially as a metaphor for the growing interconnectedness of the world but then as 'an increasingly realistic model of the present information society' (Heylighen and Lenartowicz 2017, p. 1; Heylighen and Bollen 1996). It was an idea that originated with two of the nineteenth century founders of sociology, Emile Durkheim and Herbert Spencer, and their intuitive observation that society was in many ways similar to an organism. That led in the 1920s to the original conceptualization of the 'noosphere' by Teilhard de Chardin (1959)

and Vladimir Vernadsky (1926). In some ways a natural extension of the concept behind the internet (Berners-Lee and Fischetti 1999) and in others ‘a conceptual framework for the augmentation of man’s intellect’ (Engelbart 1988; McLuhan 1967), the global brain was defined in modern-day terms as ‘the self-organizing, adaptive network formed by all people on this planet, together with the information and communication technologies that connect them to a cohesive system’ (Heylighen and Lenartowicz 2017, p. 1). While it is, strictly speaking, outside the remit of this thesis, it brings the question of information technology as complex adaptive system straight to the heart of contemporary research in sociology and information technology, research where the switch from linear to non-linear thinking is an intellectual ‘given’, as is the complementary view of the world as a self-generating network of interacting and interdependent complex adaptive systems.

At a more specific level, the relationship between complex adaptive systems theory and information systems research is examined by Onix et al. (2012) in a literature review that examines how concepts associated with complex adaptive systems are used for theorizing information systems phenomena. They identify three key areas in which complex adaptive systems provide a new way of exploring ‘dynamic phenomena’ in information systems: agile software development and processes (Vigden and Wang 2009; Martin 2002), system dynamics (Duggan 2016, pp. 1-24; Hildebrand et al. 2012), and bottom-up IT use processes (Nan 2011), all areas where emergence, interaction, and self-organisation are features of their development. While there is a clear fit between complexity theory and those particular aspects of information systems, the mistaken assumption of most traditional researchers in this area, say Onix et al. (2012, p. 10), has been that systems/organizations tend towards a state of equilibrium where ‘all unstable dynamics are deemed to be a consequence of social disorganisation, faulty design, malfunction or deviancy’ (Young 1991) and therefore excluded from consideration. A similar mistaken approach is often taken to interdependence in research, which is driven out of research designs to reduce the level of uncertainty in their outcomes (Fleming and Sorenson 2001, p. 1036).⁵⁶ This, argue Onix et al. (2012, p. 10) is short-sighted and ‘undervalues research attention to the dynamic properties of systems, which are

⁵⁶ As the introduction to this chapter notes, it was shown first by Henri Poincaré towards the end of the nineteenth century that systems could be unstable.

core to complex adaptive systems', where an understanding of disorder is as important as one of order. Among those dynamic properties, they specify, is 'co-evolution of IS resources'.

From information systems, Fleming and Sorenson (2001) look at information technology as a complex adaptive system and are clear that their study 'presents empirical support for complex adaptive systems theory' (2001, p. 1037). They argue that technological change and invention are forms of evolution, a view they underpin by pointing to a long tradition of borrowing biological frameworks to understand both. More than 80 years ago, Gilfillan (1935, p. 275) noted: 'The nature of invention ... is an evolution rather than a series of creations, and much resembles a biologic process'. Schumpeter (1942, p. 82) noted that inventions 'illustrate the same process of industrial mutation – if I may use that biological term – that incessantly revolutionizes the economic structure *from within*, incessantly destroying the old, incessantly creating a new one'. Abernathy and Utterback (1978, pp. 40-47) argued that technologies follow a 'technological life-cycle' like living organisms, in that they are born, mature, obsolesce, and die. Tushman and Anderson (1986), drawing on paleontology and life before the Holocene Epoch (Eldredge and Gould 1972), took the view that technology moves through periods of equilibrium punctuated by intervals of rapid change. In terms of complexity, these might be regarded as periods of order and disorder, one only being possible because of the presence of the other, with constant emergence towards the edge of chaos and significant structural change. This, in a sense, is the lifecycle of information technology as complex adaptive system.

Nowhere, perhaps, is information technology as complex adaptive system more evident than in the form of the internet, described by Rupert et al. (2008, p. 133) as 'a complex, open dynamic network exhibiting a self-organizing adaptive behaviour'. They approach the Web by identifying the key characteristics of complex adaptive systems and showing how those are reflected in its basic behaviour. It is non-linear in that its development cannot be predicted by simply understanding how each component works, and this is evident from an analysis of its growth and evolution (2008, p. 13). In terms of emergence and self-organization, the web has no global control or authority. Web authors are free to add or delete pages and websites, and to create hyperlinks to any page or node in the web graph. Despite this decentralized process, the web self-organizes into communities (Flake et al. 2002, pp. 66-71). Observe Rupert et al. (2008, p. 134): 'Since its creation, the structure, content and usage of the web

have been coevolving and adapting to each other'. An example of how complex adaptive systems reinforce promising tracks and thus allow adaptation is the way in which new pages are typically linked to a more connected page, such as Google. This is a textbook example of preferential attachment (Flaxman et al. 2007) and has distinct echoes of Hayden's description of core-periphery networks in the context of terrorism, where elements on the periphery join the core to exploit economies of scale (Hayden 2013, p. 8). Page tagging, which helps to analyse the behaviour of users when they move between different page views, is the mechanism that facilitates the formation of aggregates by making the system more responsive with every person who uses it. Flows, the manner in which information circulates through the nodes of a complex adaptive system, can be seen in the way information flows from web page to web page through hyperlinks. Diversity, which ensures the dynamic adaptive behaviour of a complex system, can be seen in the way the web has a large number of interacting elements and actors, including users classified as random users, rational users, and recurrent users. All of this diversity contributes to resilience (Duchek et al. 2019).

Another concept underpinning the view of the internet and information technology as complex adaptive systems is that of stigmergy, developed by Pierre-Paul Grassé (Theraulaz and Bonabeau 1999; Grassé 1959) in his examination of termite behaviour. It shows how simple systems can produce a wide range of more complex co-ordinated behaviour simply by exploiting the influence of the environment. Thus, in relation to information technology, weblogs, web communities, and search engines such as Google, all exhibit stigmergic behaviour (Gregorio 2002). 'When one modifies the environment, the other replies to the new environment and modifies it and so on' (Rupert et al. 2008, p. 136). Heylighen (2016b) regards stigmergy as 'a universal co-ordination mechanism' which remains poorly understood and underappreciated, with potential applications in web communities, robotics, and studies of human society. 'It enables complex coordinated activity without any need for planning, control, or communication, simultaneous presence or even mutual awareness' (Heylighen 2016b, p. 4). Phister (2011) finds clear evidence of this stigmergic behaviour in 'cyberspace', defined as 'a global domain within the information environment consisting of the interdependent network of information technology structures, including the internet, telecommunications networks, computer systems and embedded systems and control' (England 2008 cited in Mesic et al. 2010, p. 3). He concludes:

[T]he network as a whole has many unexpected large-scale properties involving its overall structure, the way in which it grows, how information propagates over its links, and the co-evolutionary relationships between the behaviour of search engines and the web's link structure, all of which lead to what could be called adaptive behavior of the system as a whole. (Phister 2011, p. 19)

In other words, the cyber domain – essentially, every non-biological manifestation of information technology – is, as Phister (2011) goes on to describe it, 'the ultimate complex adaptive system'.

Terrorism, information technology and the role of communication

Although it moves marginally beyond the boundaries of the thesis, this chapter will end by arguing that not alone are terrorism and information technology complex adaptive systems that co-evolve, but that both are also social systems as defined by German sociologist Niklas Luhmann. It is taking this route because, firstly, of the close parallels between complexity theory and Luhmann's particular brand of social theory (Emmeche 1997, pp. 43-46; Luhmann 1982a), not least the fact that both use autopoiesis (Maturana and Varela 1980) to explain how social systems perpetuate themselves, and, secondly, because uniquely in sociology, Luhmann (1997, 1995, 1990, 1987, 1986, 1982a) places communication and not human agency at the heart of social systems, reflecting the central position it also occupies in terrorism studies (Jenkins 2015; Nacos 2007, p. 14; Hoffman 2006, p. 198). It is also worth noting that while Luhmann explicitly promotes communication to the dominant position in the pantheon of systems, two of the other leading systems thinkers of the twentieth century, McLuhan and Beck, implicitly demote human agency as well. While it is not possible to deal with them in detail here, McLuhan takes the view that 'in operational and practical fact, the medium is the message' and that, in relative terms, content – what actors say – is irrelevant (McLuhan 1967, p. 15;), while Beck (2009, p. 15) argues that 'global terrorism', among other risks, arises unintentionally from the reflexive 'self-endangerment of modern Western society', where, if a threat were not posed by one group, society would generate it using another.

For Luhmann (1995, pp. 16-17) the key to systems theory analysis is the difference between a social system and its environment outside and around it. That enveloping environment is infinitely complex and chaotic, while the interior of the system itself is a zone of reduced

complexity. Communication within a system involves selecting a limited amount of information from outside the system and using this to reduce uncertainty internally. The criterion according to which that information is selected and processed is 'meaning'. For Luhmann, however, that meaning is not something generated or attributed by humans. Luhmann's framework describes social systems not as systems in which people are the fundamental components. Instead, he contends, the fundamental components of social systems are 'sense-making, meaning-processing communications' (Lenartowicz et al. 2016, p. 2), although those communications are, certainly, 'communications among *people*' (author's italics). This argument challenges the conventional wisdom on social systems today, which is that while they may indeed be complex and adaptive, they are not 'bearers of cognition'. A reversal of this view, contend Lenartowicz et al. (2016, pp. 1-2), 'is not only due, but also rational'. Such a reversal would posit social systems, or self-organizing systems of communication, as defined by Luhmann – which emerge through an evolutionary selection process strikingly similar to that of genetic algorithms (Holland 1992, p. 24; 1975, pp. 89-140) – as 'proper, non-metaphorical, holders of cognition', while acknowledging, counterintuitively in terms of traditional sociology, that human beings are not, and never were, at the heart of society:

A communication happens as a difference-making selection, or more precisely: 'a synthesis of three different selections, namely the selection of *information*, the selection of the *utterance* [*mitteilung*] of this information, and the selective *understanding* or *misunderstanding* of this utterance and its information' (Luhmann 2002, p. 157) ... Only if all three selections take place a process called 'communication' occurs. (Lenartowicz, Weinbaum and Braathen 2016, p. 17, italics in original)

As Roth (2011, p. 30) puts it: 'The hero of 21st century sociology is communication'.

Conclusion

It has long been contended that both technology and media act as force multipliers for terrorism (White 2012, pp. 135-136, 146-148). How does this happen? The proposition at the heart of this thesis is that as complex adaptive systems, terrorism and information technology co-evolve to their mutual benefit rather than simply evolving along parallel, linear, paths. It argues that as co-evolving complex adaptive systems, especially where the information technology represents a new iteration generated by a phase transition aimed at self-

optimization (Langton 1990), that multiplier effect is given additional propulsive power. But while complexity theory, and co-evolution specifically, provides a much more logically compelling twenty-first century explanation than has hitherto been available for how terrorism and information technology develop 'a symbiotic relationship' (Wilkinson 2006, p. 145), it does not provide an explanation which similarly underpins the pervasive view in the discipline that terrorism is fundamentally all about communication (Nacos 2007, p. 14; Hoffman 2006, p. 198; Jenkins 2015). Looking at the co-evolution of terrorism and information technology from the viewpoint of Luhmannian systems theory, however, yields confirmation of that missing link: the primacy of communication.

For Luhmann, the function of the terrorist is solely to act as catalyst, while the leading actor is communication, the age-old message of 'violence and the fear of it' (Hoffman 2002, p. 313) expressed in the action of the terrorist attack. From the point of view of autopoiesis, which expresses 'a fundamental dialectic between structure and function', this 'sense-making, meaning-processing' communication (Lenartowicz et al. 2016, p. 2) is fulfilling its role as a bearer of cognition and perpetuating itself by doing so. Already driven by the compulsion to co-evolve, here, in Luhmann's terms, lies terrorists' 'imperative to act' (Hoffman 1999, p. 35). So not alone can the view that terrorism and information technology 'evolve' (Jenkins 1999, p. ix) and have 'a symbiotic relationship' (Wilkinson 2006, p. 145) be better explained by understanding how they co-evolve as complex adaptive systems, but their imperative to communicate is better explained by Luhmann's view that communication is the dominant social system and that terrorists are but one set of catalysts among many, all of them serving communication. As a consequence, while the medium, information technology, is undoubtedly the message and delineates through its architecture how terrorists will strike, terrorist messaging itself – whether they say this-and-that rather than that-and-this – is unimportant by comparison. This analysis of the processes at work in the interaction of terrorism and information technology is possible only by examining both as complex adaptive systems and leveraging their most influential element, co-evolution, the system key to their evolutionary trajectories.

CHAPTER THREE

Aligning methodology with complex ontology: Designing a template to investigate the co-evolution of networked terrorism and information technology

Introduction

The fundamental problem of linking human agency and social structure – the question of the degree to which one determines one’s own behaviour – ‘stalks through the history of sociological theory’ (Archer 2010 [1982], p. 225). For most of the twentieth century, social reality was investigated in terms of the structure and agency dichotomy (King 2010, p. 225). Archer’s morphogenetic approach (later renamed critical realism) and Giddens’ structuration were two of the most influential models. The morphogenetic approach (also known as analytical dualism) aimed to develop the distinctions between social structure and human agency in order to explore their interaction (King 2010, p. 254; Archer 1996). Structuration theory, on the other hand, sought to unite the functionalist and interactive traditions in a single theoretical framework that would explain social reproduction without detracting from the human factor (King 2010, p. 254; Giddens 1979, p. 71). Since the start of this millennium, however, a new approach has looked at social reality not in terms of structure and agency but in terms of networks (King 2010, p. 258), where the focus is entirely on the interactions within a system and ‘the detailed properties of each element on its own are simply ignored’ (Caldarelli and Catanzaro 2012, p. 4). It is that network-centric perspective that sits most comfortably with the modernising approach of this thesis. Such an impact has this perspective had that ‘a new consensus is apparent in sociology globally’ (King 2010, p. 258). Rather than the closed systems favoured by functionalist sociology, these are ‘open and indeterminate social webs which transcend national borders’. In that sense, the relationship between structure and agency is no longer one between an individual agent standing outside a ‘completed’ network. In a description that is strikingly reminiscent of the terminology of complexity, agents ‘should be understood collectively as joint participants in the network, recurrently and mutually constituting themselves through their interactions’ (King 2010, p. 258). As Archer (2010, p. 245) puts it in terms that would be fully at home within the

literature of complexity: ‘Emergence is embedded in interaction’.⁵⁷ This can also be seen as a description of co-evolution.

The new ‘network sociology’, as King (2010, p. 258) describes it, is typified, he suggests, by Latour (2005, p. 37), who sees social reality as ‘dynamic’ and the product of ‘often quite contingent “assemblages” of very wide social networks’, with, as he puts it colourfully, ‘no big reassuring pot of glue to keep all those ties together’. King also cites Castells (1998) and his extensive theory of social networks, and Collins (2004, 2000) and the ritual chain theory and actor network theory that form part of his sociology of philosophy. He might also have added Manuel De Landa, particularly ‘*A Thousand Years of Nonlinear History*’ (De Landa 2014) which traces non-linearity through geological, biological and linguistic time. For these sociologists, King says (2010, p. 259), the aim of the discipline is not to demonstrate how structure is reproduced or changed by an individual agent but to demonstrate ‘how distinctive forms of collective agency arise in particular milieus’. In the context of this thesis, one such example might be terrorism as a form of collective agency arising from the networks of interaction that will be described in each of the forthcoming case studies: Hezbollah, Al-Qaeda, and Islamic State. Indeed, King might well be writing about the emergence of post-Cold War terrorist networks when he observes that the ‘vertical’ paradigm of structure and agency dominant in the twentieth century might usefully be replaced in the twenty-first by ‘a horizontal perspective’ in which sociologists ‘think sideways’ and see social reality ‘in terms of multiple participants negotiating as they interact with, and co-operate or struggle with, each other’. To reflect this new networked reality, it is important to ‘align methodology to ... causal complexity’ (Blatter and Haverland 2014, p. 59). This thesis does that by using causal process tracing to uncover the multi-tiered causal mechanism at work when terrorists leverage new iterations of information technology (see next section). In line with Archer’s view, ‘any social ontology adopted has implications for the explanatory methodology endorsed’ (Zeuner 1999, p. 79).

⁵⁷ At the cutting edge of what is today known as ‘cognitive and computational neuroscience’, Seth (2021, 2021a) noted in a BBC interview that broadly speaking ‘perception is a process of perpetual updating,’ including of selfhood – which goes some way towards explaining the urge towards self-transcendence in art.

Given that complex ontology, this chapter will (i) underline the appropriateness of process tracing as a means of identifying the causal mechanism at the centre of this thesis, leveraging which terrorism and information technology interact and co-evolve; (ii) examine the variants of the methodology and show why causal process tracing sits most comfortably with the twenty-first century demands of complexity science; (iii) develop a series of Bayesian tests that can be applied consistently in each of the three case studies to establish whether the idea of co-evolution more satisfactorily explains the symbiotic relationship between terrorist networks and new iterations of information technology than previous explanations based simply on availability, chance, or even the idea of terrorists compulsively following a hardwired 'imperative to act' (Hoffman 1999, p. 35); and (iv) show how those tests will be operationalised by using intelligence community methods for gauging probability which link directly to the data (Irwin and Mandel 2020).

Process tracing and the route to causality

The term 'process tracing' has its origins in the cognitive psychology of the 1970s as a means of understanding the heuristics through which human beings make decisions (Bennett and Checkel 2015, p. 5). It was co-opted into political science by Alexander George (1979) to describe the use of evidence from within case studies to make inferences about explanations of historical events, such as why the Cold War ended peacefully, for example, or to attempt to uncover the causal mechanisms behind specific policy decisions (Tannenwald 2015, p. 220). This was a time – the 1960s and 1970s – when, as Della Porta (2008, p. 199) observes, the field of comparative politics 'boomed' as analysts began to acknowledge the 'accelerated interdependence of the world arena' (Lasswell 1968, p. 3), in other words, the complexity of the information-driven world in which they were living.

Process tracing is applied by 'working backward from the known outcome to uncover the causal mechanism that can *sufficiently* explain the outcome' (Beach and Pedersen 2012, p. 8). It involves 'following a set of rules of scientific inference whose purpose is attempting to infer beyond the immediate data to something broader that is not directly observed' (Della Porta 2008, p. 199). In slightly different manifestations, it is also known as 'historical analysis' or 'detailed case studies' (King et al. 1994, p. 86). Its methodological foundations are in Bayesian probability, the statistical method that originated with Thomas Bayes (Bellhouse 2004) which

assigns probabilities or distributions to events based on experience before experimentation, and then revises them in the light of the experimental data, allowing the development of causal inferences (Fairfield and Charman 2015, p. 1; Humphreys and Jacobs 2015, p. 9). Bennett and George (1997, p. 1) describe how the adoption of process tracing by political science was rooted in the need to offset the limitations of covariation – the correlated variation of two or more variables, which eighteenth-century philosopher David Hume termed ‘constant conjunction’ (Beauchamp and Rosenberg 1981, p. 4) – and covariation analysis, based on statistical methods as sources of causal inference. What are those limitations? Essentially, they are limitations exposed by the fact that, on their own, covariations are not evidence enough to conclude that X causes Y: ‘Underlying causes, no matter how numerous or deep-seated, do not make an event inevitable. Their consequences may depend on fortuitous co-incidences in timing or on the presence of catalysts that are independent of any of the underlying causes’ (Lebow 2000-2001, pp. 591-592).

Therefore, testing covariations involves estimating the causal effects of variables, in other words, the degree to which X does, in fact, cause Y (Bennett and George 1997, p. 1). This raises what Paul W. Holland (1986, p. 959) calls ‘the fundamental problem of causal inference’, which is that one can never know a causal effect for certain. The only way to be sure of the cause-effect relationship would be to re-run history (Bennett and George 1997, p. 1) or to stage the perfect experiment and compare it to what actually happened. However, this does not mean that causal inference is impossible. ‘What *is* impossible is causal inference without making untested assumptions’, Holland (1986, p. 959) argues. ‘This does not render causal inference impossible, but it does give it an air of uncertainty’. In that context, ‘tests of covariation are an avowedly imperfect alternative to perfect experiments’ (Bennett and George 1997, p. 1).

Reducing the uncertainty surrounding causal inference in case studies means generating and assessing evidence about causal mechanisms through process tracing, which has a number of theoretical equivalents such as ‘pattern-matching’ of variables in the conceptual and operational domains (Trochim 1985; Campbell 1966), for example, or the ‘modus operandi’ method (Scriven 1991, p. 234; Nyre and Rose 1979; Scriven 1974;) which seeks to uncover the ‘set of footprints’ which identify a cause as ‘effective’. It also means distinguishing between causal effects and causal mechanisms, though the two are inextricably linked and at the heart

of the concept of causality and its explanation. Bennett and George (1997, p. 4) make both the connection and the distinction clear. 'A variable cannot have a causal effect on an outcome unless there is an underlying causal mechanism', they point out, 'and it makes no sense to define any entity as a causal mechanism if it has no causal effect.'

This latter distinction, Bennet and George accept, would be 'a harmless debate of the chicken and egg variety' were it not for the fact that that the methodology one uses to 'unpack' the causal process depends on whether one is in pursuit of a causal effect or a causal mechanism. Different methods have different strengths and weaknesses when it comes to measuring one or the other. Large *N* statistical studies are typically strongest for attempting to measure causal effects, whereas when using case study methods, process tracing is a more effective means of identifying causal mechanisms, which is why it is particularly appropriate to this thesis. So, returning to Jackson's earlier distinction between whether one is examining the *effects* of technology adoption or the *process* through which that adoption occurs, 'tests of covariation attempt to address the former, and process tracing assesses the latter' (Bennett and George 1997, p. 5), as it does in this thesis.

With that confirmation of its suitability in mind, process tracing has three key elements, says Beach (2017, p. 2): (i) theorization about the causal mechanisms that link causes and outcomes; (ii) analysis of the observable manifestations of theorized mechanisms; and (iii) the complementary use of comparative methods to enable generalizations about findings from single case studies to other causally similar cases. But achieving this, he warns, involves more than 'the production of detailed, descriptive narratives of the events between the occurrence of a purported cause and an outcome' (2017, p. 2). Process tracing must examine the theoretical causal mechanisms linking causes and outcomes together, which is what this thesis does in examining the workings and implications of co-evolution:

The essence of making a mechanism-based claim is that we shift the analytical focus from causes and outcomes to the hypothesized process in-between them. That is, mechanisms are not causes, but are causal processes that are triggered by causes and that link them with outcomes in a productive relationship. (Beach 2017, p. 2)

Beyond this point, however, there is little agreement about the nature of mechanisms or how they should or can be measured, though there are striking parallels in meaning at various

points in the work of various leading theorists. It is not possible in this section to parse the entirety of the literature, so the aim in the next section is to follow some of the key ideas through the work of those scholars, with Beach (2017) as a consistent guide.

Process tracing: minimalist and systems understandings

Beyond the various definitions in the literature of what constitutes a causal mechanism and how it works, there are two distinct understandings of how such mechanisms should be analysed, says Beach (2017, p. 3). In the first, a minimalist understanding, 'the causal arrow between a cause and an outcome is not', as he puts it, 'unpacked in any detail, either empirically or theoretically'. Instead, there is a search for 'diagnostic evidence' (Bennett and Checkel 2015, p. 7), which is produced by asking, 'If causal mechanism, M, exists, what observables could it leave in a case?', a method strikingly similar to the search for mechanistic evidence in Russo and Williamson (2007). In the second, a systems understanding, the aim is the opposite: to unpack, explicitly, every element of the causal process, and to trace each of those parts individually. The aim is to 'dig deeper into how things work' in order to make stronger causal inferences about how causal processes actually play out in real life (Beach 2017, p. 4). In the minimalist understanding, therefore, there is less direct mechanistic evidence, and therefore inferences about the operation of a causal process are weaker.

Although he concedes that these two understandings have created 'confusion', Beach (2017, p. 6) takes the view that it is more helpful, perhaps, to regard them as two distinct varieties of process tracing because they are applicable in different research situations. The minimalist understanding can be used, for example, early in mechanism-focused research while still unsure about which mechanisms link causes and outcomes together. For most causal theories, he points out, there are multiple plausible mechanisms than can constitute that link, depending on context. King et al. (1994, p. 57) agree, observing: 'The political world is capable of producing multiple data sets for every problem'. This multiplicity phenomenon is known as 'causal equifinality' (Gerring 2005, p. 164), where 'several causes act independently of each other to produce, each on its own, a particular effect'. In this situation, it makes sense, says Beach, to use a minimalist approach, engaging first in what he describes as 'a form of process-tracing *plausibility probe* where mechanisms are not unpacked in any detail', in order to establish which mechanism links a given cause and effect, before moving on to examine the

inner workings of that mechanism. It is also possible, having engaged in a more thorough systems understanding of one or more cases, to then use a minimalist understanding to establish whether what was found in the intensively studied cases also holds in others of the population of what appear causally similar cases. As far as the systems understanding variety of process tracing is concerned, this can be used after an initial minimalist plausibility probe has indicated that a more intensive examination could be productive. In essence, the difference between the two is one of analytical depth:

In a minimalist understanding, we ask ourselves about what observables the operation of a mechanism has to leave in a case, and if found, whether there are any alternative explanations for finding them. In contrast, in the systems understanding, we ask ourselves about what observables would be left in a case by the data-generating process for the activities of entities for each part of the mechanism. (Beach 2017, p. 8)

Both minimalist and systems understandings of process tracing share certain assumptions, stresses Beach (2017, p. 6). One is that when examining mechanisms, ‘asymmetric’ claims are being made about the links between a cause and an outcome; asymmetric in the sense that no claims are made about what happens when a cause, mechanism, or outcome, is not present. This, he says, is important because it means one only has to define the ‘positive pole’ of cause and outcome and ‘the qualitative threshold at which the cause and outcome have causal properties in relation to a given mechanism’. Context is also important because – as already encountered with causal equifinality (Gerring 2005, p. 164) – ‘formally similar inputs, mediated by the same mechanisms, can lead to different outcomes if the contexts are not analytically equivalent’ (Falletti and Lynch 2009, p. 1160). It is interesting to note, too, that mechanisms, in either understanding, can be thought of as ‘a series of parts composed of entities engaging in activities’ (Beach and Pederson 2011, p. 8; Machamer 2004; Machamer et al. 2000). ‘Entities’, including human beings, are the parts of the mechanism that engage in ‘activities’, while those activities are ‘the producers of change, or what transmits causal forces through a mechanism’ (Beach and Pedersen 2011, p. 8). This is noteworthy for two reasons: Firstly, because the idea of mechanisms as a series of interacting parts whose interaction forces change through the mechanism depicts mechanisms themselves as complex adaptive systems. Secondly, it is reminiscent of Luhmann’s view, as set out earlier, that, as social systems, human beings engage in communication as catalysts, but it is ‘sense-

making, meaning-processing communications’ (Lenartowicz et al. 2016, p. 2) that generate change. Apart from their own inherent value to the internal logic of this thesis, such insights serve to underline the significance of Hall’s call for ‘aligning methodology to those aspects of causal complexity that are at the heart of many current theories in public policy and beyond’ (Blatter and Haverland 2014, p. 59).

Process tracing: assessing the causal evidence

Having looked at the two options for applying process tracing, how is the empirical evidence it generates assessed for its value in pursuit of causal inference? At the heart of Bayesian logic, says Beach (2017, p. 8), is the question of what the evaluation of different types of material can tell us about the ‘truth’ of causal theories. The Bayesian interpretation takes the view that some pieces of evidence are more powerful in yielding strong causal inferences than others. In the application of Bayesian logic to process tracing, the literature suggests focusing on two questions: first, whether one needs to find a particular piece of empirical material, in other words to achieve ‘certainty of evidence’; and second, if that material is found, whether there are any other plausible explanations for finding it. If not, the search has achieved ‘uniqueness of evidence’ (Beach 2017, p. 10; Rohlfing 2014). That challenge of assessing certainty and uniqueness applies to each piece of evidence. ‘Certainty and uniqueness are both matters of degree’, says Van Evera (1997, p. 31). ‘Predictions fall anywhere on a scale from zero to perfect on both dimensions.’ Examining those dimensions involves constructing a number of propositions that set out why each element of the putative mechanism would leave particular specified mechanistic evidence. It is important to be clear, says Beach (2017, p. 10), *where* that mechanistic evidence should be found, and why the data-generating process for that particular part of the mechanism should leave that specific evidence. It is also important to remember that the probative value of individual pieces of mechanistic evidence is typically quite low. However, if multiple pieces of evidence are independent of each other and all point in the same direction, their probative value can be taken together (Good 1991, pp. 89-90).⁵⁸ Logically, if two pieces of evidence are dependent on each other, finding both does not add to the sum of knowledge. This means that establishing the independence of

⁵⁸ Good’s example is of a coin, properly tossed ten times, giving the same face each time. Each toss has the same weight of evidence, but despite that, ten tosses increase the probability that the coin is double-headed.

individual pieces of evidence, and more broadly 'evidential diversity', is particularly important because 'collections of evidence that are "diverse" or "varied" should (*ceteris paribus*) confirm more strongly than collections of evidence that are "narrow" or "homogenous"' (Fitelson 2001, p. 48; Howson and Urbach 2006; Bennett 2014).

As to testing the plausibility of a hypothesis, there have traditionally been four main tests for causal inference in process tracing: straw-in-the-wind tests, hoop tests, smoking gun tests, and doubly decisive tests (Collier 2011, pp. 826-828; Van Evera 1997, pp. 30-34). Mahoney (2010, pp. 125-131) added a fifth, the auxiliary outcome test. These tests either indicate the veracity of a hypothesis to a greater/lesser, weaker/stronger degree or raise doubts about it. Straw-in-the-wind tests are the weakest of the four and 'place the least demand on the researcher's knowledge and assumptions' (Collier 2011, p. 826). However, they are useful in that they give an initial assessment of a hypothesis. So passing multiple straw-in-the-wind tests can be important affirmative evidence. Hoop tests are more demanding: they propose that a piece of evidence from within a case should be present for a hypothesis to be true, the idea being that the hypothesis must 'jump through a hoop' to avoid serious doubts about its validity. Failing a hoop test counts heavily against a hypothesis, so passing is important, though even passing is not enough to confirm a hypothesis (Mahoney 2015, p. 207-210). Passing a smoking-gun test provides a sufficient but not necessary criterion for accepting a causal inference (Collier 2011, p. 827). It can strongly support a hypothesis, but failure to pass does not rule it out, though it can 'substantially hurt' it (Mahoney 2015, p. 211). In addition, if a hypothesis passes, it substantially weakens rival hypotheses. Doubly decisive tests are the highest level of validation, both necessary and sufficient to confirm a hypothesis. Passing 'confirms one hypothesis and eliminates all others' (Collier 2011, p. 827), so that as Van Evera (1997, p. 32) observes: 'one test settles the matter'. Mahoney (2010, p. 129-131) poses an additional hurdle with his auxiliary outcome test. Auxiliary outcomes, he says, are not intervening variables connecting the cause to the putative effect, nor do they provide data about the existence of the cause. 'Rather they are *separate* occurrences that should be generated if the theory works in the posited fashion' (2010, p. 129). They can be regarded as additional and potentially helpful 'traces' or 'markers'.

Allowing typologies in the evaluation of evidence can also be useful, says Beach (2017, pp. 10-11). He lists four types of evidence: patterns, sequences, traces, and accounts. Patterns

refer to predicted statistical patterns in the empirical record. Sequences refer to the chronology of events predicted by the putative mechanism. Traces are pieces of evidence which constitute proof. Accounts deal with the content of empirical material. He cautions, however, that evidence is often very case-specific. That being so, 'to develop empirical fingerprints that are sensitive to the particulars of individual cases ... requires considerable case-specific knowledge and expertise' (Beach 2017, p. 11). In order to achieve maximum transparency, there is a view in the literature that degrees of prior confidence in the mechanism, as well as degrees of certainty and degrees of uniqueness should be quantified, set explicitly on the record using numbers or percentages. The argument against this is that it can lead to oversimplification of what are invariably complex interpretations of a variety of related evidence. Like Beach, who leans on the author's 'case-specific knowledge and expertise' to balance the need for quantification, Fairfield and Charman (2015, p. 32) observe: 'The most probative pieces of evidence are precisely those for which quantification is least likely to provide added value. The author can explain why the evidence is highly decisive without the need to invent numbers.'

Given that the context here is terrorism and counterterrorism – where imprecise or ambiguous estimates in decision-making may precipitate intelligence failure – there is, however, an alternative to 'inventing numbers'. That alternative is the NATO Allied Joint Doctrine for Intelligence Procedures (NATO-AJP-2.1) estimative probability standard used by the 30 NATO members and their external partners (Irwin and Mandel 2020, p. 18-2). This is a scale of probabilistic language that uses five verbal terms to describe five specific margins of probability covering the full range of the probability interval [0, 1], as follows: More than 90% (highly likely); 60% to 90% (likely); 40% to 60% (even chance); 10% to 40% (unlikely), and less than 10% (highly unlikely). Using this type of terminology adds a probabilistic dimension to process tracing and follows the general principles of Bayesian updating without creating a false impression of mathematical accuracy (Zaks 2021). The reality is that intelligence analysis and national security decision-making are 'pervaded by uncertainty' (Mandel and Irwin 2021, p. 558). Analysts using the NATO standard are discouraged from ever using the term 'confirmed' which is explicitly omitted 'given the nature of intelligence projecting forward in time' (Irwin and Mandel 2020, pp. 18-20).

Process tracing in a complex adaptive world

An earlier advocate than King of 'the network model of reality', Abbott (1988, p. 181) warned of the tendency among some theorists even then to construe the social world in terms of a 'general linear reality', treating social causality as if it were invariably subject to linear rules. That being so, the general linear model (GLM), as he characterised it, 'tests substantive models of social reality on the assumption that those models entail linear regularities in observed data' (Abbott 1988, p. 181), whether or not that is, in fact, the case:

They do this by assuming ... that the social world consists of fixed entities with variable attributes; that these attributes have only one causal meaning at a time; that this causal meaning does not depend on other attributes, on the past sequence of attributes, or on the context of other entities. (Abbott 1988, p. 181)

What Abbott (1988, p. 169) describes as this 'set of deep assumptions about how and why social events occur' yet again misses – as he implies – 'the significance of interactions' (Crenshaw 2010, p. 2) and allows for none of the 'ambiguity' typically associated with complex non-linear systems (Fellman et al. 2010, p. 6) and certainly with terrorism (Sorel 2003, pp. 366-367). It leads to 'a limited way of imagining the social process' and an 'unnecessarily narrow approach to causality' (Abbott 1988, p. 183). So how does one test a complex theory in a manner that prevents the very methodology being used to interrogate its core propositions from skewing not just the accuracy but the relevance of its outcomes? Citing Waltz (1979), a key characteristic of any theory, says Hall (2013, p. 2) is that it does not simply identify an empirical regularity, but adduces reasons why that empirical regularity should exist, and 'setting out those reasons usually entails outlining causal mechanisms associated with the phenomenon at hand'. That is precisely how this thesis progressed in the early stages of its development. The proposition that there might be a common mechanism at work in some terrorists' exploitation of information technology, especially in circumstances where the technology they were leveraging was new, led to the question of what elements might be essential for such a mechanism, and then to the putative answers to that question. Waltz (1979, p. 12) himself puts it: 'Theories indicate what is connected with what and how that connection is made. They convey a sense of how things work, of how they hang together, of what the structure of the realm of inquiry may be.' However, even a plausible theory, combined with the ancillary data that naturally accompany it, is not enough. 'Due process of

inquiry', exhorts Landau (1972, pp. 219-221), requires one to follow the logic and procedures of one's chosen methodology. In that sense, methodology must be more than 'merely a tactical matter' (Waltz 1979, p. 13).

Causal process tracing and the importance of time

In terms of how things 'hang together' in this thesis, it is important to identify and describe the specific variant of process tracing used in the development of this methodology. Without restating the rationale for the broad choice of process tracing as the optimum methodological match not just for within-case analysis but for the complex ontology with which this thesis engages, what is most important to underline here is the crucial role of time. Change can only be defined and studied over time. 'Temporality is central to causal inference and to the logic of historical explanation' (Grzymala-Busse 2011, p. 1268). Additionally, in his landmark analysis of organisational complexity, Dooley (2002, pp. 1-3) notes that all complex adaptive systems incorporate the dimension of time, something few previous organisational paradigms have done. This, he reasons, is because models using complexity theory typically go beyond 'the mere progression of activities and events' in pursuit of 'the generative mechanisms responsible for change', as indeed this thesis does. Thus, says Dooley, such complex models 'tend to have characteristics of both a variance theory, in that they conceptualize causal links between variables and/or constructs', and of a process theory, in that they 'make explicit how change over time occurs'. As a result, they 'answer both the "how" and "why" of organizational change', as, again, this thesis seeks to do. Because of that central position of time, causal process tracing (CPT) – a particular variety of process tracing which takes 'temporality' and 'configurational thinking' as its 'ontological and epistemological cornerstones' (Blatter and Haverland 2014, p. 1) – is 'the most important move in small-*N* studies' towards re-aligning methodology with ontologies that are fundamentally 'incompatible with the assumptions required by regression analysis' (Hall 2003, p. 399). On that basis, CPT is uniquely suited to tackling the propositions in relation to the complexity of both terrorism and information technology at the heart of this thesis.

In this setting of 'causal complexity', Blatter and Haverland (2014, pp. 10-12) specify the use of three types of causal-process observations: comprehensive storylines, smoking-gun observations, and confessions. In relation to the first, they argue that a small-*N* study such as

this thesis, based on causal process tracing, should provide ‘a comprehensive storyline’ in which the development of potentially relevant causal conditions is presented in narrative style. A major goal here is ‘to differentiate the major sequences of the overall process and identify the critical moments that further shape the process’. Secondly, they say the study should provide more detail into the causal processes that occur at those ‘critical moments’. Here the aim is to find evidence that provides a high degree of certainty that a causal factor, or a combination of causal factors, leads to the next step in the causal pathway or to the final outcome of interest. ‘In other words, we attempt to find smoking-gun observations embedded in a dense net of observations that show the temporal and spatial proximity of causes and effects.’ Thirdly, in order to gain deeper insights into important actors, the aim is to find ‘confessions’ that complement potential smoking-gun observations. In identifying such detail, the approach should be to ‘think like attorneys who have to convince juries, and not so much like statisticians’. An important aspect of confessions is that they reduce the problem of making causal inferences on the basis of temporal succession. This is because ‘actors can anticipate certain developments or actions and react to these anticipated developments in advance’. Public reflections by Brian Michael Jenkins, for example, on how he and the RAND researchers initially missed the significance of the internet while continuing to focus on weapons (Jenkins 2015a), and on how terrorism has changed counterterrorism in the sense that the two have co-evolved (Jenkins 2015b), are valuable insights providing important evidence of thinking at critical junctures.

Causal process tracing and configurational thinking

From the point of view of configurational thinking, too, the parallels with complexity theory are striking. Often found in management research, configurational thinking (Ragin 2008, pp. 109-146) looks at how organisational outcomes may be influenced by ‘alignment or conflict among interdependent attributes’ (Misangyi et al. 2017, p. 1; Siggelkow 2002). It starts from three notably non-linear propositions: (i) that social outcomes are the result of a combination of causal factors; (ii) that there are divergent pathways to similar outcomes, the idea of ‘causal equifinality’ (Gerring 2005, p.164) encountered earlier; and (iii) that the effects of the same causal factor can be different in different contexts and combinations, known as ‘causal heterogeneity’ (Western 1998). Within that eco-system, ‘causal configurations’, or

'causal chains' (sequential combinations of causal factors), may be 'situational' and therefore time-dependent, and, as a result, may be specified as 'causal conjunctions' (Blatter and Haverland 2014, p. 15), a term that may well fruitfully be applied to the point in this thesis where the co-evolution of terrorism and information technology is accelerated by the flowering of a new technological iteration. In this context, systems are regarded as 'constellations of interconnected elements' (Misangyi et al. 2017, p. 1) and an organisation as a 'multidimensional constellation of conceptually distinct characteristics that commonly occur together' (Mayer et al. 1993, p. 1175), a description that can readily be seen as applying to a complex terrorist network as unpacked by Hayden (2006, 2013), for example.

Causal process tracing also uses the idea of 'path dependency' (Pierson 2000, p. 259) to describe the positive feedback loops that maintain a process on a particular path despite evidence that an alternative trajectory might be preferable. Early events in that path dependency process are more decisive than later ones, but, broadly speaking, path dependency again points towards the importance of time, timing, and sequences' (Blatter and Haverland 2014, p. 4). CPT also uses the idea of 'critical junctures' (Soifer 2010), meaning combinations of 'permissive conditions' and 'productive conditions' that 'come together at a specific point in time and are individually necessary and jointly sufficient to produce change' (Blatter and Haverland 2014, p. 5). While permissive conditions 'weaken structural constraints', productive conditions 'determine the outcome that emerges from the critical juncture' (Soifer 2010, pp. 1574-1576). Again, Hayden (2013, p. 15), in her examination of the degree to which terrorist organisations can be described as complex adaptive systems, characterises their behaviour as driven by a series of positive and negative feedback loops, where a group's successes, its resources, and new learning that reinforces the culture that led to those successes are regarded as positive feedback, while failures, learning that challenges the dominant culture, and, ironically, innovation leading to change are seen as negative feedback. Given those tensions, at critical junctures, when change finally comes, the impact is often disproportionate to the elements that generated it. As noted in Chapter Two, small 'perturbations' can lead to 'massive changes' (Hayden 2013, p. 2).

Process tracing and case studies

Within a research design, a case study, is, in effect 'your unit of analysis' (Miles and Huberman 1994, pp. 25-27). There is, however, no consistency in the way case studies are chosen, a fact that has caused 'no little consternation' in the academy (Gerring 2007, p. 231; Levy 2002; Collier and Mahoney 1996; Achen and Snidal 1989; Lijphart 1971, 1975). Smelser (1976, p. 174) suggests five criteria for case selection. They should be (i) appropriate to the kind of theoretical problem posed by the investigator; (ii) relevant to the phenomenon being studied; (iii) 'empirically invariant' with regard to the criteria for their classification; (iv) a reflection of the available data, and (v) selected on the basis of 'standardized and repeatable procedures'. Eckstein (1975, p. 157) adds another option: the 'crucial' case 'that *must closely fit* a theory if one is to have confidence in the theory's validity, or, conversely, *must not fit* equally well any rule contrary to that proposed'. Gerring (2007, p. 231) interprets this as meaning: 'A case is crucial if the facts of that case are central to the confirmation or disconfirmation of a theory.' Both King et al. (1994, pp. 209-212) and Gerring (2007, p. 249) ultimately take the view that while a single case can provide useful evidence for or against a general causal proposition, few theoretical arguments of interest rest solely on one case unless 'the argument is anodyne enough to obviate the collection of additional evidence'. This, Gerring says, however, points to a broader conclusion: that 'case studies are best viewed in conjunction with cross-case studies', as is the case in this thesis. The three case studies against which this thesis is tested are Hezbollah and its exploitation of satellite television, Al-Qaeda and its adoption of the internet, and Islamic State and its embrace of social media. Together, they cover a period of more than 20 years, during which both terrorism and the information technology used by terrorist groups changed dramatically. With the argument already made that both terrorism and information technology can reasonably be described as complex adaptive systems, and with Smelser's guidelines for the selection of case studies in mind, that timeline is worth exploring briefly for any indicative traces or patterns in what may be seen as informal minimalist understandings.

Hezbollah and satellite technology

The first case is Hezbollah, Lebanon's Shia militia formed in 1985 in response to Israel's invasion and occupation of south Lebanon (Norton 2018; Levitt 2013; Addis and Blanchard 2011; Conway 2008a, 2007, 2005, 2003a; Kramer 1990). It established its terrestrial television

channel, Al-Manar, on June 4, 1991, began satellite broadcasting in May 2000 and merged the two services in 2014 (Media Ownership Lebanon N/D). The aim of its propaganda machine was to establish Hezbollah and its followers in the international mind as freedom fighters rather than terrorists, despite, or perhaps because of, their designation as a terrorist organisation by the United States in 1995.⁵⁹ In terms of the technology, the first satellite TV signals had been relayed across the Atlantic on July 23, 1962, a landmark event about which McLuhan (1967, p. 63) wrote five years later: “Time” has ceased, “space” has vanished. We now live in a “global village”.’ Like the RAND terrorism researchers in 1972, McLuhan’s only shortcoming was his inability to anticipate that the speed of technological change, rapid though it already was, would continue to accelerate. ‘Information pours upon us, instantaneously and continuously’, he wrote. ‘As soon as information is acquired, it is very rapidly replaced by still newer information.’ Indeed, such was the pace that by the mid-1980s, the same satellite technology was allowing CNN International to broadcast to hundreds of millions of viewers in more than 200 countries (Culf 1996). Its founder, Ted Turner, would soon describe his global news service in geopolitical terms as ‘one of the straws that broke the camel’s back’ by shining a light on Soviet oppression and helping to bring a peaceful end to the Cold War (De Moraes 1998). In that context, the Hezbollah case study in Chapter Four will look in detail at the new scale (McLuhan 1967, p. 15) satellite broadcasting injected into the organisation by (i) turning a predominantly local and, at best, regional, presence rapidly global, and (ii) giving it an invaluable psychological edge in its 2006 war against Israel by enabling it to beam ‘actual battlefield footage showing Israeli soldiers being killed and maimed’ into homes from Tel Aviv to Jerusalem (Clarke 2017). For now, however, it is enough to note that in August 2010 an analysis for the Obama White House described Hezbollah as ‘the most technically capable terrorist group in the world’ (Addis and Blanchard 2011, p. 4), with links across the Middle East, West and Central Africa, Latin America, and North America. Its adoption of fledgling satellite TV was *a critical juncture*.

Al-Qaeda and the internet

⁵⁹ As of October 2020, Hezbollah or its military wing were considered terrorist organisations by at least 25 countries, including the US, the European Union *en bloc*, and the majority of the states of the Arab League.

The second case study examines Al-Qaeda and its adoption of the internet both in the run-up to 9/11 when it was used extensively and invisibly for ‘cyberplanning’ (Thomas 2003) and immediately afterwards when the Al-Qaeda leadership fled Afghanistan for Pakistan and used the inaccessible tribal areas as a ‘virtual sanctuary’ (Ranstorp 2006) to reconstitute the organisation online as diffuse and leaderless. This bifurcation, in fact, is a feature of all three case studies which is emerging gradually in this thesis: in the early stages of co-evolution the terrorists identify a new iteration of information technology and become early and innovative adopters, which, typically, gives them the benefit of increased ‘power and network centrality’ (Burkhardt and Brass 1990, p. 104). Following a quantum of interaction, however, the balance of influence becomes reversed and the terrorist organisation begins to reflect the structural architecture of the technology it has taken on. In the case of Hezbollah and satellite broadcasting, Hezbollah, in effect, became an international terrorist organisation once it had the capacity to amplify its threat to that level via satellite and was consequently classified as such by the US. In the case of Al-Qaeda and the internet, the change in behaviour before and after 9/11, as just described, is more striking. Most striking of all, however, is the case of Islamic State and social media, where the jihadists leveraged Twitter to its upmost in the months before their capture of the northern Iraqi city of Mosul to project an image of monstrous barbarity and invincibility which led the Iraqi army to flee before them. Having declared the caliphate established, the second phase of its offensive began, a blizzard of attacks in Europe carried out by individuals with little structured connection to the organisation but empowered by the architecture of social media – which allows users to influence the direction of the technology – to take independent action and thus influence the direction of the organisation as a whole. Because of that ad hoc influence, it is clear that those attacks were not planned as a series but developed organically. Before the internet, the American historian Elizabeth Eisenstein (1979, p. 11), in her landmark survey of the impact of the printing press on the socio-cultural systems of early-modern Europe, concluded that it was ‘the primary agent of change’ (Elwell 2020),⁶⁰ suggesting that before the invention of printing, learning relied on the spoken word, ‘producing a hybrid half-oral half-literate culture

⁶⁰ In terms of McLuhan’s question of scale (1967, p. 15), by identifying the printing press as the primary agent of change behind the turmoil and innovation of the sixteenth century, Eisenstein (1979), in effect, ranks its impact ahead of the discovery of the New World, the class struggle and the triumph of capitalism, the scientific revolution, and the Great Schism of Christianity (Elwell 2020).

that has no precise counterpart today'. She also maintained that because it involved both the storage and dissemination of information and data, communications technology was 'a great intensifier of the evolutionary process' (Elwell 2020). Like McLuhan in 1967 and the RAND researchers in 1972, Eisenstein's prescience was only limited by the technology of the times. It is arguable, however – particularly on the basis of co-evolution and 'the deep interconnectedness of the technological and the social' (Axtell 2004, p. 2) – that the invention of the internet has produced, to paraphrase Eisenstein, a hybrid half-literate half-technological culture that will have no precise counterpart until, most likely, technological autonomy becomes a reality with the widespread application of the Internet of Things (Elkhodr et al. 2016; Tucker 2016; Ashton 2009), still only in its infancy. There are many striking descriptions of the internet in this thesis that give an insight into the new scale it brought to information technology (McLuhan 1967, p. 15), among them that it has been 'perhaps the most transformative invention since Gutenberg' (Healey 2014), opening a vista of evolution right back to Eisenstein's late Middle Ages. Al-Qaeda's early adoption of the internet gave it access to an 'information infrastructure' without borders (Leiner et al. 1997) which empowered its international network of followers and gave it global reach (UNODC 2012, p. 2). It was, in retrospect, says Jenkins (2015) 'the most profound development' in terrorists' already-lethal arsenal. It was *a critical juncture*. The Al-Qaeda case study in Chapter Five will examine that co-evolutionary relationship in much greater detail in the context of 9/11. For now, however, it is enough to note that:

The enormity and sheer scale of the simultaneous suicide attacks on September 11 eclipsed anything previously seen in terrorism. Among the most significant characteristics of the operation were its ambitious scope and dimensions; impressive coordination and synchronization; and the unswerving dedication and determination of the 19 aircraft hijackers who willingly and wantonly killed themselves, the passengers and crews of the four aircraft they commandeered, and the approximately 3,000 persons working at or visiting the World Trade Center and the Pentagon. Indeed, in lethality terms alone, the September 11 attacks are without precedent.' (Hoffman 2002, pp. 303-304)

Islamic State and social media

The third case study examines Islamic State's rapid adoption of social media in the period leading up to its capture of Mosul at the high point of its insurgency in Iraq on June 10, 2014, (Hassan 2017) and continuing through the series of assaults in Europe until the Barcelona

attacks on August 17 and 18, 2017, in which 16 civilians were killed and 152 were injured (Iguarada 2021; Bourekba 2018; Tremlett et al. 2017). Islamic State was established in 1999 by Jordanian jihadist Abu Mus'ab al-Zarqawi (Stern and Berger 2015, pp. 13-26), as Jama'at al-Tawhid wal-Jihad, becoming known as Al-Qaeda in Iraq (AQI) when he pledged allegiance to Osama bin Laden in 2004. The Syrian civil war that broke out in 2011 caused strategic tensions between the new organisation and Al-Qaeda's leadership and the two severed their ties in February 2014 (Byman 2015) in a hostile and very public 'divorce' (Hoffman and Ware 2019). Bin Laden was the first terrorist leader to embrace internet technology as early as 1997, understanding that 'rhetoric and satellite propaganda can be on equal footing with unmanned bombers and cruise missiles' (Kepel 2004, p. 119). His successor, Ayman al-Zawahiri, likewise declared, 'We are in a battle, and more than half of this battle is taking place in the battlefield of the media' (Lynch 2006, p. 50). That culture remained as pivotal in al-Zarqawi's Islamic State, though there was an important difference in approach. While Al-Qaeda and its affiliates saw the internet as a place to disseminate information covertly and meet anonymously, Islamic State supporters were 'loud and noisy, tweeting, streaming and Instagramming their exploits', said Liang (2015, p. 2), exploiting its psychological impact for all it was worth. So, as Islamic State fighters swept across northern Iraq towards the ancient city of Mosul, combining their twenty-first century social media offensive with mediaeval beheadings and crucifixions for unprecedented shock effect, she added, 'Terror is now being transmitted across the globe in real time.' It was in this context that, as Islamic State marched into Mosul, its triumphant arrival was marked by almost 40,000 followers' tweets in a single day, leading Berger (2014) to observe, 'The advance of an army used to be marked by war drums. Now it's marked by volleys of tweets.' In 2015, before its caliphate was dismantled, it was estimated to have a force of some 30,000 fighters and a war chest of around US\$1 billion (Gerges 2016, pp. 21-22). Its adoption of social media was *a critical juncture* in the generation of that new scale and the force multiplier effect that it enabled. In retrospect, what was new about social media in a terrorism context was that it 'empowered extremist movements and terrorist groups to network and organize online, making it far easier for them both to recruit newcomers and to direct and inspire attacks' (Hoffman and Ware 2020). More than that, as evidenced by its lone-actor and small group attacks across Europe, its organisational structure allowed followers to influence the direction of the group itself by taking strategy into their own hands in an unprecedented manner. The Islamic State case study in Chapter Six will

revisit these issues. For now, Singer and Brooking (2018, p. 219) put it tellingly: ‘There’s no historical analogue to the speed and totality with which social media platforms have conquered the planet.’

The order of the case studies

The order in which the three case studies are examined is crucial to the narrative they uncover. On the face of it, there are arguments for a number of approaches. For instance, simply taking the terrorist groups in order of their chronological emergence suggests Hezbollah, Al-Qaeda, and Islamic State, and there are certainly interesting threads to be traced through the evolution of their individual variations of jihadism. On the other hand, the fact that all three groups continue to exist and function might suggest that they be taken instead in order of their terrorist impact. This would certainly position Al-Qaeda first given that 9/11 was the most lethal attack in the history of terrorism. This placement is also interesting given that of the three new iterations of information technology leveraged by the groups, the emergence of the internet was, and remains, undoubtedly the single most significant. It is not adequate, of course, to take the view that there are a number of equally plausible options. What is required is a galvanizing argument that leaves no doubt about the logic of the order. Given that the focus of this thesis is the idea of a co-evolutionary mechanism which can be shown to have applied in each of the three cases over a period of more than 20 years, and whose influence will remain compelling into the future, it seems more productive to examine the evolutionary trajectory of the information technology involved. This reveals a clear developmental pathway from satellite technology to the internet to social media. It began with a US Department of Defence Cold War project named ARPANET (Advanced Research Projects Agency Network), whose aim was to find a way of linking computers by satellite so that critical communication could be maintained in the event of a nuclear war (Hauben 1994). That project – and particularly Polish-American engineer Paul Baran (Metz 2012) – developed and pioneered ‘packet switching’ in 1969, a method of grouping data into chunks before it was transmitted digitally. Many of the protocols used by computer networks today were developed for ARPANET, which is considered the forerunner of the modern internet (Wright 2021). On January 1, 1983, a new communications protocol,

TCP/IP,⁶¹ enabled revolutionary new levels of interoperability, so that all computer networks could now be connected by a universal language. Social media, in turn, are ‘a group of internet-based applications that build on the ideological and technological foundations of Web 2.0 and that allow the creation and exchange of user-generated content’ (Kaplan and Haenlein 2010, p. 61). Increasing interoperability is leading to increasing scale. On that basis, the order of the case studies must follow those evolutionary and co-evolutionary trajectories: (i) Hezbollah and satellite broadcasting, (ii) Al-Qaeda and the internet, (iii) Islamic State and social media.

The data sources

As reflected in the bibliography, this thesis uses predominantly qualitative data originating from the two distinct disciplines it brings together: terrorism studies and complexity theory. Both are disciplines with foundations that draw on large, well-established reserves of foundational quantitative research combined with parallel qualitative analysis that ‘aids in contextualizing the material that is developed’ (Ross 2004, p. 26) and, in so doing, provides the all-important link between the ‘what’ and the ‘why’ of social phenomena (Ahmad et al. 2019, p. 2828) that is at the heart of this thesis. In that sense, much of the qualitative data drawn upon here is grounded in the quantitative. In the case of terrorism studies, this foundational quantitative data is contained in the multiple databases established since the RAND analysis of modern terrorism began in the 1970s (Jenkins 1999. p. iv; Fowler 1980). The RAND Database of Worldwide Terrorism Incidents (RDWTI)⁶² stretches back to 1968, with some 40,000 incidents coded up to 2009. The Global Terrorism Database⁶³ at the University of Maryland includes more than 200,000 attacks from 1970 to today and is the most comprehensive unclassified database of terrorist attacks in the world, focusing on tactics and operations. The BAAD (Big, Allied And Dangerous) Database is curated by the University of Albany’s Rockefeller College of Public Affairs and Policy and includes intelligence on organisational structure and history (Hayden 2013, p. 18). Bowie (2021) provides a

⁶¹ Transfer Control Protocol/Internetnetwork Protocol: prior to this, different computer networks did not have a standard means of communication (Davidson 1988).

⁶² RDWTI is at <https://www.rand.org/nsrd/projects/terrorism-incidents.html>

⁶³ Global Terrorism Database: <https://www.start.umd.edu/gtd/>

comprehensive list of 40 more specialised terrorism databases and data sets, many of which offer open access.

Quantitative data on terrorism is not confined to databases. In the case of 9/11, the deadliest terrorist attack on American soil, the commission set up to investigate the attack produced a 600-page report based on the entirety of the quantitative data available to US state agencies. That included primary data from airport security, airline flight paths, air traffic control recordings⁶⁴ and eyewitness accounts of events on board the jets, and secondary data in the form of the qualitative analysis that led to its conclusions. While this information is not directly relevant to Al-Qaeda's adoption of the internet, it does give considerable insight into its organisational structure, system behaviour, and operational priorities (*The 9/11 Commission Report 2004*). Similarly, in the case of Hezbollah, US government reports such as *Hezbollah: Background and Issues for Congress* (Addis and Blanchard 2011) based advice for policymakers on quantitative data wherever possible, as well as on expert qualitative analysis of that data. In the case of Islamic State and social media, much had already been written about the rapid acceleration of the new media, including statistics to illustrate its unprecedented spread by the time it was adopted by the jihadists (Morgan et al. 2012; Weimann 2015) and their networks (Parekh et al. 2018).

In the case of qualitative data in terrorism studies, this is typically comprised, says Ross (2004, p. 26) of 'descriptive accounts of terrorists, their actions, and measures to combat these actions'. These, of course, are also used here. Given the dramatic nature of terrorist attacks, media reports are also an important source of data. While journalism is almost always produced under time pressure and is therefore not always reliable, 'the quality and reliability of information usually increases with time' (Nesser 2004, p. 16). It is also true that, seen as 'the first rough draft of history' (Barth 1943), media coverage of regions such as the Middle East, where access is frequently difficult or dangerous, is often one of very few sources of information. It is common for such information to begin as journalism before being subsumed into academic research. Investigative reporting is increasingly rare but invaluable (Hersh

⁶⁴ These air traffic control recordings are freely available on YouTube: https://www.youtube.com/watch?v=-60jRZCiM_s

2018). A good example of forensic attention to detail is the *Der Spiegel* team's minute-by-minute recreation of 9/11 (Der Spiegel 2001), widely cited by Hoffman (2002). 'A symbiotic relationship exists between popular and academic writers; at various times they depend upon or use research from each other.' (Ross 2004, p. 26) In such circumstances, informal triangulation of data (Carter et al. 2014; Patton 1999) and cross-referencing are natural precautions that go to the root of credibility (Patton 1999, p. 1190), even in journalism. Having been a working journalist in the region, including Beirut and south Lebanon on several occasions, and having interviewed Hezbollah figures arguably gives this thesis rare additional on-the-ground familiarity.

In the case of complexity theory, foundational quantitative data take the form of cutting-edge scientific research into the non-linear nature of systems and networks based on rigorous mathematical proofs modelled using high-powered computers (Holland 2006b, 2006a, 2003, 2002, 1999; Gell-Mann 2002, 1994, 1988; Kaufmann 1993, 1992, 1991b, 1991a), particularly since the establishment of the multi-disciplinary Santa Fe Institute in 1984. Much of that data has flowed from the mould-breaking implications of early research in quantum physics (Cresser 2011). Using that data, the key concepts of complexity theory are identified here, allowing the central propositions of this thesis – (i) that terrorism and information technology may reasonably be described as complex adaptive systems, (ii) that a core characteristic of such systems is that they co-evolve with others in their environment that they judge may be beneficial, and (iii) that this is the most satisfactory explanation for the 'symbiotic' relationship between terrorism and information technology, particularly when the information technology is undergoing structural change to a new iteration allowing increased scale and interoperability – to be examined in the context of each of the three case studies using the tests outlined above.

There is, however, an important additional dimension to the research data collated here. That added dimension relates to the strategic switch of perspective at the heart of this thesis away from the old linear view of terrorism and its relationship with the media to a new interpretation of that relationship as mediated by complexity theory and driven by the imperatives inherent in competitive co-evolution between terrorism and information technology. What that reveals is that while the data used here may once have told a linear story, this new interpretation of the same data reveals an altogether different more complex

set of processes at work, as befits our understanding of science and social science in the twenty-first century. In that sense, the methodology used here has rendered it not just new data, but new data with increased ‘causal potency’ (Hogg 2018).

Testing causal inference across the case studies

‘We are inveterate searchers after causes’ (Brady 2011, p. 1). However, ‘every claim invoking causal concepts must rely on some premises that invoke such concepts; it cannot be inferred from, or even defined in terms of, statistical associations alone’, writes Pearl (2010, p. 2), a champion of Bayesian networks in the development of artificial intelligence (Pearl 1988; Pearl and Russell 2002).⁶⁵ In addition, he says, causal analysis ‘goes one step further’ than standard statistical analysis in that ‘its aim is to infer probabilities under conditions that are *changing*’. In the case of this thesis, the overarching premises required by Pearl are that (i) the intellectual foundations of knowledge have changed with the transition from reductionist, linear thinking to non-linear thinking (De Landa 2014); (ii) as a result, a whole series of new concepts is being applied across a plethora of knowledge silos, revealing deeply embedded connections not previously realized; (iii) this new vista has been scientifically underpinned by the unprecedented power and sophistication of computer-based mathematical modelling, and (iv) as a consequence, the twenty-first century scientific understanding of ‘the world’ is that it is a series of interacting biopolitical networks, multi-tiered, emergent and unpredictable, as complex crises such as the covid-19 pandemic and climate change demonstrate. On the other hand, a harmonising effect of non-linear thinking and the development of complexity science is frequently that ‘previously partitioned disciplines and enterprises find themselves collaborating, not competing’ (Negroponte 1996, p. 230). These are the premises that underlie this entire thesis, and from which co-evolution as a structural answer to the question posed by the symbiotic relationship between terrorism and the media emerges. In that context, Pearl’s second point that causal analysis aims to infer probabilities under conditions that are changing again underpins its appropriateness for tackling complex issues.

⁶⁵ Judea Pearl, a winner of the Turing Award among others, is an Israeli-American expert in artificial intelligence and Bayesian networks. His son, Daniel Pearl, a journalist on *The Wall Street Journal*, was beheaded by Al-Qaeda in Pakistan in 2002 (Mount 2007).

Having reviewed the three case studies briefly, it is essential to design and apply a research methodology that identifies and separates the main theoretical strands of this thesis, allowing them to be examined and traced individually, before showing how they intertwine (Gell-Mann 2002, p. 17) and co-evolve.⁶⁶ The internal logic of describing that process and how it changes over time will demonstrate that co-evolution provides a more theoretically satisfactory explanation of how and why terrorism and information technology interact symbiotically than is possible by examining the ‘working relationship’ between terrorists and journalists, for example, previously thought to have been one possible locus of that symbiosis. In doing so, it will also identify the critical junctures in the co-evolutionary dynamic as it unfolds. In order to uncover the mechanism this process describes, it is necessary to apply four tests to each of the case studies to ensure consistency of investigation across the three. The results will also allow cross-case comparisons, as recommended by Gerring (2007, p. 249), allowing similarities and differences to be traced over time, and allowing attention to be paid to previously undetected nuance that may perhaps have disproportionate effect. While Chapter Two has already made the case that both terrorism and information technology may reasonably be described as complex adaptive systems, it also notes that even groups that may *sometimes* be described as such may not *always* be so described. Sometimes they meet the high bar, other times not. Therefore, evidence of networking, of productive interaction, and of co-evolutionary behaviour will be tracked in each case. Each case study will be updated in Bayesian manner from ‘traditional’ (linear) interpretation to ‘complex’ (non-linear) interpretation. To operationalise this assessment, the NATO probability standard will be applied.

The Bayesian tests

Test 1 will look at each terrorist group in sharp focus, describe its roots and history, and ask what its organisational structure, its links to its *ummah*, its behaviour in conflict, its ability to learn and innovate, and the relationship between its leadership and its followers confirm, disprove, or throw into doubt about its behaviour as a complex adaptive system (Hayden

⁶⁶ ‘Which strata should be separated from others’, asks Foucault (1977, pp. 3-4) when he notes that in historical analysis, ‘linear successions’ have been replaced by ‘discoveries in depth’, each with ‘its own peculiar discontinuities and patterns’.

2013, 2006; Goolsby 2006; Fellman 2010; Fellman and Post 2010; Hoffman 2006a, 2006b, 2003, 2002). It is essential to find: (i) a networked organisational structure that is central to its development; (ii) convincing traces of CAS behaviour.

Test 2 will examine each organisation's pursuit of 'autonomous communication' using information technology. It will look at the technology it adopted, how and why it used it, at what point in the lifecycle of the technology it was selected as potentially beneficial, and how the organisation and the technology interacted in a symbiotic manner that demonstrated a mutually beneficial imperative to co-evolve (Jenkins 2015; Liang 2015; Ingram 2017; Conway 2005; Ilachinski 2005). It is essential to find: (i) a new iteration of information technology which has just emerged through structural change/phase transition; (ii) convincing traces of co-evolutionary behaviour.

Test 3 will look at the information technology as a force multiplier that generates 'new scale' by amplifying the messaging of its terrorist partners and allowing them greater autonomy of communication. It will ask whether that force multiplier effect reflects the greater interoperability achieved when a new iteration of information technology succeeds a less pervasive one (Brachman 2006; Emery, Earl and Buettner 2004; McLuhan 1967). It is essential to find: (i) evidence of the new scale generated; (ii) convincing traces of greater technological interoperability.

Test 4 will ask whether – working backwards from the known outcome (Beach and Pedersen 2012, p. 8) – the causal mechanism described by the interaction of the terrorist network and the information technology in the three previous tests provides a more appropriate explanation for their interaction than has hitherto been available in the literature of terrorism studies (Nacos et al. 2011; Nacos 2007, 2006, 1994; Wilkinson 2006; Jenkins 1999). If that putative mechanism has high causal credibility using the NATO standard at the end of each case study and across the three, then it is reasonable to suggest that it (i) sufficiently explains (Beach and Pedersen 2012, p. 8) the interaction of terrorism and information technology in terms of co-evolution between two complex adaptive systems; (ii) allows inference beyond the immediate data to something broader that is not directly observed (Della Porta 2008, p. 1999), in this case an enduring co-evolutionary relationship between terrorism and

information technology, reflecting ‘the deep interconnectedness of the technological and the social’ described by Axtell (2004, p. 2).

Conclusion

To reach its full potential, each new iteration of information technology must ‘break down the silos’ that limit its impact, particularly those that hinder its interoperability⁶⁷ (Elkhodr et al. 2016) as the underlying information-driven architecture evolves (Roca et al. 2016). It is the capacity of complex adaptive systems to send ‘exogenous shocks’ (Barley 1986, p. 80) through that architecture – which, interestingly, Lala and Kumar (2003) propose should be modelled on the complexity of the human immune system in order to absorb shock in the form of error more efficiently – that leads to cascades of change in related systems, frequently out of proportion to the transformative power of the original catalyst (Knorr-Cetina 2005). This thesis proposes that in each of the three cases under examination that catalyst is the propulsive power generated by the co-evolution of terrorism and information technology, particularly when combined with the untapped ‘vitality’ (Bishwas 2011) of a new technological iteration on the cusp of replacing its predecessor in a process of ‘creative destruction’ (Perez 1983, p. 3). Causal process tracing (Blatter and Haverland 2014) as the methodology chosen to test that complex proposition incorporates the ability to design not alone change but change over time, which is crucial since change can only be studied over time, and time is central to the contention that the same causal mechanism is at work in each of the three case studies. The four-test design used here allows the emergence of a multi-dimensional model in each case, revealing (i) the pattern of evolution inherent in the disaggregation of the technology (McShea 1996); (ii) the impact of the co-evolutionary dynamic as it affects both co-evolving systems (Yip et al. 2008), and (iii) the architectural progression from one iteration to another – satellite to internet to social media – in terms of the path to greater interoperability and the additional scale (McLuhan 1967) that this interoperability affords its users. The result is a holistic rather than a reductionist view of terrorism that accurately reflects its identity as a complex adaptive system which is constantly changing (Ahmed et al. 2008, p. 2). As Hoffman (2006, p. 295) observes: ‘Countering terrorism

⁶⁷ Interoperability, as Ferrer (2009) succinctly describes it in the title of her paper, means ‘making information systems work together’.

is akin to taking a series of time-lapse photographs. The image captured on film today is not the same as the image yesterday, nor will it be the same tomorrow.’⁶⁸ The design of this methodology reflects that complex reality.

⁶⁸ Hoffman is paraphrasing French terrorism expert Xavier Raufer, April 2003. See note 113 in Hoffman 2006, p. 368.

CHAPTER FOUR

Deadly Embrace 1 – Hezbollah and satellite broadcasting as co-evolutionary partners in a mutually beneficial trajectory towards greater scale and interoperability

Introduction

In order to examine and understand continuity, it is crucial to understand what is going on at the point of change, and how that point of change is related to further change (Williams and Dyer 2017, p. 3). That involves ‘theorising a system (or mechanism) that will provide an explanation’, and where some form of measurement of that mechanism is possible, especially in complex systems. This thesis proposes just such continuity between the three case studies that follow: Hezbollah and its leveraging of digital satellite broadcasting just prior to the turn of the millennium; Al-Qaeda and its covert exploitation of the internet as the revolutionary new technology emerged in the years preceding 9/11, and Islamic State and its dramatic and very public adoption of internet-based social media, which gathered momentum rapidly from 2006 onwards. The possibility – indeed the overwhelming likelihood – of an evolutionary trajectory from one to the other is not something that has been explored before, despite (i) the clear cultural similarities between the groups involved, and (ii) the clear pattern of incremental change that led from one iteration of the information technology to another. Without exploring or even identifying those individual pathways, it was, of course, impossible then to follow the downstream logic which leads to the conclusion that the ‘symbiotic relationship’ so widely written about in the discipline of terrorism studies amounts, in fact, to a co-evolutionary relationship between those three networked groups and their information technology of choice, the common foundation stone of whose architecture is its networked nature. One could indeed go further and identify information as the common denominator between the two (Gillings et al. 2016) and this will be addressed later.

The expository trail, however, begins with the Lebanese Shia militia and terrorist organisation Hezbollah – literally *hizb Allah* or ‘the party of God’ – which emerged in the early 1980s, inspired by the Islamic revolution in Iran in 1978 and 1979 and Israel’s invasion of Lebanon in 1982 (Norton 2018, pp. xii-xix). It would take Hezbollah a number of years to subsume its competitors, particularly the popular and reformist Amal movement (Norton

1987), but even before it had been formally constituted, it had already been involved, 'in league with Iran' (Norton 2018, p. xii), in a number of major attacks. The most notorious were the 1983 truck bombings targeting the US Marine and French paratrooper bases in Beirut, which killed 241 Americans and 58 French. It had also achieved worldwide notoriety for taking Western hostages during the 1980s and into the 1990s, including CIA station chief William Buckley, who died in captivity (Thomas 2006). With its roots in the rural soil of south Lebanon, particularly the Bekaa Valley, Hezbollah evolved from a complex web of family, tribal, religious, and regional alliances to form 'a state within a state' in Lebanon (Robinson 2020), a country where 'no government can rule' without its approval (Hazran 2009, pp. 1-2). It is still identified today as 'the world's most heavily armed non-state actor' (Shaikh and Williams 2018). This chapter examines Hezbollah's use of information technology as part of its formidable operational repertoire, focusing on its transition from terrestrial to satellite television in May 2006 and the dramatic new global reach and force multiplier effect this gave it, particularly in the PSYOPS battle with its primary adversary, Israel, during their 2006 war. It will (i) explain how Hezbollah's co-evolution with satellite broadcasting led naturally to Al-Qaeda's co-evolution with the internet, and on to Islamic State's co-evolution with social media, (ii) identify the key drivers that underlay that co-evolutionary trajectory over a period of more than 20 years, and (iii) show how that trajectory now inevitably leads away from jihadist groups to other emergent naturally networked terrorist organisations. As regards its characterisation at the start of this paragraph as a Shia military and terrorist organisation, it is apposite here to consider Hamzeh's contention in his study of Hezbollah (2004), as set out by Hirst (2011), that it is:

...not very useful to speculate whether it was an inherently extremist and primarily military organisation, or a moderate and primarily political one, or about its possible eventual gravitation from the first condition to the second. As a jihadist movement, it was constitutionally bound to strive for the establishment of an 'Islamic order' and for the 'liberation of Jerusalem'. (Hirst 2011, pp. 215-216)

The same may be said for all three groups, Hezbollah, Al-Qaeda and Islamic State, and underlines their fundamentally imprecise and changing nature as complex adaptive systems.

Because there are two distinct strands to this thesis, the development of terrorism from Hezbollah to Al-Qaeda to Islamic State, and the development of information technology from satellite broadcasting (initially terrestrial but more importantly digital) to the emergence of

the internet, and then internet-enabled social media, it is crucial to trace both strands and the manner in which they interact, and to consider what that indicates about the evolutionary drivers and processes involved. For that reason, this chapter will next introduce both strands briefly by (i) locating Hezbollah in the political context of the time, and (ii) locating satellite broadcasting in the rapidly changing landscape of information technology (NASA 2020; Maini and Agrawal 2011). Following that, as outlined in Chapter Three, this chapter will update Hypothesis 1 (the idea that Hezbollah's adoption of satellite technology was purely random) in a Bayesian manner, using four tests to compare the 'traditional' linear interpretation with the 'complex' non-linear interpretation, Hypothesis 2. The four tests (i) ask if Hezbollah shows significant operational evidence of a networked organisational structure that is central to its development, combined with convincing traces of CAS behaviour, as referenced by Hayden (2013, 2006); (ii) look for evidence of its pursuit of autonomous communication (Conway 2005, p. 9), specifically in its leveraging of satellite technology; (iii) trace the manner in which that co-evolution had a force multiplier effect for Hezbollah, particularly during its war with Israel in 2006; and (iv) consider whether Hypothesis 2 'sufficiently explains' the interaction of the two – Hezbollah and satellite technology – in terms of co-evolution. It applies the NATO causal confidence standard in Test 4. If co-evolution is found to be unconvincing, then the already established Hypothesis 1 remains the dominant explanation in terrorism studies. If co-evolution is found to be more convincing and appropriate to the level of twenty-first century knowledge, then it provides a new way of understanding the interaction of terrorist networks and the constantly emergent information-driven technology that has transformed the manner in which they strategize, radicalize, plan and attack. In all four tests, the likelihood of co-evolution wins out over the more traditional hypothesis, never rating less than an even chance – a likelihood of 40 to 60 percent – using the NATO standard.

Hezbollah in its political setting

Like other countries 'grafted onto Near East societies' by the Great Powers after World War 1, Lebanon was always 'a weak state' lacking the usual intermediating socio-political framework that typically develops over time between a nation-state and its society (Wege 2010; Ayubi 1990). The mandate system had been established in 1919 under Article 22 of the Covenant of the League of Nations (*Treaty of Versailles* 1919) and, to protect its interests,

France sought the creation of a Christian-Arab state in the area around Mount Lebanon, previously part of the Ottoman Empire (Daniş 2019). In 1920, the resulting *État du Grand Liban* incorporated areas historically ruled as the Emirate of Mount Lebanon. In 1943, in pursuit of independence from the French mandate administration, an unwritten accord between Sunni, Shia and Maronite leaders, known simply as *al-mithaq al-watani*, ‘the national pact’, agreed that an independent Lebanon should become a multi-confessional⁶⁹ state with a Christian (including Maronite) to Muslim (including Druze) ratio of 6:5 in the new parliament (Rabah 2020; Khalaf 1987, p. 102; Binder 1966, p. 276).⁷⁰ Thus, Lebanon became independent on November 22, 1943. The last French troops left on August 31, 1946. Parliamentary elections were held on May 27, 1947. The effect of multi-confessionalism, however, was that it became a fragmented country riven by crisis after crisis. The most prolonged was the civil war from 1975 to 1990 for much of which ‘government almost ceased to function’ (Goldschmidt Jnr 1991, p. 362). Its modern history since then has been little different (Karam and El Deeb 2021; El Hoss 2008). What *has* changed beyond recognition, however, has been the lot of the Shi’ites, transformed ‘from the most disadvantaged community into the most powerful one in Lebanon’ (Hazran 2009, pp. 1-2). Hezbollah was the agent of that change, despite the fact that when it first emerged between 1982 and the mid-1980s it was ‘less an organisation than a cabal’ (Norton 2018, p. 23) comprising young revolutionaries such as Abbas al-Musawi, who would co-found Hezbollah before being killed by Israeli forces in February 1992; ‘firebrand’ sheikh Subhi al-Tufayli, who would become its first secretary-general; and Hasan Nasrallah, who has served as secretary-general since Al-Musawi’s assassination. Their commitment was identified early on by both Iran and Syria. The former saw them as a means of spreading the fervour of the Islamic revolution. The latter saw them as a valuable link to Iran, as an indirect means of striking at Israel and the US, and as a proxy to keep other Lebanese ‘allies’, such as Amal, in line. As a result, they had many co-evolutionary constituencies, all of whom contributed to their growing presence in a range of different settings. Although these were essentially pre-internet days, Hezbollah was cognizant of the need to use media in whatever form was available, as long advised by its revolutionary

⁶⁹ ‘Confessional’ is used here as a translation of the Arabic term *ta’ifi* to refer to collective identities rather than to religious doctrines and tenets or *madhhab* (Firro 2012, p. 245).

⁷⁰ The Taif Agreement of 1989, which ended the Civil War, changed that parliamentary ratio to 1:1 and reduced the power of the Maronite president (Krayem 2012).

forebears (Marighella 1969). However, it was the transition from terrestrial to satellite television that would promote their image from local to regional to global. Using it, Hezbollah 'laid the groundwork for the effective use of information warfare' by new generations of terrorists, such as Al-Qaeda and Islamic State (Clarke 2017). In terms of a new form of complex terrorism, they set in train a co-evolutionary trajectory that remains operational and as unpredictable as ever.

Hezbollah in its technological setting

With Hezbollah as the starting point, the evolutionary trajectory of the information technology under examination across the three case studies in this thesis begins to emerge. As anticipated by McLuhan (1967, p. 15), the increase in scale in the case of each new technological iteration is crucial to its impact, that being, in the case of exploitation by terrorists, its force multiplier effect. As noted by Gilfillan as early as 1935 in his landmark study of invention and social organisation, *Inventing the Ship*, 'The nature of invention ... is an evolution rather than a series of creations, and much resembles a biologic process' (Gilfillan 1935, p. 275). By just such a process, physically limited analogue television technology evolved into the satellite technology used to such operational effect by Hezbollah. Satellites have three types of communications function: telecommunications, broadcasting, and data transmission, all of which are varieties of electronic information diffusion (NASA 2020; Orbital Today 2020; Maini and Agrawal 2014). Essentially, a digital signal⁷¹ was uploaded to a satellite where it was amplified and retransmitted back to earth to be re-amplified by a diffuse network of earth stations that hugely magnified its reach and distributed it through equipment ranging from global broadcast networks to networks of direct-to-home satellite dishes, to mobile reception equipment in aircraft, satellite telephones, and other hand-held devices, such as global positioning systems. Over time, smartphones were one of the biggest beneficiaries of advances in satellite technology, driving record technology consumerism (Lee 2011).⁷² Satellites circling the earth were frequently self-directing, their orbits determined by

⁷¹ As noted in Chapter One, Claude Shannon's 'breathhtaking conceptual leap' was that 'once information became digital, it could be transmitted without error' (Waldrop 2001). Digital in that sense meant encoded in bits.

⁷² According to Deloitte in 2017, six main trends were driving mobile use and consumer activity in emerging and nature markets. In order of importance, the first was the launch of 4G and the second was smartphone addiction. This 'reliance' increased 'as more features become available' (Wigginton 2017).

onboard computers. Similarly, the use of more efficient computer-controlled ‘phased array’ transmissions boosted broadband capacity and ‘enhanced internet access throughout the world’ (Orbital Today 2020; Balanis 2015, pp. 302-303; Milligan 2005). The scale of this evolution meant that data was now ‘transferred in gigabytes per second rather than megabits per second’. At the same time, the breaking down of barriers between analogue and digital and between terrestrial and satellite technology increased interoperability, scale, and therefore force multiplier effect. That transformed Hezbollah’s global presence and its message of violent defiance. In the case of Al-Qaeda and the internet, to be examined in Chapter Five, the process will be similar. The internet was originally developed as a system that would allow the US military to link satellite systems and to transmit information to and from the front lines of conflict. Again, enabling satellite systems to work together increased interoperability, scale, and force multiplier effect. So, too, with Islamic State in Chapter Six and its early adoption of social media. This Hezbollah case study also reveals the first step towards recognising diffuse terrorist entities as ‘microstructures’ which are ‘global in scope but microsociological in character’ (Knorr Cetina 2005, p. 215). That microsociological nature means they are networks but ‘not simply networks’ (Knorr Cetina 2005, p. 216). They exhibit temporal complexity. While they are on some level organised or co-ordinated systems, the co-ordinating elements are not of the kind associated with formal authority, complex hierarchies, rationalised procedures or deep institutional structures. They are “light” institutionally speaking’ in the sense that they are not associated technologically with hardware or organisationally with structured leadership, and as their interoperability increases, that lightness also increases. ‘Continual disintegration creates the space for successor-elements and this increases the complexity and the chances of survival of the overall system’ (Knorr Cetina 2005, p. 217). In each case, the co-evolutionary mechanism is in play in the context of an overarching evolutionary trajectory leading towards greater interoperability and a world based on a ‘network science of global governance’ (Kim 2019).

Test 1: Hezbollah – linear tacticians or complex network?

The Lebanese state and the emergence of Hezbollah

There was no linear route by which the epic reversal of fortune which led to Hezbollah’s dominance in Lebanon could have come about. In fact, the society from which Hezbollah

emerged was the very definition of non-linearity, where non-linear systems are born of ‘strong mutual interactions (or feedback) between components’, typically leading to ‘endogenously generated stable states as well as sharp transitions between states’ (De Landa 2014, p. 14). Lebanon’s Twelver⁷³ Shia community – often called the *matawila* – was such a system. It was dominated between 1920 and the outbreak of the civil war in 1975 by a handful of powerful families (Hazran 2009) who acted as ‘nodes’ (Wege 2010) around which wider society coalesced. Those families, and the clans and tribes of which they formed part, were inward-looking and characterised by ‘personalism, clientelism and paternalism’, though a new political awareness evolved during the late 1960s, particularly as Shia religious scholars began arriving in Lebanon from Najaf’s ‘circles of learning’ after Iraq’s Ba’athist coup in 1968 (Shapira, 1988, p. 116). Many of those scholars or *ulema* – in particular, Hussein Fadlallah, often described as Hezbollah’s spiritual mentor (Cambanis 2010);⁷⁴ Abbas al-Musawi, the organisation’s first secretary-general (Ranstorp 1997, p. 46), and Hassan Nasrallah, Al-Musawi’s successor and current secretary-general (Kaplan 2010) – would, as noted earlier, become leaders of Hezbollah’s founding theological cadre (Hamzeh and Dekmejian 1993, p. 36). As an overwhelmingly Shi’ite movement for the establishment of an Islamic state through the implementation of Islamic law, the *ulema* occupied a position of influence equivalent to that of clerics in Iran’s Islamic Republican Party. ‘The dynamics of emergent Shi’a student-teacher networks ... changed the worldview of Lebanon’s Shia community and the worldview of what would become Hizballah’ (Wege 2010).

There was more than a hint of the ‘restored caliphate’ (Ruthven 2015), the idea of an overarching clerical hierarchy to replace the Turks’ repudiation of the Islamic Caliphate in 1924 (Halverson et al. 2011; Lewis 1994, pp. 41-49) when al-Musawi declared, ‘We are not a party in the traditional sense. Every Muslim is automatically a member of Hizballah, thus is it impossible to list our membership’. To that extent – like Al-Qaeda and Islamic State – Hezbollah could be described as a ‘jihadi proto state’ (Lia 2015), where the threshold of acceptability is ‘very low’ (Lia 2015, p. 32) and the term emirate can be applied even to a small

⁷³ The Twelver (also known as *Imamiyyah*) community is the largest branch of Shia Islam, so called because its adherents believe in 12 divinely ordained imams, the last of whom will be the Madhi, an eschatological Messianic figure who will appear at the end of times (Momen 1985).

⁷⁴ Fadlallah’s relationship with Hezbollah could also be ‘strained and tense’ (Norton 2018, p. 104), denoting an important source of feedback.

number of true believers. 'The very scalability of the jihadi state-building project, from a mere group of committed fighters to a full-fledged state with a multi-million size civilian population, enables the jihadis', says Lia, 'to view every action they take as relevant for the ultimate goal of a powerful Caliphate ruling the Muslim world'. In that constant struggle for scale and influence, 'international terrorism is a legitimate weapon' (Lia 2015, p. 36) deployed in a shifting environment characterised by 'internal and external dynamics which may alter the overall calculus'. This is reminiscent of Hayden's view that while 'at some times, some terrorist organisations exhibit characteristics of complex adaptive systems', they do not always function as such (Hayden 2013, pp. 19-20). That is because they are constantly under the influence of two counteracting feedback loops: the need for secrecy and the need for recognised success, where the greater the former, the less likelihood there is of innovation leading to the latter. Hezbollah's identity as a complex adaptive system, driven by interaction and feedback, was beginning to emerge.

Hezbollah: From armed militia to international terrorism

Not surprisingly for such a complex organisation, Hezbollah's development as a 'security apparatus' (Wege 2008) was propelled by three significant and intertwined regional events: the Lebanese civil war that began in 1975, the Iranian revolution of 1979, and Israel's invasion of Lebanon in 1982. In the background, the failure of Gamal Abdel Nasser's secular Arab nationalism in Egypt in the 1950s and 1960s may also have lent credence to the idea of Islam as a political force whose time had finally arrived (El Hourri 2012, p. 13). The first social and political radicalisation of the Shia grew out of *Harakat al-Mahrumin* (The Movement of the Deprived) established by Musa al-Sadr in 1974 (El Husseini 2010, p. 806), better known by the name of its militia, Amal (Hope) (Kepel 2015, p.125). A year later, the civil war was sparked by tensions over the growing Palestinian presence in the country and the marginalization of Shia Muslims by the ruling Christian minority (Robinson 2020). Palestinian militants had begun attacking Israel from south Lebanon in 1968 and had also become involved in a battle for dominance with Christian factions from the early 1970s. Syria reacted to the growing unrest by moving into Lebanon in 1976 (Dawisha 1978) to prevent 'a power vacuum that might lead to it being outflanked by Israel in the event of war' (Lawson 1984, p. 452; Tschirgi and Irani 1982). Israel responded by invading southern Lebanon in 1978, This, along with the fact that

they could no longer make a living from the land, led to a Shi'ite 'exodus' to the southern suburbs of Beirut (Kepel 2015, pp. 124-125). The Israelis moved north in 1982 to expel the Palestinian fighters, some 8,500 of whom were finally evacuated by ship that August after a seven-week siege of Beirut in which 5,000 civilians died (Shlaim 1999, p. 413), a siege whose brutality would inspire the 9/11 attacks 19 years later (Bin Laden 2004).

Into this tinder box came Hussein al-Musawi in July 1982, founding the Islamic Amal militia (*Amal al-Islamiyah*), co-ordinating his operations against the Israelis with Hussein al-Khalil, formerly of Fatah, the largest faction of the PLO, and forming links with elements of Iran's Islamic Revolutionary Guard Corps (IRGC), which was deploying in the Bekaa Valley at around the same time (Levitt 2021). Of those Revolutionary Guard units, the Sepah al-Quds Pasdaran was particularly skilful at engendering the revolutionary zeal that morphed al-Musawi's followers from Islamic Amal into Hezbollah, literally *hizb Allah* or 'the party of God', taking its name from the Qur'an (5:56). 'Iran's presence in the Bekaa integrated Khomeini's foreign policy goals of exporting the revolution and creating an Islamic Republic in Lebanon through Hizballah' (Wege 2010). At the same time, the Pasdaran⁷⁵ offered the Shi'a of the Bekaa 'an articulation of resistance that conformed to Shia religious tradition while creating a vision of something greater than a mere confessional militia.' That extraordinary confluence of events led to the emergence of Hezbollah, whose 1985 manifesto 'vowed to expel Western powers ... called for the destruction of the Israeli state, and pledged allegiance to Iran's supreme leader' (Robinson 2021; Hizballah 1985). By the time the IDF withdrew from most of the country – apart from its self-declared 'security zone' along the southern border – that same year, Hezbollah had become 'the most prominent actor in compelling Israel's retreat' (Mapping Militant Organizations 2019) and was emerging as a formidably networked franchise for exporting terrorism abroad. Strindberg and Warn (2005, pp. 24-25) argue that to describe Hezbollah (and Hamas) as 'enemies of the United States', as they are frequently characterised, is an over-simplification given that their attacks have been overwhelmingly against Israel. As against that, Kramer (2008) argues that Hezbollah's 'deep-down' ideology is to return to a time 'when Islam dominated the world as the West dominates it today'.

⁷⁵ The Pasdaran is an informal name for Iran's Islamic Revolutionary Guard Corps (IRGC).

Irrespective of whether one or the other is correct, both display a longing for the scale and influence of the caliphate.

An Iranian proxy with a global terrorism mandate

What was Hezbollah? There was inevitably debate about whether it was a terrorist organisation or a highly motivated resistance movement with roots in the Bekaa Valley, where it gradually replaced the ‘virtual alphabet soup of secular guerrilla organisations, the bulk of which were defined by Marxist or pseudo-Marxist ideologies’ (Wege 2010).⁷⁶ It has since become apparent that this was part of a generational change, sparked by the end of the Cold War, that moved away from old hierarchical groups and towards their networked ‘flatarchical’ (Morgan 2015) successors, such as the PLO (Hoffman 2006, pp. 76-77), which drew strength from their global ummah. In fact, Hezbollah was making the transition from ‘a loose collection of underground terrorist cells’ to ‘a hybrid organization woven into the structure of Lebanese society’ (Mapping Militant Organizations 2019). In the first sign of its emphasis on perception management, it made a calculated effort to ‘blur its image as a pan-Islamic terrorist group, while at the same time strengthening its image as a legitimate Lebanese resistance movement fighting an occupying army’ (Azani 2006). It was learning, through a process of co-evolution, to adopt multiple different identities in acknowledgment of its diverse origins, its demanding sponsors, and its well-armed opponents (Opall-Rome 2006). Azani (2011) describes the organisation’s delicately executed strategy of ‘walking on the edge’ between political activism and political violence, while Flanigan and Abdel-Samad (2009) describe what they term its ‘social jihad’ – the process of adding to its support base and radicalising followers not through its military arm but through involvement in highly effective non-profit health and social welfare networks. Norton (2018, p. 34) describes it as ‘a Janus-faced organization’. It has, agrees El Hussein (2010), ‘a dual and contradictory reputation’. El Hour (2012) similarly writes of the ‘layers to the movement’s political identity’, each of which represents a new stage in its ‘transformation’. Attempting to understand it as a simple linear proposition distinct from its secretive interactions is doomed to failure.

⁷⁶ Among the organisations gradually replaced in the Bekaa were the Democratic Front for the Liberation of Palestine, the Popular Front for the Liberation of Palestine, the PFLP General Command, and the Abu Nidal Organization (Wege 2010).

Arguably the best example of this strategic deception was the creation of 'Islamic Jihad', which took responsibility during the 1980s for a number of assassinations, kidnappings, and bombings, but which subsequently transpired to have been an alias used by Hezbollah to give it 'a modicum of plausible deniability' in order to muddy the reality of its symbiotic relationship with Iran (Jaber 1997, p. 113; CIA 1985, p. 9). Islamic Jihad was behind the abduction of several foreign hostages between 1982 and 1992 and claimed to have executed one of the most high profile, CIA station chief William Buckley, in March 1984 (Kross 2014, pp. 255-259; Thomas 2006; Rida 2001). Among its founders was Imad Mughniyeh, 'a brilliant military tactician'⁷⁷ who doubled as Hezbollah's chief of international operations (Levitt and Schenker 2008). Less evasive was Ali Akbar Mohtashemizakat, a Khomeini loyalist and former Iranian interior minister, who described Hezbollah as 'part of the Iranian rulership' and 'a central component of the Iranian military and security establishment' (cited in Azani 2006). In other words, an Iranian proxy (Lane 2021).⁷⁸ It was no accident then that the Hezbollah flag featured the same symbols as the *sepah* or badge of the IRGC, a hand holding aloft an AK47 with a globe in the background depicted in green, the colour used by the tribe of the Prophet Mohammed (Matusitz 2018, pp. 9-10).⁷⁹ Tutored by Iran, the 'extremist militancy' that led to Hezbollah's international designation as a terrorist organisation began on April 18, 1983, when it launched the first in a series of signature suicide bomb attacks on foreign targets in Lebanon (Helmer 2006; Kramer 1990). A suicide truck bomb hit the US embassy in Beirut, killing 63 people – including eight members of the CIA – and injuring 120. On October 23 of the same year, a further 299 died in two more car bombs – one at the US Marine barracks in Beirut – killing 241. The Marines were part of a multi-national force overseeing the PLO withdrawal. Later the same morning, a French military compound a few kilometres away was also bombed, adding 58 more deaths. In 1984, a car bomb attributed to Hezbollah killed 24 at a US embassy annexe in east Beirut (Kifner 1984). At around the same time, CIA intelligence showed that Hezbollah ran a training camp near Janta in the eastern Bekaa Valley, just three miles from the Syrian border, where more than 2,000 Shia militants were in training, including

⁷⁷ Mughniyeh was killed in a joint Mossad-CIA car bomb in Damascus in 2008 (Goldman and Nakashima 2015).

⁷⁸ See also: The Soufan Centre, 2012. *A Way Forward with Iran? Options for Crafting a US Strategy*, p. 25. Available from: https://thesoufancenter.org/wp-content/uploads/2021/02/TSC-Report_A-Way-Forward-with-Iran-Report_18Feb2021.pdf [Accessed 19 October 2021].

⁷⁹ The dome above Mohammed's tomb in Medina is known as "the green dome" (Petersen 1999, pp. 182-184).

around 60 from Saudi Arabia and Bahrain who would return to the Gulf to carry out operations there. Here was an organisation building in regional stature towards the moment when its secretary-general, Hassan Nasrallah, would declare that the global hegemon was in its sights: 'Death to America was, is, and will stay, our slogan' (Meyer 2003). True to his word, before 9/11, Hezbollah was responsible for more American deaths than any other terrorist organisation (El Husseini 2010, p. 803; Byman 2003, p. 54).

Test 2: Hezbollah – satellite TV and autonomous communication

Satellite television and the global village

Sputnik 1, the first artificial satellite,⁸⁰ launched on October 4, 1957, set humankind on the path to a high-tech interconnected world (Wallace 2017). So while it may seem easy in retrospect to dismiss satellite television as having been merely an add-on to its terrestrial predecessor, the reality is that in just a few years it resulted in a revolution in both reach and speed that de-territorialised news consumption in particular (Widholm 2018), democratising the availability of information across the globe. It was easy to underestimate because viewers saw nothing different on their living room screens. The invisible element was that its architecture was underpinned by space technology: the product of the Cold War space race between the United States and the Soviet Union, which the Soviets clinched with Sputnik's launch. The 'public outcry' (David 2002) that followed in the US 'kickstarted the United States' technological renaissance'. It led to the rushed establishment of the National Aeronautics and Space Administration (NASA) in 1958. US telecommunications conglomerate AT&T launched Telstar, the first active communications satellite, on July 10, 1962, and the first trans-Atlantic television signal was transmitted that same day. However, in an effort to retrieve some national pride after the Sputnik debacle, the US staged a high-profile relaunch later the same month, on July 23, watched by more than 200 million viewers in the US, Canada, and 16 European countries (Reynolds 2001, p. 500).

Despite this new potential and scale, the television industry did not use satellites for broadcasting until the late 1970s. In the interim, most satellite applications had military or

⁸⁰ An 'artificial' Earth satellite as distinct from a natural satellite such as Earth's moon.

dual military-civilian uses. An example were GPS systems developed by the US Defence Department in early 1970s to help missiles find targets (McDuffie 2017). After the debacle of Vietnam, this was part of a strategy of using information technology to ‘clean up’ war by reducing collateral damage. That would assume even greater importance during the so-called War on Terror, and even later during Obama’s drone years when 563 strikes targeted Pakistan, Somalia and Yemen compared to 57 strikes under Bush (Purkiss and Serle 2017). Information and communications technologies had become integral to the conduct of military operations, and state actors were committed to constant technological innovation (Lee and Steele 2014, p. 71). However, there was more to this technology than its weapons capability. In 1989, CNN was introducing a new type of satellite broadcasting to the world with a constant flow of global real-time⁸¹ news (Jakobsen 2000, p. 131; Robinson 1999), turning Tiananmen Square and the fall of the Berlin Wall into ‘live events’ and showing that news could drive and change foreign policy. In Lebanon, Hezbollah was looking for a new partner to help burnish its multiple images: political, philanthropic, militaristic, and terrorist. That partner was satellite television. McLuhan’s global village had arrived. The new scale introduced by rapidly evolving information technology meant ever increasing numbers were networked and ripe for co-evolution.

Hezbollah and the weaponization of information

The broad interaction of terrorism and information technology was identified from the 1990s, but the nature of that interaction – the mechanism behind it, as proposed in this thesis – remained unclear and scattergun. The acknowledgment that information was ‘the new lifeblood of the international system’ (Conway 2003, p. 1) led to a fresh US government information strategy characterised by Arquilla and Ronfeldt (1999) as ‘noopolitik’, an extension of the ground-breaking biopolitics developed by Foucault (Terranova 2007, p. 139) based on the geopolitics of knowledge. In that context, Arquilla et al. (1999, p. 72) took the view that terrorism was not just about communication, as originally proposed by their RAND predecessors (Jenkins 2015a), but ‘about information’. They noted the disparate but probably not unrelated facts, for example, that trainee suicide bombers were prevented from accessing

⁸¹ ‘Real-time’ news is defined by Jakobsen (2000, p. 131) as ‘the transmission of pictures less than two hours old’.

international media, that terrorists aimed for spectacular attacks that would ‘consume the front pages’, and that among the consequences of those spectacles were increasing public demands for more state surveillance and intelligence gathering. The rapid spread of networked information infrastructures (Luke 2001, p. 113) was driving changes in political, military, economic, social, and cultural affairs, cutting across traditional temporal and spatial boundaries and contributing to the new idea of globalisation (Conway 2003, p. 2). Interconnected computer networks were leading to ‘a paradigm shift’ in tactical intelligence collection that was transforming counterterrorism for the first time since the Cold War (Fitsanakis and Bolden 2012, p. 28). The world was becoming ‘hyperconnected’ (WEF 2013).

The importance of information may have been clear, but there was little attempt to identify how, in the form of information technology, it linked so pervasively and so almost-organically to the wide range of users who adopted it and gradually came to find that it dominated their lives.⁸² It was as if the technology and its users shared a common element of their make-up, which, of course, they did: information. This thesis proposes that that link between information technology and its users – among them terrorists – is explained by co-evolution. In terms of its understanding of the importance of information technology and information warfare, Hezbollah prepared the way for the relentlessly innovative manner in which Al-Qaeda exploited the internet and Islamic State followed with social media. Although satellite technology was pre-internet technology, it had the same ‘lifeblood’ in that it too was technology driven by information. Using it, Hezbollah ‘laid the groundwork for the effective use of information warfare’ (Clarke 2017). The indomitable image it generated and projected around the world – including across the border into Israel, to the intense frustration of Israeli jammers (Opall-Rome 2006) – meant it was becoming, and is likely to remain, ‘the most dominant and capable terrorist group in the Middle East for decades to come’ (Clarke 2017). In essence, it is a perfect example of what Tofler and Tofler (1997) call a ‘deep coalition’ of interactive parts constantly changing in response to its environment:

⁸² In ‘Futurepublic: On Information Warfare, Bio-racism and Hegemony as Noopolitics’, Terranova (2007, pp. 126, 141) conceptualises a series of ‘publics’ as ‘deterritorialized and heterogeneous assemblages’ linked to power as both biopolitical and noopolitical. According to that logic, terrorists could be one such public.

It is multi-dimensional, with all of these groups operating all the time, in continuous flow – multiplying, fissioning, then fusing into others, and so on. It is part of a nonequilibrium order in which there may be instability at one level and temporary stability at another. (Tofler and Tofler 1997, p. xix)

That description is strikingly reminiscent of the characteristics of a complex adaptive system: that state of vacillating between the predictable and the unpredictable that marks an organisation as capable of high levels of performance (Hayden 2013, 2006). Enabling that ‘agile’ system performance (Atkinson and Moffat 2005; Moffat 2003) was and remains the primary aim of Hezbollah’s media strategy. It is what makes Hezbollah ‘masters of long-term strategic subversion’ (Ranstorp cited in Goldberg 2002).

Hezbollah and ‘autonomous communication’

‘Autonomous communication has long been a paramount objective for Hizbollah’ (Conway 2007b, p. 402). Its media journey began with the launch in June 1984 of a weekly newspaper, *Al-Ahed* (The Pledge), the first of a total of six titles, each targeting – like the organisation itself – a different niche in the market. It launched a radio station, *Al-Nour* (The Light) in 1986. *Al-Manar* (The Lighthouse), describing itself as ‘the station of the resistance’, began as a terrestrial TV channel on June 4, 1991, having laid the groundwork by providing footage of significant Shia events to other stations. One such event was Hezbollah’s assault on the Israeli-occupied Sujud fort in south Lebanon in 1986, of which Hezbollah’s deputy secretary-general, Naim Qassem, declared: ‘Following the first television broadcast of this operation, the camera became an essential element in *all* resistance operations’ (Qassem 2005, p. 257, fn 1). It also broadcast the funeral of Ayatollah Khomeini in June 1989.⁸³ The element of scale was already beginning to kick in even with terrestrial TV. It initially broadcast just five hours a day, employing a handful of technicians to operate a single transmitter covering just the southern suburbs of Beirut (Harb 2015, p. 3). A year later, it was broadcasting regular news bulletins promoting Hezbollah’s first-time candidates in the 1992 election. They did better than expected, winning a surprise eight seats (Hamzeh 1993, p. 321). The Lebanese government granted Al-Manar a satellite licence in 1997, but only on the insistence of Syrian president

⁸³ These events were examples of the fledgling station already co-evolving with its Shia base. The Khomeini funeral in particular attracted ‘millions’ of mourners to the streets of Tehran and many millions more watched via satellite TV (BBC News 2015b).

Hafiz al-Asad, having initially refused its application (Jorisch 2004c, pp.24-25) as part of an official licensing round. Its launch was scheduled for July 2000 but, in an indication of its importance as a Hezbollah mouthpiece, it was moved forward to May 25, the well-flagged date on which Israel planned to withdraw from south Lebanon. It subsequently became 'the secret weapon of the Palestinian Intifada against Israel', devoting at least half its 24-hour-a-day satellite broadcasting to the conflict on the West Bank and in Gaza (Fisk 2000). The ownership of the station was typically ambivalent. Whereas it was registered as belonging to the Lebanese Media Group Company, it was operated openly by Hezbollah members, answered to Hezbollah directors, and received its strategic direction from Hassan Nasrallah's office (Jorisch 2004c, p. 20).⁸⁴ Not surprisingly, its news reporting reflected Hezbollah's strategic alliance with Syria and Iran (Fawaz 2013, p. 104). There was no pretence of neutrality. It would never interview Israeli officials in order to achieve balance in a news story. 'We are not looking to interview [Ariel] Sharon', said its director of news, Hasan Fadlallah. 'We just want to get close enough to kill him' (Goldberg 2002). This attitude alone runs so deeply counter to the instincts of most independent minded journalists as to define Al-Manar as a politically and militarily compromised mouthpiece for Hezbollah. In that theoretical sense, the station sits four-square with the organisation's pursuit of unmediated autonomous communication. What Hezbollah called its 'message of resistance' led to Al-Manar being placed on the US terrorist watchlist in December 2004 and being named a Specially Designated Global Terrorist Entity in March 2006 (US Department of the Treasury 2006). In other words, the station itself, Hezbollah's primary means of global communication, was sanctioned using a counterterrorism measure. Today, it is also banned in Germany, France, and Spain, and unavailable in Canada, Australia, and the Netherlands.

Hezbollah's use of its suite of media outlets in a networked 'all-channel' manner (Conway 2010, p. 10) was in many ways characteristic of jihadist terrorist organisations, which were typically transnational networks rather than stand-alone groups (Arquilla et al. 1999, p. 41). Because all resources were bent to the service of jihad, it regarded information technology as both a means of communication and a weapon, in the same way that Al-Qaeda regarded the internet, and Islamic State regarded social media. Driven by its socio-religious imperative, it

⁸⁴ Hassan Nasrallah has been secretary-general of Hezbollah since February 1992.

used whatever technological tools were available with a hyper-conviction that increased the likelihood of operational success. Part of that drive to succeed meant it was also motivated to use the next generation of information technology as quickly as it became available and gained the not-inconsiderable tactical benefits of being an early adopter, identified by Burkhardt and Brass (1990, p. 107) in Chapter Two of this thesis, as ‘increased network centrality and power’. Within the specific ‘public’ (Terranova 2017) that is terrorism, that first-mover advantage marked Hezbollah as experts to be sought out by others (Crenshaw 2008, p. 26), so that their expertise cascaded through their networks. ‘In contemporary conflicts, free-thinking and determined adversaries continually test the limits and are continually on the lookout for patterns, seams, and opportunities to exploit’, observes Bazin (2017). ‘Simply put, chaos is their business.’ In the co-evolution of terrorism and information technology, that appetite for chaos comes combined with the fact that each new iteration of the technology is propelled by new self-organising and flexible ‘emergent architectures’ which evolve in a manner analogous to ‘swarm formation’, bypassing ‘potentially brittle’ centralized and hierarchical silos (Roca et al. 2016, pp. 1-4). Every time those potentially brittle silos are bypassed, the interoperability of the technology is increased, in turn increasing the scale it delivers.⁸⁵ Full technological autonomy will require a new non-static paradigm of interoperability (Elkhodr et al. 2016) to match the needs of a world moving inexorably towards a broadly based ‘network science of global governance’ (Kim 2019). That is why terrorist groups such as Hezbollah, Al-Qaeda, and Islamic State, in co-evolving with information technology, seek autonomous communication: not just because it allows unmediated control of messaging, but because the new information technology involved is a move towards greater interoperability and scale, to a greater or lesser extent depending on the degree of evolutionary innovation involved. This thesis also argues that co-evolution between information technology and its users leads to greater interoperability between the two. Because interoperability presupposes data/information exchange mechanisms that allow it to take place (Heubusch 2016), that raises the intriguing question of the nature of those putative mechanisms (Gillings, Hilbert and Kemp 2016).

⁸⁵ A mobile phone is often given as the perfect example of interoperability because no matter what brand of phone or network is used, essentially any phone can call any other phone (Heubusch 2006, pp. 26-30). In that, it is similar to the counterintuitive fact that the firing of billions of neurons in the brain can instantly produce coherent behaviour through a form of swarming collective computation (Flack 2017; Russell 1995).

Test 3: Satellite broadcasting as a force multiplier for Hezbollah

Hezbollah: Spearhead of the ummah

Hezbollah's television channel, Al-Manar, was created in its likeness. Its first general manager, Ali Dahir, said in 1992 that it had been established 'to express the views of the oppressed ... and to advocate a mass media that respects Islamic morals and Muslim tradition' (Jorisch 2004c, p. 20). In that context, the evolution from terrestrial to satellite broadcasting allowed Hezbollah to plug into the worldwide Muslim *ummah*, beaming what has been described as its anti-Semitic 'hatred' (Jorisch 2004c) to between 10 and 15 million viewers a day, a new scale that almost instantly gave it a global presence. Hassan Nasrallah referred to this when he described Hezbollah as the 'spearhead of the ummah'. He said the conflict in which it was engaged was one 'surpassing Lebanon ... It is the conflict of the ummah' (Saad-Ghorayeb 2006, p. 4). In terms of co-evolution, Al-Manar was used to cultivate the 'community of the Islamic resistance' within and beyond the Shi'ite constituency (Dakhlallah 2010, cited in Harb 2015, pp. 5-6), while that community turned to it in increasing numbers for reassurance. The new scale also allowed Hezbollah to engage in 'psychological warfare against the Israeli enemy' to a degree not possible before. It broadcast into Israel, frequently in Hebrew, giving its versions of deaths, casualties, and encounters between the two sides. It claims this played a 'very sensitive and important role' in Israel's withdrawal from south Lebanon in 2000, though Israel says such claims were overblown (Jorisch 2004b). Mind games of this kind, noted Van Creveld (1991), were symptomatic of the increasingly information-orientated approach to the 'irregularization' of non-military modes of conflict that had become synonymous with 'netwar' (Arquilla and Ronfeldt 1997). The aim of such irregularization, particularly in the realm of information warfare or manipulation, says Rothrock (1997) was 'the degradation of ... adversaries' capacity for *understanding*' [author's italics], a tactic that Hezbollah has used again and again in Lebanese domestic politics. In geopolitical terms, its 'destabilizing actions' now had a global reach (Feltman and Benjamin 2010). While many had predicted that access to satellite television and the speed with which it was adopted during the 1990s would lead to the 'Westernization' of the Middle East (Jorisch 2004c, p. xiii), Al-Manar turned the tables on that assumption. With a tactical skill that would challenge even

the expertise and resources of Israel and its superpower American ally, it began to effectively counter the narrative of Israel's invincibility. In a positive feedback loop that is characteristic of complex adaptive systems, its success played into the essence of Hezbollah's notion of resistance: empowerment and 'constant readiness to face the enemy'.

Empowerment is expressed in the media and discursive strategies of Hezbollah, in its efforts to understand its enemy, its inventive military tactics, and the articulation of a narrative of resistance by actively producing new meanings and challenging old ones. (El Hourri 2012, p. 11)

Critics of Hezbollah and Al-Manar saw this playing back of the 'Western' technology against its creators as 'the darker side of the media revolution in the Arab world' which sought 'to promote profoundly anti-Western agendas' (Jorisch 2004b, pp. 1-2). Amongst the most vociferous critics was Israeli scholar and innovation expert Avi Jorisch, who noted at the time that Hezbollah had exploited its 'privileged position' in Lebanon – a position 'fortified by its successful guerrilla war' to end the Israeli occupation in 2000 – to create 'a mass media outlet of global reach'. In that reading of events, Hezbollah's operations and its use of Al-Manar to project the same image of dominance that Israel had managed to project since the 1967 War, were inextricably linked. The result, he said, had been that 'with access to continuous funding from Iran, the station has grown by leaps and bounds from a clandestine, ramshackle operation to a comprehensive satellite station'. He agreed with Hezbollah that 'the significance of the station goes far beyond Lebanon'. This was a textbook case of co-evolution, not alone between Hezbollah and Al-Manar, but between Hezbollah and Iran as well. Who was paying the piper? Seed capital for Al-Manar was reported to have come from Iran, along with an annual start-up budget of around \$1 million. Just three years later, in 2004, reflecting the scale of its development, the annual budget was around \$15 million (Jorisch 2004b). Over the years, Iranian subsidies to Hezbollah have been put at between \$100 million and \$200 million, some of which also went to Al-Manar. The Iranians were known to be very 'results-orientated' when it came to funding (Levitt 2005) and they therefore believed that the impact of the station was strategically worthwhile.⁸⁶ There were large donations, too, from the Shia communities in Europe, the US, and Canada, some going to 'The Resistance Media Donation

⁸⁶ *The New Humanitarian* (2006) pointed out that in the same year, 2006, the US subsidized Israel to the tune of \$3 billion, though of course this was government to government.

Fund' and to 'Support the Resistance Media Al-Manar Television'. Less well-off supporters among the *ummah* donated in the form of annual *zakat*,⁸⁷ almsgiving required of every good Muslim (Del Cid Gómez 2010, p. 8). Hezbollah's own drug trafficking is also alleged to have contributed (Jorisch 2004b). All of this, plus a relentless programme of 'brand management' (Matusitz 2018), led Hezbollah in 2004 to move beyond the idea of resistance and to begin describing itself as *qanat al-'Arab wa'l-Muslimin* (the station of Arabs and Muslims). It was taking advantage of its latest resource, 'a gleaming public identity' (Matusitz 2018, p. 13). It gave its community of supporters the idea that they belonged to 'something greater than themselves': something that was 'pan-human, pan-Muslim, and pan-Arab' (Jorisch 2004b).

Hezbollah: Global reach and global terrorism

In terms of exporting its terrorism, Hezbollah's ambitions were global, too (Robinson 2020). Since its 1985 manifesto, it had been increasingly active overseas, beginning with the hijacking of TWA Flight 847 from Cairo to San Diego on June 14 of that year, during which 23-year-old US Navy diver Robert Dean Stethem was beaten and shot dead and his body thrown onto the Beirut runway. In March 1992, a car-bomb at the Israeli embassy in Buenos Aires killed 29. In July 1994, a suicide bomb at the AMIA Jewish Cultural Centre in Buenos Aires killed 85 and injured more than 300. The same month, a car bomb exploded outside the Israeli embassy in London, injuring 20, while a second bomb exploded in Finchley at a charity with links to Israel. In June 1996, a truck bomb next to a housing complex used by US air force personnel in Dhahran in Saudi Arabia killed 19 and injured 498, of multiple nationalities (Leonnig 2006). In February 2005, former Lebanese prime minister Rafik Hariri was assassinated in Beirut in a truck bombing first attributed to Syria, although Hezbollah was later implicated (Blanford 2006). Hezbollah also showed itself adept at recruiting overseas, with specific instances in the US, Canada, Russia, China, Uganda, Thailand, and Cyprus. In 1989/1990, police found a Hezbollah cell operating in Valencia, Spain, scouting US and Israeli targets across Europe. In Africa, operatives helped to finance the organisation by dealing in 'blood diamonds' in Sierra Leone and Liberia (Leuprecht et al. 2015, p. 2; Farah 2001). Israel was the first to declare Hezbollah a terrorist organisation in 1989. The United States followed suit in 1995 (Addis and

⁸⁷ *Zakat* is calculated at 2.5% annually of savings and assets (Del Cid Gómez 2010, p. 8).

Blanchard 2011, p. 1). The Arab League and the Gulf Co-operation Council did likewise in 2016. Following a suicide bomb attack on a bus carrying young Israeli tourists in Burgas in Bulgaria on July 18, 2012, in which seven were killed and dozens injured, the EU belatedly added Hezbollah's military wing – but not its political wing – to its list of terrorist organisations. Amplified by Al-Manar, Hezbollah's uncompromising message of defiance and threat was resounding far beyond the Middle East.

That defiance paid dividends. According to Israeli press reports in 2002, Syria had integrated elements of Hezbollah into the Syrian army stationed in Lebanon (Levitt 2005). And in a 'major shift' from the caution exercised by his father, Bashar al-Assad had agreed to supply them with heavy arms, including a new 220 mm rocket (Schiff 2002) in addition to Iranian arms being trans-shipped as usual via Damascus. At the same time, Hezbollah and Iranian Revolutionary Guards were 'more active than ever' in recruiting, training, and tasking operatives from their own and other groups, a good example being a cell of Palestinians who killed seven Israelis in a raid into Metsuba in northern Israel in March 2002. According to senior UN officials, Hassan Nasrallah worked closely with Imad Mughniyeh in planning terrorist attacks globally and across the UN-certified blue line separating Israel and Lebanon. 'To a group like Hezbollah', writes Levitt (2005), 'which maintains parallel and intertwined terrorist, guerrilla, political and social welfare wings under the banner of one large movement, the multiple and varied forms of support Iran (and to a lesser degree, Syria) offer, are at least as significant as the cash Tehran deposits in the group's bank accounts.' Such links powerfully illustrate the multi-dimensional operational structure of Hezbollah and the reason secrecy, compartmentalisation, and control of the diffusion of information are imperative to its survival. What Solvit (2012) observes about war as a complex adaptive system applies as readily to Hezbollah and terrorism:

The agents and the system are adaptive because the individual and collective behaviours of its agents change as a result of experience, which has repercussions for war itself. War comes to resemble an 'ecosystem' where living organisms are continually engaged in a set of relationships with every other element constituting their environment. Thus war can be understood as a generative social phenomenon which is accordingly uncertain and self-modifying – or, said differently, a CAS. (Solvit 2012, p. 121)

Hezbollah: The 'divine victory' of 2006

In the years immediately before its 2006 war with Israel, and despite its complex ties to Iran and Syria, Hezbollah had come of age as a complex and multi-dimensional social phenomenon with multiple operational branches all driven by the same overarching commitment to Shia pre-eminence. Despite the results-orientated generosity of its two main regional sponsors, future independence became a strategic priority. This, says Levitt (2005) was designed to ensure that no matter how the domestic politics of Iran played out over time – in the sense that a more moderate regime in Tehran might at some point strike a 'grand bargain' with the West, trading an end to its sponsorship of terrorism and pursuit of nuclear weapons for full economic and diplomatic relations – the organisation could continue to function autonomously using its own resources and international networks of contacts and affiliates. Its relationship with Syria had likewise shown greater operational 'autonomy' since Syria's withdrawal from Lebanon in 2005 (Scheller 2013, p. 159). The war was sparked in the summer of 2006 when Hezbollah kidnapped two Israeli soldiers it intended to use in a prisoner exchange and Israel responded with massive force, killing more than 1,000 people, leaving around one million displaced, and severely damaging Lebanon's infrastructure and economy (International Crisis Group 2006). Given Hezbollah's steady expansion under Iran's auspices, some saw the conflict as 'the First Israel-Iran War' (Zisser 2011, p. 3). A day after the fighting began, Al-Manar was attacked by Israeli jets. There were consistent attempts – only briefly successful – to jam its transmitters, turning the conflict into 'a battle to stay on air' (Cochrane 2007, p. 7). The multiplier effect was again in evidence: by broadcasting the 2006 war 'live' and by providing important footage to other local, regional, and global channels, the station's popularity across the Middle East leapt from 83rd to 10th between July 15 and July 28 (Goldman 2006). That enormous propaganda value was exemplified on July 14 by the Hezbollah attack that used a Chinese-designed C-802 radar-guided anti-ship missile to hole the Israeli flagship, *Hanit*, a 1,275 tonne Sa'ar 5 class corvette, on the waterline as it patrolled in Lebanese territorial waters ten nautical miles off Beirut (Harel 2006). The attack killed four sailors, set the flight deck alight, and crippled the propulsion systems inside the hull according to the usually reliable online military commentary, *Defence Update* (2006), published in Israel. Within minutes, Hezbollah had posted video of the stricken ship on YouTube, were broadcasting it on Al-Manar, and distributing it to media outlets globally (Clarke 2017). With

the fighting still going on, the outcome of the war, it seemed, was predetermined despite the odds. Billboards appeared across Lebanon bearing the words, 'Divine Victory' (Matar 2008). The same slogan appeared endlessly on Al-Manar (Matusitz 2018, p. 10). It echoed the surname 'Nasrallah', which translates literally as 'victory from God' (Khatib 2012, p. 23), part of a 'hyper-populist narrative' carefully nurtured and targeted by Hezbollah's brand managers (Matar 2008, p. 122). Hassan Nasrallah had indeed promised victory in April 2006 and the war, showing live on the airwaves of Al-Manar, elevated him to 'quasi-divine status – Lebanon's only saviour' (Khatib 2012, p. 23).

The ferocity of the conflict led, in military terms, to Hezbollah's biggest evolutionary step change in years (Blanford 2017, p. 6), transforming it from one among many Lebanese militia to a regional player with global reach. In terms of scale, one assessment in 2017 said it had 'grown enormously' since the war and put its strength in personnel and materiel at more than 20,000 fully trained combatants; a large special forces unit; a signals intelligence unit; an amphibious warfare unit including semi-submersible craft; some 100,000 rockets and missiles, including sub-ballistic guided missiles fitted with 1,100 pound warheads, and anti-ship missiles; and even, in Syria, an armoured brigade. It had 'benefitted from combat experience in a multitude of environments', using 'reconnaissance and intelligence data to develop more complex operations' (Blanford 2017, p. 7). As a consequence, Israel's Institute for National Security Studies, in its annual strategic assessment for 2017, ranked Hezbollah as 'currently the gravest military threat facing Israel' (Shapir 2017, p. 76). It had, said retired brigadier general Assaf Orion, 'a larger arsenal of artillery than most nations enjoy'. Military threat? Terrorist threat? Regional threat? Geopolitical threat? In reality, all four and more. As Shapir (2017, p. 67) observed: 'It is difficult to view Hezbollah through a single prism.' The United States, however, had no such difficulty. Since the killing of the 240 Marines in Beirut in 1983, White House policy-makers had routinely adopted Deputy Secretary of State Richard Armitage's description of Hezbollah as 'the A-team of terrorism', while regarding Al-Qaeda as 'the B team' (El Hussein 2010, p. 803). However, there was nothing static about this organisation. 'Hezbollah emerged as a response to a particular historical situation, and the organisation continues to evolve along with the changing situation in the region' (El Hussein 2010, p. 804). What that sentence describes is a snapshot of mutually expedient co-evolution,

where information technology provides an operating system for the interaction that drives both stable and unstable emergence in complex adaptive systems.

Test 4: Estimating the causal credibility of co-evolution

The aim of Test 4 is to review Tests 1, 2 and 3, and, using the NATO estimative probability yardstick, to assess the degree of causal credibility attached to co-evolution as the most likely explanation for the symbiotic relationship between Hezbollah and satellite television, the new iteration of information technology it seized upon in mid-2000.

Test 1 Reviewed: Hezbollah as complex adaptive system

In Test 1, it was essential to find in Hezbollah: (i) a networked organisational structure that is central to its development; (ii) convincing traces of CAS behaviour.

Without rehearsing in detail what has gone before in this chapter, everything about the emergence and development of Hezbollah has been non-linear, generated by interaction. Networking was a fundamental part of its place in the Twelver Shia community, where interaction with other 'nodes' (Wege 2010) such as powerful families and clans was part of its identity. The Shia religious scholars who arrived from Najaf in 1968 added an additional dimension that prepared the ground for the radicalism that would be engendered by the Lebanese civil war, the Iranian revolution in 1979, and Israel's invasion of Lebanon in 1982. In that context, Hezbollah's identify as a jihadi proto-state (Lia 2015) fits squarely with its constant pursuit of scale and influence, which it was afforded by the powerful patronage of Iran and Syria. That perpetual search for greater differential fitness in the evolutionary landscape is among the core features of complex adaptive systems (Kauffman 1993, 1992, 1991a) and one of the main drivers of their evolution. One can also see its 1985 manifesto challenge to the United States and pledge to destroy Israel in the same light. One can co-evolve with one's enemies as well as with one's friends, hence the co-evolution of terrorism and counter-terrorism (Jenkins 2015b).

In each of the case studies in this thesis, Hayden (2013) has important observations in relation to the organisation's structure, how that influences its ability to learn and innovate, and what that, in turn, says about whether or not the organisation can be described as a complex

adaptive system. As regards Hezbollah's blurring of its identity, Hayden (2013, p. 2) notes that while linear systems typically respond proportionately to stimuli, non-linear systems such as Hezbollah 'make the relationship between causes and effects difficult to observe'. As illustrated by Hezbollah, non-linear systems 'self-organise to find optimal positions in fitness landscapes', where the capacity to self-organise means they evolve based on the natural selection of 'accidents' for 'their ability to improve the overall fitness of the system relative to its goal' (Jantsch 1980). Co-evolution may occur 'where the existence of one element ... is tightly bound up with the existence of another', such as Hezbollah and the scale generated by Al-Manar as a global broadcaster. Beyond that, a key hypothesis is that network structures that evolve from system dynamics influence learning and innovation through information exchange mechanisms, in the sense that they promote or constrain processes of adaptation. Hayden (2013, p. 8) says that organisations that are state sponsored, 'such as Hezbollah', are likely to evolve into core-periphery networks. These emerge as 'elements on the periphery join the core to exploit economies of scale, or 'as cores expand into outlying neighbourhoods for resource exploitation'. Core periphery networks exhibit a high degree of 'clustering', which is the extent to which all their nodes are connected to all other nodes. For instance, social networks, information diffusion, and virus propagation exhibit core-periphery structures (Gomez-Rodriguez et al. 2010). They typically have much higher transmission rates for complex contagions – such as the emergence and spread of new societal norms through social contact or the adoption of technological innovations such as satellite broadcasting (Coleman et al. 1966, 1957)⁸⁸ – than other structures. That is because multiple short paths between nodes build many 'wide' bridges in core periphery networks, creating highly effective transmission rates (Reid and Hurley 2011). 'This has significant implications for state-sponsored terrorist organisations which enjoy both the resources and the network structure to support innovation against adversaries' (Hayden 2013, p. 8). So, while one might have expected organisations with state sponsors to be hierarchical and bureaucratic, Hezbollah, whose system architecture favours more innovation, instead shows innovative tendencies in its choices of 'targets and tactics'.

⁸⁸ Complex contagions 'require social affirmation from multiple sources'. They depend primarily on the width of bridges across a network (Damon and Macy 2006, p. 702).

Assessment

Given the empirical evidence that emerges from the intertwined narratives that constitute any 'history' of Hezbollah's multiple personalities, together with Hayden's analysis of how and why the organisation functions as effectively as it does, the likelihood that (i) its network structure has been central to its development is rated 'highly likely' (more than 90 percent) using the NATO probability standard. The likelihood that (ii) this analysis of Hezbollah has shown convincing traces of CAS behaviour is also judged highly likely.

Test 2 Reviewed: Satellite TV and autonomous communication

In Test 2, it was essential to find: (i) a new iteration of information technology being adopted by Hezbollah in a manner that increased the organisation's power and influence; (ii) convincing traces of co-evolutionary behaviour between the terrorists and the information technology.

In *Mini-manual of the Urban Guerilla*, Marighella (1969, p. 30) famously exhorts, '[N]ever fail to install a clandestine press', noting that 'small clandestine newspapers, pamphlets, flyers and stamps' all played a role in 'propaganda and agitation against the dictatorship'. In line with that exhortation, Hezbollah used every means available to amplify its propaganda and increase its reach. As a terrestrial channel, Al-Manar gave it a national presence to underpin its political, social, and Islamist strategies. As a satellite channel from May 2000 onwards, it brought its message of Shia resistance to the world, challenging and engaging the global *ummah* in a way not previously possible, reflecting for the first time the views of the oppressed in a televisual setting where Islamic morals and tradition were the norm. It played to the radical idea of a 'global village', where local concerns were of global import, made possible by rapidly developing information technology (McLuhan and Powers 1992). Hezbollah were early adopters of satellite broadcasting and with it came 'increased network centrality and power' (Burkhardt and Brass 1990, p. 107) in the world of terrorism: a new stage, new credibility, and a newly amplified threat reaching 10 to 15 million viewers worldwide every day.

The power of that global presence galvanized and empowered every aspect of the organisation. Unlike other large-scale television enterprises, its aim was not commercial but

wholly propagandistic. It allowed Hezbollah to engage in successful psychological warfare against Israel during the 2006 conflict, lending it an operational edge unanticipated by the Israelis, to their intense tactical frustration (Clarke, 2017; Khatib, 2013, pp. 36-71; Conway, 2008a, p. 20; Jorisch 2004c, 2004b, 2004a; Fisk 2000). As a result, its strategy became a potent mixture of conventional and psychological warfare. Every Hezbollah operation was subject to the requirements of its media handlers. Every Hezbollah unit included a cameraman. The 'highlights' of every confrontation were edited to Hezbollah's advantage. As far as its own constituency was concerned, Hezbollah was winning in all circumstances. Its co-evolution with the global reach of Al-Manar was part of what Tofler and Tofler (1997, pp. xix-xx) described as a 'deep coalition' of disparate elements changing 'at hyper-speed' in a conflict zone dominated by knowledge and power rather than force. Control of information through autonomous communication was the key to controlling the narrative.

Assessment

The likelihood that (i) Hezbollah's adoption of satellite broadcasting increased its influence and network centrality is rated 'highly likely' (more than 90 percent). Some might see it as self-evident. As regards (ii) there being convincing traces of co-evolutionary behaviour between Hezbollah and the satellite technology, that is rated 'likely' (60 to 90 percent), the narrative being earlier in the co-evolutionary trajectory and therefore somewhat less compelling in the case of Hezbollah than in the subsequent cases of Al-Qaeda and/or Islamic State.

Test 3 Reviewed: Satellite TV as a force multiplier

In Test 3, It was essential to find: (i) convincing evidence of the new scale generated by the interaction of Hezbollah and satellite television and leading to a force multiplier effect; (ii) convincing traces of greater technological interoperability as a result of the interaction of the two.

There is no doubt about the new scale that Al-Manar as a satellite broadcaster brought to Hezbollah. On the basis of the figures alone, the case is made: less than five years after it went on air, it had a budget of \$15 million a year plus regular multi-million dollar budgetary top-ups from Iran. An audience of between 10 and 15 million viewers a day gave it global reach.

It leapt from 83rd to the 10th most watched channel in the Middle East over a period of just 13 days during the 2006 war. To suggest, however, that this scale had a force multiplier effect, which implies some degree of military/terrorist benefit, is to go further. This thesis contends that the reason the force multiplier effect is beyond doubt is because Hezbollah took a calculated decision to combine its military and its psychological warfare strategies so that the two were inextricably linked. That this was a strategy that worked is evidenced by the fact that from the start of the 2006 war and repeatedly thereafter, Al-Manar sites and transmitters were bombed by Israeli jets and there were continuous efforts to jam its broadcasts. By the end of the month-long war, despite the fact that the two sides had fought one another to a virtual standstill, the perception among its own people was that Hezbollah had scored a 'divine victory' given what should have been Israel's overwhelming firepower. Going on air first with the funeral of Ayatollah Khomeini, then building its audience with Israel's withdrawal from south Lebanon and with the Al-Aqsa Intifada a few months later, identified Hezbollah as 'the spearhead of the sacred Muslim struggle against foreign occupation' (Ranstorp 1997, p. 38), a committed organisation with the power ultimately to 'create a new Islamic world order' (Matusitz 2018, p. 12).

The very public assassination of Rafik Hariri in 2005⁸⁹ and the war with Israel in 2006 changed the image of Hezbollah forever. Within the parameters of how it saw itself, it had come of age as a credible regional threat in what Israel is given to describing wryly as 'a tough neighbourhood'. In the realm of information technology, equivalent scale was generated by the technological interoperability that came with the transition from terrestrial to satellite broadcasting. Technological interoperability aims for friction-free information exchange between differing systems (Elkhodr et al. 2016). Because it breaks down internal architectural barriers, each new iteration of information technology allows greater system scale. Al-Manar – and thus Hezbollah – saw its reach increase from local to global and its audience increase from tens of thousands to tens of millions. As complex adaptive systems, that greater interoperability will have served to confirm the technological 'wisdom' of the co-evolution of the two, predisposing them towards continuing interaction in the future.

⁸⁹ Hariri's was the most internationally high-profile of a series of assassinations that year. The others included journalist and academic Dr Samir Kassir; the publisher of daily newspaper *An Nahar*, Gibran Tuëni, and the former head of the Lebanese Communist Party, George Hawi (AP News 2013; Scheller 2013, p. 143).

Assessment

The probability that (i) the interaction of Hezbollah and satellite television generated new scale, leading to a force multiplier effect for the former is rated 'likely' (between 60 and 90 percent). As regards (ii) convincing evidence of greater interoperability, this is rated as 'an even chance', meaning a 40 to 60 percent likelihood. That is slightly less than might be expected due to the lack of empirical evidence of greater interoperability and the consequently circumstantial nature of the argument.

Conclusion

This chapter set out to establish whether co-evolution was a more plausible explanation for the symbiotic interaction of Hezbollah and satellite broadcasting at the start of the new millennium than previous explanations based on a mix of chance, availability, or psychological manipulation of the media, among other random explanations. It applied four tests – three plus this overview – to examine the credibility of that proposition of co-evolution, identifying aspects of the Hezbollah narrative that, seen from the updated point of view of complexity science, might reasonably be expected to lead to that conclusion. In all four tests, the likelihood of co-evolution won out over the more traditional hypothesis, never rating less than an even chance – a likelihood of 40 to 60 percent – using the NATO estimative probability standard for assessing secret intelligence (Irwin and Mandel 2020, pp. 18-20). However, in order for co-evolution to be described as a mechanism that typically applies in cases where terrorist organisations adopt new iterations of information technology – in other words, 'to infer beyond the immediate data to something broader that is not directly observed' (Della Porta 2008, p. 199) – it will have to receive similar cross-case underpinning in the cases of Al-Qaeda and the internet and Islamic State and social media which now follow.

CHAPTER FIVE

Deadly Embrace 2 – How Al-Qaeda leveraged the internet, the most powerful new technology since Gutenberg, to stage the world’s most lethal terrorist attack

Introduction

Al-Qaeda’s suicide attacks on the World Trade Centre, the Pentagon, and the Capitol, on September 11, 2001, were ‘the deadliest terrorist attacks in history (Morgan 2009, p. 222). They left 2,977 dead, apart from the 19 hijackers of the four airliners used in the co-ordinated attacks. Al-Qaeda was an early adopter of the internet (Weimann 2014, 2008, 2006, p. 67; Denning 2009, p. 3). It ‘intuitively grasped’ its ‘enormous communicative potential’ and sought to harness that power to ‘facilitate [its] tactical operations’ (Hoffman 2006, p. 214). In line with that strategy, it used the powerful new information technology as an online ‘operating system’ to plan and execute the 9/11 attacks, while remaining, in effect, invisible to Western intelligence services (Tenet 2002, p. 4), for whom ‘cyberplanning’ (Thomas 2003) was still an unknown concept. The scale of the fatalities was a direct reflection of the increased interoperability generated by the ‘phase transition’ from pre-internet systems to internet-enabled systems, sweeping away internal technological barriers and allowing greater scale, reach, and ‘seamless connectivity’ (Yocabet and Reijnen 2021). The core proposition of this thesis is that as complex adaptive systems, the three terrorist organisations it uses as case studies, Hezbollah, Al-Qaeda and, subsequently, Islamic State, formed co-evolutionary relationships with three successive iterations of information technology, satellite broadcasting, the internet, and social media, and, as a result, experienced heightened force multiplier effects. At the heart of co-evolution as a central tenet of complexity theory is the idea that, as in biological systems, it comes about because the co-evolutionary partners find reciprocal interaction mutually beneficial (Nuismer 2017; Holland 1992, p. 20).⁹⁰ In the case of high-performing terrorists, it enables them to strike more effectively. In the case of the technology, it spreads and evolves more quickly as a result of being used innovatively by

⁹⁰ As noted by Holland (1992, p. 20) in Chapter Two, co-evolution between systems or within systems is ‘how aggregate behaviour *emerges* from the interaction of the parts’.

networked terrorist organisations at the height of their operational efficiency, the point at which they may be described as complex adaptive systems (Hayden 2013).

Because there are two distinct strands to this thesis, the development of terrorism from Hezbollah to Al-Qaeda to Islamic State, and the development of information technology from satellite broadcasting (initially terrestrial but more importantly digital) to the emergence of the internet, and then internet-enabled social media, it is crucial to trace the evolution of both strands, the manner in which they interacted and continue to interact, and to consider what that information indicates about the evolutionary drivers and processes involved. For that reason, it may be useful here to introduce both strands briefly by (i) locating Al-Qaeda in the political context of the time, and (ii) locating the emergence of the internet in the rapidly changing landscape of information technology (Naughton 2016). Following from that, the same four tests will be applied to Al-Qaeda and its leveraging of the internet as were applied in Chapter Four to Hezbollah and satellite broadcasting. Those tests will (i) ask if Al-Qaeda shows significant operational evidence of a networked organisational structure that is central to its development, combined with convincing traces of CAS behaviour; (ii) look for evidence of its pursuit of autonomous communication, specifically in its adoption of the internet which it used not just to amplify its message but to remain operationally 'invisible' in the run-up to 9/11; (iii) trace the manner in which its co-evolution with the internet had a force multiplier effect, culminating on September 11, 2001, in the deadliest terrorist attack in history (Morgan 2009, p. 222) and (iv) ask whether co-evolution 'sufficiently explains' (Beach and Pedersen 2012, p. 8) the interaction of Al-Qaeda with the powerful new internet technology that would 'catalyse awareness of the need for Muslims to "resist" and open new ways for them to participate in that resistance' (Brachman 2006, p. 158), an imperative already, at this early stage, strikingly at one with the resistance narrative of Hezbollah.

Al-Qaeda in its political setting

Al-Qaeda is a highly networked Salafist jihadist organisation (Livesey 2005) which emerged from the Soviet-Afghan War from 1979 to 1989 (Taylor 2014). It was co-founded in Peshawar, Pakistan, in August 1988, by former mujahideen including Osama bin Laden and Palestinian cleric, Abdallah Azzam, the latter of whom had already set up *Maktab al-Khidamat* (MAK) to channel funds and fighters from the Middle East to Afghanistan to oppose the Soviets

(McCormick 2014; Burke 2007, pp. 72-73; ; Bergen 2006; Marion and Uhl-Bien 2003, p. 59). Azzam is sometimes credited with having coined the term *al-qaeda al-sulbah* or 'the solid base', from which the name 'Al-Qaeda' emerged, the idea being to create a vanguard of jihadists ready to fight around the world as required (Thomas 2021; Migaux 2007, pp. 314-315). After Azzam's death in 1989, MAK was expanded and incorporated into a more diffuse Al-Qaeda, and without that fortuitously wider network, Al-Qaeda might not have had the reach ultimately to carry out the 9/11 attacks (Marion and Uhl-Bien 2003, p. 60). This was typical of its organic, non-linear development with its roots in the global *ummah*, although it is worth noting that Lynch (2006b p. 13) takes the view that much of Al-Qaeda's rhetoric about a global Islamic identity was and remains self-serving, aimed at 'driving a self-fulfilling prophecy' rather than reflecting reality. After 13 years of increasingly bloody bombings in the Middle East and Africa, Al-Qaeda attacked the United States⁹¹ on September 11, 2001. Nineteen terrorists hijacked and crashed four commercial airliners, two of them into the Twin Towers and a third into the Pentagon, while the fourth came down in Shanksville, Pennsylvania, about 20 minutes flying time from Washington DC, when passengers tried to overcome their attackers (Williams 2021). In all, 2,977 innocent civilians were killed. It was the greatest loss of life of any terrorist attack in history (Morgan 2009, p. 222). 'Cyberplanning' via the internet played a new and significant role before and after the attack (Kimmage 2010; Ranstorp 2006; Thomas 2003). Public outrage led President George W. Bush to instigate the 'Global War on Terror' (Rogers 2009) and to pursue Bin Laden into Afghanistan, from which he and his remaining fighters decamped in October 2001 to their 'virtual sanctuary' (Ranstorp 2006) in Pakistan, where Bin Laden was shot dead by US forces on May 2, 2011 (Hersh 2016, pp. 13-51). It was the supercharged combination of Al-Qaeda's networked structure and its links to the *ummah*, combined with its co-evolutionary relationship with the revolutionary new technology of the internet (Castells 2004, pp. 3-4), that allowed it to strike with such unexpected ferocity at the information-driven heart of the West (Dillon 2002, p. 1). A US intelligence estimate since America's withdrawal from Afghanistan and the return of the Taliban suggests Al-Qaeda is resurgent and could again pose 'a significant threat' beyond Afghanistan's borders (Jones 2022).

⁹¹ The 1993 World Trade Centre truck bombing on February 26, 1993, was not officially an Al-Qaeda attack, although Ramzi Yousef did spend time in an Al-Qaeda training camp in Afghanistan before he began planning.

Al-Qaeda in its technological setting

The research that would lead to the development of the internet began in 1973 and the new network became operational in January 1983 (Naughton 2016, p. 5). Even in 1983, the extent to which its networked structure would revolutionize trans-global communication (Healey 2014) was widely underestimated. This was because it had originally been developed by the US military to link satellite systems together and to allow the transmission of information to and from the front lines of conflict. Consequently, early access was limited to a silo of academic and military researchers. From the 1990s, however, it began to percolate into mainstream society, until, almost unnoticed, it became what's known as a 'general purpose technology'⁹², one 'without which modern society could not function', such as mains electricity (Naughton 2016, p. 5). That sea-change was already well underway when Al-Qaeda began planning 9/11 in late 1996 and subsequently set up its 'virtual sanctuary' (Ranstorp 2006, p.1) in Pakistan in late 2001. This thesis proposes that what was happening was that as the technology of mass communication first became digitised in the case of satellites, and then moved online with the arrival of the internet, its internal barriers were being broken down and its interoperability increased. This increased interoperability led, in turn, to increased disruptive capacity, scale, reach and force multiplier effect for the technology involved (Castells 2003, pp. 3-4). This same technological evolution, this thesis also suggests, involved a gradual move away from hard infrastructure, such as transmitters in the case of terrestrial broadcasting and earth stations in the case of digital satellites, to online infrastructure and 'socio-technical' terminology in the case of the internet, such as platforms, operating systems, and communications protocols (Lash 2003, p. 54). Networked users began to mirror the networked technology by behaving 'in an internetted manner without a precise central command' (Zanini and Edwards 2001, p. 30), and in this Al-Qaeda had a naturally networked structural advantage. As Al-Qaeda became more diffuse and leaderless, the internet effectively became its operating system (Lia 2006, p. 17) in more than a metaphorical

⁹² More commonly referred to as 'a GPT' (Naughton 2016).

sense, allowing 'operational agility and stealth mode' far in excess of what was possible pre-internet (Ranstorp 2006, pp. 5-6).

Test 1: Al-Qaeda – linear tacticians or complex network?

In Test 1, it is essential to find in Al-Qaeda: (i) a networked organisational structure that is central to its development; (ii) convincing traces of CAS behaviour.

Al-Qaeda: Why Islamic terrorism is amenable to complex structures

Al-Qaeda's non-linear highly networked organisational structure, its roots among the global *ummah*, and its natural cultural and operational fit with the internet, identify it immediately as a complex adaptive system.⁹³ There is a reason for this. In their study of how complexity theory fits with the structure and behaviour of Al-Qaeda specifically, Marion and Uhl-Bien (2003, pp. 56-57) contend that Islamic terrorists are particularly amenable to complex structures and leadership, not least because the contradictory nature of the radical Islamic movement juxtaposes a highly visible organisational persona against the need for absolute operational secrecy. At the same time, the 'self-reinforcing interdependent interaction' which characterises the networked manner in which Islamist terrorists typically function, hones their operational skills and 'creates evolution, fitness and surprise'. As a result, they are 'simply too complex, with too many unique and diverse functions, to be tightly led or structured'. In this context, the similarities between Al-Qaeda and Hezbollah are striking: in particular, both could be described as having multiple personalities. For instance, in order to raise funds, Al-Qaeda owns a range of businesses that are run relatively normally as 'formalized bureaucracies' (Marion and Uhl-Bien 2003, p. 57).⁹⁴ For this reason, Hoffman (2004, p. 14) describes it as 'a private multinational corporation', with Osama bin Laden in the role of 'a terrorist CEO', an inspirational figure not unlike Hassan Nasrallah in the case of Hezbollah (Khatib 2012, p. 23). To support those businesses, Al-Qaeda also has extensive

⁹³ Indeed, in terrorism terms, Al-Qaeda's symbiotic relationship with the internet is arguably the perfect illustration of what McLuhan had in mind when he presciently described 'electronic' media as 'extensions of man', where 'we have extended our central nervous system itself in a global embrace' (McLuhan 1967, p. 11).

⁹⁴ Figures from the CIA (cited in Del Cid Gómez 2010, pp. 3-4) suggest that Al Qaeda's financial requirements before 9/11 came to US\$30 million annually. The cost of the 9/11 attacks is put at between \$400,000 and \$500,000.

banking arrangements (Del Cid Gōmez 2010, p. 3). On the other side of the coin, however – as also identified with Hezbollah – Al-Qaeda’s ‘main business, terrorism, is fogged in secrecy’ (Marion and Uhl-Bien 2003, p. 57). Its ‘tightly controlled cells’ are ‘loosely to moderately linked with outside resources’. Like Hezbollah, it possesses ‘numerous loci of leadership bound by common purpose’. It is structured so as to adapt and learn. At bottom, contend Marion and Uhl-Bien (2003, p. 57), such descriptors leave no doubt: ‘Al-Qaeda represents a complex system’.

While complex organisational dynamics are beyond the capacity of leaders to determine or control, they may, however, be *influenced* by leaders who ‘foster or enable’ (Marion and Uhl-Bien 2003, p. 56) the emergence of the small-group bottom-up networks that are typical of clandestine cells (Malthaner 2018, p. 32). Osama bin Laden was such a leader (Moghadam 2013, pp. 21-23). Although the 9/11 attacks were not devised by him but by Khaled Sheikh Muhammad (KSM), Bin Laden had crucial input: he selected the operatives for the attacks, funded the operation, and insisted it went ahead despite opposition within his own ranks and from Taliban leader Mullah Omar.⁹⁵ In addition, he was more realistic than KSM and reduced the latter’s original plan to hijack ten planes to the more manageable plot eventually executed. While Bin Laden’s leadership was clearly important pre-9/11, it was just one element. Ronfeldt (2003) suggests an analytical framework that explains the resilience of the ‘polymorphic constellations’ associated with Salafist jihadist networks such as Al-Qaeda. The strongest, he says, are integrated across five levels: at the organisational level they display networked design; at the doctrinal level they use collaborative strategies; at the technological level there is particular emphasis on information systems; at the social level they are closed systems where relationships are based on loyalty and trust; and at the narrative level, Ronfeldt (2003, p. xv) observes, the strongest networks will be those whose ‘organisational design is sustained by a winning story and a well-defined doctrine, and all this is layered atop suitable communications systems and strong personal and social ties at base’. Those social ties are underlined by Sageman (2005, 2004) in his study of 400 Al-Qaeda members which showed that 70 percent made the initial contact with the organisation as a result of close friendships and the remainder through networked links such as family. This is reminiscent of

⁹⁵ Mullah Omar died in 2013 (O’Donnell 2015).

the roots of Hezbollah among the ‘inward-looking’ families, clans, and tribes of South Lebanon (Wege 2010). Such social dimensions, notes Ranstorp (2006, p. 2) are ‘difficult to penetrate but critical to understand’ because codes of honour – such as respect, pride, trust, dignity, reciprocity, and revenge – are all powerful tribal motifs that ‘confer legitimacy’ on violence and are powerful instruments of mobilisation. These cultural themes recur across many different levels of Salafist propaganda and psychological warfare, offering a window into ‘the connectivity between past battles, contemporary realities and future missions’, in other words, the different conceptions of time and space conjured by figurative symbolism such as the black flag (*al-riya*) and the iconography of martyrdom (Ranstorp 2006, p. 3).⁹⁶ As Pisani (2002) notes: ‘Al-Qaeda is a particularly complex organisation, halfway between a sect and a medieval military order. It is a network of networks.’

Al-Qaeda: From mujahideen to global jihad

As is the case with Hezbollah, the meaning of the word ‘organisation’ as applied to Al-Qaeda is difficult to pin down given the group’s highly dynamic structure (Moghadam 2013, p. 2). As a result, like Hezbollah, “‘Al Qaeda’ is a messy and rough designation’ (Burke 2007, p. 1), the diametric opposite of a highly structured hierarchical military. Its evolution was organic, unpredictable, non-linear. In fact, argues Burke (2007, p. xxv), ‘the nearest thing to “Al Qaeda”, as popularly understood’, existed for just a short period, between 1996 and 2001. During that time its base was Afghanistan and the battle of Tora Bora, which raged for 18 days in December 2001 in a cave complex in the White Mountains near the Kyber Pass, represented ‘the final scenes of its destruction’ (Burke 2007, p. xxv). During the battle, small groups of US and UK special forces sought but failed to capture or kill Bin Laden and his high command. Thereafter, Al-Qaeda reverted to its role as ‘the extremist fringe of the broad movement that is modern Islamic militancy’ (Burke 2007, p. xxv). Like Hezbollah and its mission ‘to express the views of the oppressed’ (Jorisch 2004c, p. 200), Al-Qaeda’s grievances too were political but articulated in religious terms and in the context of a religious worldview. The movement was, and remains, rooted in social, economic, and political contingencies. That was underlined by the fact that many of the thousands of young would-be fighters who sought Al-Qaeda

⁹⁶ ‘In the mindset of Salafist jihadi adherents, 9/11 was a *ghazwah*, a raid following in the footsteps of the Prophet’s many raids as a warrior emir’ (Ranstorp 2006, p. 3).

training camps as late as 1998 had never heard of Osama bin Laden (Burke 2007, pp. xxv-xxvi). In fact, the first reference to 'al-Qaeda' appeared in a CIA memo of 1996 entitled 'Usama bin Laden: Islamic Extremist Financier' (Burke 2007, p. 5) which notes that 'by 1985 bin Laden had ... organized an Islamic Salvation Front, or al-Qaeda' to support mujahideen in Afghanistan. There is no other mention of Al-Qaeda at the time, even in memos between the US State Department and its representatives in Pakistan. In 1996, Bin Laden is described by senior diplomats as an 'ex-Saudi financier and radical Islamist'. In 1997, the year after he moved from Sudan to Afghanistan and the year before he issued the *fatwa* against the United States⁹⁷ (Ranstorp 1998, p. 322), the State Department uses the term 'al-Qaeda' for the first time, describing it accurately in terms of its non-linear organisational design as 'an operational hub' predominantly for 'like-minded Sunni extremists'.

Bin Laden's 1998 *fatwa*, says Ranstorp (1998, p. 323), essentially a declaration of war against the 'far enemy', the US, was illustrative of his 'general political astuteness', his tactical awareness of local, regional and global issues, and his recognition that globalisation, especially as a result of new information technology, was networking Islamists ever more seamlessly into what he (Ranstorp 2006, p. 5) termed a 'cyber-ummah'. That networking allowed Al-Qaeda and other jihadists to reach far beyond 'their core support base in the MENA region to diaspora populations, converts, and political sympathizers' (Conway and McInerney 2008, p. 10). It gave them new global scale in the form of a vast propaganda platform, totally without editorial mediation. In that sense the *fatwa* could be regarded as a catalyst, which, in the terminology of complexity theory, is a fillip generated by the process of interaction itself to enhance or speed up an emergent dynamic (Marion and Uhl-Bien 2003, p. 62; Holland 1995; Kaufmann 1993, 1986)⁹⁸. 'Catalysts do quickly what [natural] selection, with its random trials and errors, can only do slowly' (Marion and Uhl-Bien 2003, p. 62). Even before Bin Laden's *fatwa* the US was already being relentlessly targeted. Two attacks in Saudi Arabia in 1995 and 1996 were designed to shake both the country's royal family and the willingness of Americans to do business there. The first was in November 1995 when a car

⁹⁷ The *fatwa* was issued by Osama bin Laden and a coalition of four other radical Islamist leaders and sent by fax to the London-based Arabic newspaper, *al-Quds al-Arabi*, on February 22, 1998 (Ranstorp 1998, p. 322).

⁹⁸ This dynamic is called 'autocatalysis'. It refers to a tendency in recursive systems to self-generate catalysts that speed up or enable emergence and evolution (Kaufmann 1993, 1986).

bomb in Riyadh left seven dead, five of them American citizens, and more than 60 injured (Boucek 2007). It marked the start of a decade-long campaign of bombings, suicide attacks, kidnappings, and assassinations. The following June, a 5,000-pound bomb in a fuel truck killed 19 US servicemen at the Khobar Towers military housing complex in Dhahran (Garamone 1996). Then, in the months following the 1998 *fatwa*, two attacks came in quick succession, the bombing of the US embassies in Kenya and Tanzania in which 224 people died, and which were followed by retaliatory American airstrikes on targets in Afghanistan and Sudan (Thomas 2021). Washington designated Al-Qaeda a foreign terrorist organisation in October 1999. A year later, in October 2000, Al-Qaeda suicide bombers detonated a small boat beside the destroyer, *USS Cole*, a ship 'armed with the most expensive weapons in the US naval arsenal' (Isikoff 2010), as it was refuelling in the Yemeni port of Aden. The blast ripped a 40-foot-wide hole near the waterline, killing 17 sailors and injuring 39 (Combs and Slann 2007, p. 353). The attack was an ominous precursor to 9/11.

Al-Qaeda: The deterritorialization of jihadist terrorism

The loss of its Afghanistan base in the winter of 2001 was a turning point for Al-Qaeda. That is when, according to Lynch (2006b), the organisation underwent a fundamental ideational change, what he calls 'a constructivist turn' (2006b, p. 1) which combined its core Islamist ideals with two factors new to its eco-system. The first was the absence of that territorial base which inevitably led to a more diffuse organisational structure. The second was a globalized field of conflict shaped by new media and information technologies enabled by the internet. Like this thesis, though from a different perspective, Lynch (2006b, p. 3) specifically identifies the progression from satellite television to the internet as among the 'structural changes' to which Al-Qaeda was starting to 'adjust'. In the case of satellite broadcasting, the rise of a transnational Arab-language media allowed Al-Qaeda 'to reach out to a regional field of contention in real time, in ways that simply would not have been available to earlier such organisations' (Bunt 2003). It ceased to be an organisation in the literal sense and became 'an idea moving across geographic boundaries carried by satellite television' (Baddarin 2005, p. 8). The effect of that 'constructivist turn', maintains Lynch (2006b, p. 21), was that Al-Qaeda embraced a new 'grand strategy' of 'strategic social construction' where its attacks were no longer simply terrorist actions taken to send a fearsome message, but now had the more

complex aim of 'shaping the background beliefs and norms of international politics'. It made Bin Laden more than a wealthy patron. It made him 'a norm entrepreneur' (Lynch 2006b, p. 16), a complex leader in a setting where norms are 'never fixed permanently' but are 'open to challenge and reinterpretation through ongoing framing struggles' (Lynch 2006b, p. 18). Success for Al-Qaeda on this specific 'battlefield of the media' (Zawahiri 2005, cited in Lynch 2006a and 2006b) has been the extent to which both Western and Arab media have framed the conflict as a 'clash of civilisations' (Huntington 1996), strengthening Al-Qaeda's agenda of defining Muslim identity in just such monolithic and mutually exclusive terms (Lynch 2006b, p.21).

Al-Qaeda's flight from Afghanistan to Pakistan in late 2001 also led to it becoming the 'first guerrilla movement in history to migrate from physical space to cyber space' (Coll and Glasser 2005, cited in Ranstorp 2006). The *ummah* provided a networked global community to which it was already attached. Being online, the cyber-ummah was 'constantly in evolution and developing in all directions' (Ranstorp 2006, p. 5). As a result, cyberspace came to constitute 'a type of central nervous system' for its operations (Ranstorp 2006, p. 1). 'Moving constantly between these spheres of virtual and physical interaction' increased its 'interoperability and survivability in hostile environments' (Ranstorp 2006, p. 5).⁹⁹ This liminal space between the virtual and the physical was captured by Al-Qaeda strategist Abu Musab Al-Suri in his slogan '*nizam, la tanzim*' or 'system, not organisation', which is taken by Lia (2006, p.17) to mean that there should be an 'operating system' available to anyone who wished to take part in jihad, either on his own or in a small group, but there should, by contrast, be 'no organisation for operations'. In fact, he says, 'the global jihadist movement should discourage any direct organisational bonds between the leadership and the operational units'. This 'total deterritorialization of jihadist warfare'¹⁰⁰ positions 'the entire globe as the theatre of war'. That being so, terrorist networks display 'a global microstructural configuration' where 'structures of connectivity and integration are global in scope but microsociological in character' (Knorr Cetina 2005, p. 215). In effect, says Weimann (2008) Al-Qaeda has further

⁹⁹ A 2011 report on the online activities of 11- to 18-year-old children reported that just over half said they behaved differently online because it made them feel 'more powerful and confident' (Greenfield 2014, p. 6).

¹⁰⁰ 'Deterritorialisation' of jihad (Lia 2006, p. 16) is analogous perhaps to 'neomedievalism' (Cerny 2005, pp. 11-13), a world of 'durable disorder' where terrorism is more transnational and diffuse.

evolved from its networked structure to become ‘a decentralised network of networks with no structure, hierarchy or centre of gravity.’ Based on a global alliance of autonomous groups and organisations in a loosely-knit international network, it is, he goes on – as argued in Chapter Two of this thesis – ‘strikingly similar to the internet with its unstructured network, reliance on a decentralized web of nodes with no centre and no hierarchy.’ That structural similarity may well not be a matter of chance, he acknowledges, because ‘al-Qa’ida adopted the internet and has become increasingly reliant on it for its operations and survival’. This is, effectively, a working description of co-evolution between Al-Qaeda and the internet.

Test 2: Al-Qaeda – the internet and autonomous communication

In Test 2, it is essential to find in Al-Qaeda (i) evidence of its pursuit of autonomous communication, specifically (ii) in its adoption of the internet which it used not just to amplify its message but to remain operationally ‘invisible’ in the run-up to 9/11.

Al-Qaeda and the internet: controlling the message

Both Osama bin Laden and Ayman al-Zawahiri were fully aware that not just the success of Al-Qaeda but its ultimate survival depended on gaining the support of Muslim public opinion, and that, as a result, their ‘media war’ was ‘as important, if not more so, than their armed campaign’ (Gerges 2005). This is confirmed by CIA counterterrorism expert Michael Scheuer – head of the agency’s Bin Laden tracking unit, known as ‘Alec Station’, from 1996 to 1999 – who recalls that Bin Laden ‘spent large amounts of money, time, and imagination to build a world-class media and propaganda apparatus’ (Lynch 2006b, p. 5). The aim of that investment was to control the organisation’s messaging, ideally to the point of ‘autonomous communication’ (Conway 2005, p. 9), where it was consumed totally unmediated. The Al-Qaeda leader and his deputy also shared a recognition of the revolutionary significance of new media information technologies (Lynch 2006b, p. 5). They realized the new scale on offer for their messaging, first in the case of satellite broadcasting and subsequently in the case of the internet, which would allow Al-Qaeda to ‘speak with a voice out of all proportion to the small number of activists at its core’ (Kepel 2004, p. 108). Al-Zawahiri, in particular, was struck by the comparison between the potential of the new media and his experience as a 14-year-old recruit to the Muslim Brotherhood in Egypt. As he saw it (Kepel 2004, pp. 72-73), the

benefits were threefold. 'In an age of satellite television', he said, 'international media attention' would be far more effective in recruiting followers than the 'patient, close work' of Islamic charity organisations in the past. To attract that attention, television images of successful attacks, 'featuring hundreds of dead and wounded', would 'sow panic' while galvanizing the faithful. 'But above all, these events would encourage martyrs to come forth and take on future suicide missions.' Al-Zawahiri was broadly correct. What he had not anticipated, however, was that after May 2003, when Al-Qaeda attacked for the first time inside Saudi Arabia, killing a total of 56 people in two residential compound bombings in Riyadh (Hegghammer 2010, p. 160), 'a significant portion' of the Arab media had turned against it, with the result that it found its messages 'refracted and interpreted in widely varying ways among even Arabic-speaking audiences (Lynch 2006b, p. 6). In terms of autonomous communication (Conway 2005, p. 9), the internet eliminated this problem. It provided a new unmediated route direct to market for all Al-Qaeda propaganda. What was posted online was what appeared. This level of exploitation was 'a new waypoint in jihadists' professional use of the new media' (Weimann 2014, p.4). Not alone that, but, in co-evolutionary terms:

[T]he web's shapeless disregard for national boundaries and ethnic markets fits exactly with Bin Laden's original vision for Al-Qaeda, which he founded to stimulate revolt among the worldwide Muslim ummah. (Coll and Glasser 2005)

Al-Qaeda was an early adopter of the internet using its first rudimentary website, alneda.com (Kimmage 2010, p. 7; Hoffman 2006, p. 226). As noted by Burkhardt and Brass (1990, p. 104) early adopter status typically means 'increased power and centrality' for the users. That was certainly true in the case of Al-Qaeda. As a result, it was, says Jenkins (2011, p. 1), unequivocally the first terrorist organisation 'to fully exploit the internet'. That momentum grew exponentially. By the early years of the new millennium, its rapid, focused, and flexible adoption of cyber-tools amounted to its own 'stealth "revolution in military affairs"' (Ranstorp 2004, pp. 83-96). It was able to rebalance some of the unaccustomed criticism from the Arab satellite media. Its online forums, along with audiotapes, videos, and print publications allowed it to restore what US anthropologist, Dale Eickelman (cited in Lynch 2006b, p. 6) characterised as "'warm" ties' with a far-flung body of Muslims, ranging from the already committed to the merely curious. One could even pledge allegiance to Osama bin Laden by

filling out an online form (Brachman 2006, p. 149). The net effect of this embrace of new information and communication technologies was that (i) Al-Qaeda transformed itself into 'an organic social movement, making its virulent ideology accessible to anyone with a computer' (Brachman 2006, p. 149). This was in line with broader pattern of internet-related grassroots activism occurring around the world, among groups such as the Zapatistas in Mexico, for example (Martinez-Torres 2001). Its new decentralized form meant that (ii) it was now 'more dependent on field commands and affiliates to inspire local volunteers to carry out attacks' (Jenkins 2011, p. 2). It therefore embraced 'individual jihad' as against 'organisationally led jihad', which was 'a fundamental shift in strategy'. In addition, the internet had (iii) effectively allowed Al-Qaeda to 'break the media siege imposed on the jihad movement', as Al-Zawahiri (2008; 2001) saw it. For the first time, it controlled its own messaging. This communications autonomy, combined by the reach of the new internet technology, meant that – unrecognised by governments or counterterrorism experts – autonomous cells had 'full spectrum capability' online, to a degree that was 'almost limitless' (Ranstorp 2006, p. 6).

Al-Qaeda: Weaponising the internet

Throughout history, groups and networks from across the ideological spectrum have harnessed emerging technologies and sought to weaponize them in order to promote their own political and social agendas. Nineteenth century Russian revolutionaries Narodnaya Volya, and their use of dynamite in pursuit of the emancipation of the serfs, were an early example of such attacks (Chaliand and Blin 2007a, pp. 147-159), which became known as 'propaganda by the deed' (Merriman 2016). In the wake of the post-9/11 attacks in Bali in 2002, Madrid in 2004, and London in 2005, Brachman (2006, p. 150) observed that while Western governments continued to concentrate on the *operational* use of information technology by groups such as Al-Qaeda, it was its *strategic* use that now represented the 'most enduring and lethal threat over the long term' by radicalizing new recruits and followers and 'shaping their general worldview'. That governments and security services should concentrate on operational issues was not at all surprising given that Bali, Madrid, and London left yet another 447 dead and 3,043 injured, in addition to the still-fresh memories of the almost indescribable carnage of September 2001. Brachman's view, however, was very much

in line with the logic of Lynch's 'constructivist turn' and of Al-Qaeda's new 'grand strategy' of defining 'the interests of all Muslims as necessarily in confrontation with the West' (Lynch 2006b, p. 1). From a counterterrorism perspective, Brachman pointed out, countermeasures such as dismantling radical internet home pages, for instance, were ineffective because they simply popped up elsewhere and attempts to track their users or content were wasted. On the other hand, leaving them in place gave the jihadists a clear field. Either choice was problematical. However, this, in his opinion, was not the most pressing problem. The most pressing problem was the sheer scale of the internet and its often-underappreciated capacity to generate an all-encompassing online environment – a parallel world, in effect – which enabled Al-Qaeda, almost effortlessly and at minimal risk to its own operatives, to pursue the long-term ideological radicalization of large numbers of Muslim youth across the globe, turning them into 'young jihadi soldiers' (Brachman 2006, p. 163). The idea that this could be achieved was then new. Today it is the new normal.

In his retrospective analysis of how Al-Qaeda 'weaponized the internet', while at the same time mutating and growing more dangerous, Brachman (2006, pp. 153-158) noted that jihadist webmasters had been developing their internet skills since well before September 11, 2001. Web forums often served as initial entry points to a range of other material, such as scripted talking points about the religious justifications for waging violent jihad, motivational imagery depicting martyred operatives in a bounteous 'heaven', and videos from active jihad campaigns. However, it was not until they decamped from Afghanistan that the leadership used the internet to 'replace their dismantled training camps, reconnect their weakened organisation, and reconstitute their leadership'. At the same time, they increasingly looked to the internet as a way of shaping military operations on the battlefield. Like Hezbollah before them, as they perfected their combat techniques, they communicated those technologies to a larger audience through a variety of online channels. A good example of this contagion (Crenshaw 2008, p. 26) and the new reach that the internet made available is that Iraqi insurgent tactics were increasingly replicated in Afghanistan. A case in point was the Taliban's adoption of remotely triggered improvised explosive devices or IEDS, more commonly known as roadside bombs, to replace the hardwired detonators of their predecessors (O'Hara 2005). A similar trend was reported in relation to radical Islamist insurgents in the south of Thailand (Waterman 2006). Jihadi media brigades released

continuous streams of emails, propaganda videos, and pictures. They used the latest Western software to create anti-Western products, including video games which allowed the developers to control the 'reality' in which players engaged. All of this was a calculated strategic move to prompt awareness of the need for Muslims to 'resist' and to open new ways for them to participate in that resistance (Brachman 2006, p. 158). Said Abu Musab al-Suri: 'The revolution in communications, and the global satellite channels and the internet, have opened the minds of people' (Masoud 2013).

Al-Qaeda and autonomous communication

Just as Hezbollah saw an opportunity to piggyback on satellite television, a new technology that was already transforming the information landscape of its own backyard, the Middle East, Al-Qaeda too identified the 'enormous potential' of the internet (Hoffman 2006, p. 124). It was forced by its post 9/11 flight from Afghanistan to lean even more heavily on the technology soon to be recognised as 'perhaps the most transformative invention since Gutenberg' (Healey 2014). This would give it the rapid global impact that such a dramatic comparison suggests, allowing it to make sudden and unpredictable progress on a whole range of operational fronts. As regards the so-called symbiotic relationship between terrorism and the media, the internet immediately undermined the idea that it was those who controlled media outlets, whether journalists, editors or proprietors, who were somehow the primary gatekeepers of access to real scale by amplification. What made the difference was the technology itself. Its operators were catalysts in the same way that Luhmann regarded terrorists as catalysts, with 'sense-making, meaning-processing' communication as the leading actor (Lenartowicz et al. 2016, p. 2). Understandably, print gave terrorists' views very limited exposure in mainstream newspapers, though Hezbollah challenged this locally by publishing its own stable of publications in Beirut. Terrestrial TV and radio gave the Shia militia more exposure and better control of its own message. That scale increased dramatically and became transnational as a result of satellite TV. The internet, however, swept away all barriers to scale and rendered the issue of editorial judgment, interference, or censorship, however one elected to see it, totally irrelevant. Disruption by security services apart, what the terrorists published was what their adherents saw and read. The internet became 'the leading instrument of al-Qa'ida's communications, propaganda, recruitment and networking'

(Weimann 2008). It promoted contact between Al-Qaeda and groups it might never previously have reached, such as Algeria's Armed Islamic Group (GIA), Jaysh-i-Muhammad in Pakistan, or Indonesia's Jemaah Islamiyah, who learned much about tactics and, particularly, explosives (Jones 2006, p. 558; Abuza 2004; Golburt 2004). Whereas satellite television gave Hezbollah the means to purvey its resistance narrative globally for the first time, such was the scale injected by the internet that Al-Qaeda was no longer a lone religiously motivated organisation whose message of defiance had become amplified by new technology. It was now the motivational core of a diffuse all-channel jihadist 'franchise' (Weimann 2008) open for business globally.

'Conceptual uncertainties and analytical confusion' are nothing new when it comes to studying a terrorist organisation as secretive, difficult to pin down, compartmentalised, and constantly evolving as Al-Qaeda. Its ideology, as noted earlier about Hezbollah, is 'both clear and rather vague at the same time' (Bakker and Boer 2007, p. 52). For that reason, Mishal and Rosenthal (2005, p. 282) probe beyond the network approach and propose a new type of Islamist terrorist group which they call a 'Dune' organisation, based on a metaphor of 'drifting sandbanks' (Marsden and Schmid 2011, p. 187). The concept is that the strategic behaviour of Al-Qaeda 'relies on a process of vacillation between territorial presence and a mode of disappearance'. Here too deterritorialization – as identified earlier by Lia (2006, p. 17) in relation to Al-Suri's slogan '*nizam, la tanzim*' or 'system, not organisation' – plays a key role. The concept, Mishal and Rosenthal argue, is inspired by the de-territorialisation brought about by globalisation. Groups such as Al-Qaeda, they contend, are fast-moving and 'almost random' (Marsden and Schmid 2011, p. 187). They move from one territory to another, changing their characteristics as they go. While the dune concept certainly describes certain of the globalised, rootless attributes of Al-Qaeda, it does not explain why, as an entity, it acts in that manner. This thesis, however, provides a rationale: that as a complex adaptive system, networked in its structure and innovative by necessity, it is, by its nature, both agile and rapidly responsive. As a complex adaptive system that has been co-evolving productively with information technology since it first identified and co-opted the internet, it has, as noted earlier, taken the internet as its operating system. As a result, certainly in the years before 9/11, it became both autonomous in the way in which it communicated and 'invisible' in the way in which it operated, a strategy that left Western counterterrorism struggling for a logic

to allow it to catch up after the attacks. Hence, diplomat Richard Holbrooke's angry query in *The Washington Post* a month later as to how 'a man in a cave' could 'outcommunicate the world's leading communications society' (Holbrooke 2001). Hence too, CIA director George Tenet's frustrated observation (Tenet 2002, p. 4) that 'the investigation of the 9/11 attacks has revealed no major slip in the conspirators' operational security'. An understanding of the power and logic of co-evolution, and of the co-evolutionary manner in which Al-Qaeda merged with the internet, explains both.

Test 3: 9/11 and the internet as a force multiplier for Al-Qaeda

In Test 3, it is essential to trace the manner in which co-evolution with the internet had a force multiplier effect for Al-Qaeda, (ii) culminating on September 11, 2001, in 'the deadliest terrorist attack in history' (Morgan 2009, p. 222).

Al-Qaeda: How the internet enabled 9/11

'The most important failure was one of imagination', says the 9/11 Commission Report (2004, p. 9) in its executive summary. This thesis challenges that assertion. There had been warnings, underlined the report, that 'Islamist extremists' planned 'to kill Americans indiscriminately and in large numbers'. As 2001 began, counterterrorism agencies were receiving 'frequent' reports about potential threats everywhere the US had interests, 'including at home' (The 9/11 Commission Report 2004, p. 352). 'The system was blinking red'. Likewise, spectacular schemes involving airliners had already been uncovered. As early as 1995, police in Manila defused what became known as the Bojinka¹⁰¹ Plot, a plan by Ramzi Yousef and KSM to blow up a dozen US airliners while they were flying over the Pacific and to crash one of them into CIA headquarters (Brzezinski 2005). In February 1998 came Bin Laden's *fatwa* against the US. In October 2000 came the suicide attack on the *USS Cole*. What had not yet been hit was the United States homeland. At the same time there was no shortage of incitement, recruitment, and training, all newly accessible through the medium of the internet. Those searching for jihadi news updates could sign up for daily feeds direct to their cell phones via Yahoo! and other services (Brachman 2006, p. 152). Followers interested in setting up their own jihadist

¹⁰¹ 'Bojinka' means 'loud bang' in Serbo-Croat.

cells, such as those responsible for the Madrid train bombings – which a judge later found were ‘inspired by’ rather than ‘ordered by’ Al-Qaeda (Reuters 2007) – could find step-by-step instructions for communicating covertly with cell members, defining tactics, and manufacturing explosives, all of which would have been done previously in real-life training camps. In doing this preparatory research, they could have used new stand-alone ‘jihadi-approved’ browsing software, similar to Internet Explorer but restricted so as to ensure the ‘intellectual separation’ of jihadists from the remainder of cyberspace where a multiplicity of other non-violent viewpoints were available (Brachman 2006, p. 152). Such efforts to create a pressure cooker of jihadi ‘ideological space’ could be expected to accelerate as the jihadists sought and achieved ‘dominance’ over the technology, suggested Brachman (2006, p. 153). In actual fact, for as long as it was mutually beneficial, that acceleration was not alone likely to happen but inevitable as a result of co-evolution. To see such interaction otherwise was not a failure of imagination, it was a failure of understanding. Similarly in relation to the co-evolutionary relationship with the internet that powered Al-Qaeda before and after 9/11, it was ‘invisible’ because counterterrorism did not have the tools to interpret it and therefore to visualise it. This thesis proposes a modernisation of that understanding.

In operational terms, the internet was pervasive (Thomas 2003, p. 112). ‘Al Qaeda operatives relied heavily on the internet in planning and co-ordinating the September 11 attacks’ (Weimann (2004, p. 10). In fact, they had been collecting intelligence on targets and sending encrypted messages via the internet for ‘several years’ before, ‘overlapping planning for other major attacks’ (Jenkins 2002, p. 11). This is in line with the belief that the organization had come to favour the internet as an effective new tool for ‘cyberplanning’ (Thomas 2003) because it provided them with ‘anonymity, command and control measures, and a host of other measures to co-ordinate and integrate attack options’. Seen in this light, argues Thomas (2003, p. 112), ‘cyberplanning may be a more important terrorist tool than the much touted and feared cyberterrorism option’, a not-unreasonable view given that cyberterrorism has not (that we know of) yet led to the rash of attacks previously feared. In terms of intelligence gathering, US Defence Secretary Donald Rumsfeld, revealed in 2003 that an Al-Qaeda training manual recovered in Afghanistan had observed: ‘Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy’ (Thomas 2003, p. 118). That gathering of information, however, was done

invisibly online. Some of the 9/11 attackers used free web-based email accounts. Others used only minimal security online. To protect their anonymity, they used the internet in public places. In an example of how the internet allowed the main hijackers to exercise command and control, the operational leader, Mohamed Atta, went online in Hamburg in Germany to research American flight training schools (The 9/11 Commission Report 2004, p. 88). Another of the architects, Abu Zubaydah, kept thousands of encrypted messages in a password-protected area of a website that was discovered by federal officers when he was arrested. They dated from May 2001 until September 9, with the highest frequency in August. In terms of 'cyberplanning' (Thomas 2003), computers seized in Afghanistan showed the operatives were using the internet for both legal and illegal purposes, to collect simple but crucial intelligence, such as to check flight times and purchase tickets, but also to obtain fake passports and drivers' licences (Jenkins and Butterworth 2020, p. 3). Two of the hijackers who relied heavily on their laptops refused to check into a Florida hotel unless they were assured round-the-clock internet access in their room. When communicating with one another online, they used nothing more sophisticated than pre-arranged code words. Three weeks before the attacks, Mohamed Atta's final message to his 18 co-conspirators read, in code: 'The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering' (Thomas 2003, p. 119). The faculty of urban planning referred to the World Trade Centre, the faculty of fine arts to the Pentagon and the faculty of engineering to the Capitol, which they failed to hit. The code was so simple that, in retrospect, believes Melman (2002), 'it could probably have been deciphered had it been discovered in time'. Tellingly, the 9/11 Commission Report (2004, p. 88) noted in relation to Al-Qaeda's exploitation of the internet: 'Technology produces its best results when an organization has the doctrine, structure and incentives to exploit it.' Al-Qaeda had all three. In such circumstances, a terrorist organisation is likely to be at its highest performing as a complex adaptive system and co-evolution is likely to be at its strongest, most compelling, a deadly embrace.

Al-Qaeda: The 9/11 attacks

True to their complex origins, the 9/11 attacks were 'a seismic event with incalculable consequences' (Kepel 2015, p. 1). In just two hours, using the internet as a mobile command

and control system, the 19 terrorists hijacked and crashed four commercial airliners, killing 2,730 people on the ground in New York and Virginia, 213 passengers, and 33 crew, with many thousands more injured and traumatized (FBI n.d.). The first airplane, American Airlines Flight 11, a Boeing 767 loaded with 20,000 gallons of aviation fuel, crashed into the north tower at 8.46 am. The second, United Airlines Flight 175, also a 767, hit the south tower at 9.03 am. The third, American Airlines Flight 77, a Boeing 757, ploughed into the west side of the Pentagon at 9.37 am. The fourth, United Airlines Flight 93, crashed in Shanksville, Pennsylvania, after passengers put up a heroic struggle to stop it being used as a missile to attack the Capitol, seat of political power. The south tower collapsed at 9.59 am. The north tower followed at 10.28 am. As Jenkins (2001, pp. 4-5) observed at the time, these were 'casualties of epic proportions' which 'conformed to a trend of increasing lethality' in Islamist attacks. A multiple co-ordinated attack leveraging the operational benefits of the internet was an appealing option because it allowed for a substantial increase in the number of casualties. Such co-ordinated attacks are rare, but it was not unique. More than 30 years before, on September 6, 1970, the Popular Front for the Liberation of Palestine hijacked three airliners and a fourth the next day (Jenkins 2001, p. 6; Holden 1986). In August 1982, Palestinian terrorists planted bombs aboard two Pan Am jets. In June 1985, Sikh separatists tried to bring down three flights and succeeded in the case of one, Air India Flight 182, off the Irish coast. In January 1995, Ramzi Yousef, mastermind of the 1993 World Trade Centre bombing, aimed to bring down 11 jets in 'one stupendous bombing conspiracy' (Mylroie 1995-1996, p. 3). And in 1998, Al-Qaeda simultaneously attacked the two American embassies in East Africa. Group suicide attacks are even more rare. However, the 9/11 attackers were older and better educated than their typical counterparts in the Middle East, with, as it transpired, formidable 'human resolve' (Jenkins 2001, pp. 7-8). The carnage was deliberately aimed at civilians and 'struck at the principal symbols of American hegemony: commercial and financial power, military supremacy, and – missing its target in this third case only – political power' (Kepel 2015, p. 1). They, attacks and attackers, 'destroyed America's sense of invulnerability and illustrated the limits of its intelligence infrastructure' (Jenkins 2002, p. 2). They 'shattered the pre-existing, prevailing sense of personal, national, and international security' (Kegley 2003, p. 1).

All this was true but what was most significant was that Al-Qaeda used its co-evolution with cutting edge information technology to strike at the heart of the West's 24/7 information society:

The destruction of the World Trade Centre on real time network TV was a strategic surprise attack on an even more complex network, global network society itself, of which the US is the epicentre. Knowledge-based, globally linked through *complex adaptive connections* of every description, the terrorists exploited the very strategic strength of network society, its openness and connectivity, to send violent shock waves throughout the capillaries that channel its flows of image, information, technology, people and capital. (Dillon 2002, p. 1, emphasis added)

Given the almost epic proportions of that description, it is perhaps little surprise that terrorism quickly morphed into 'a new kind of war without end' (Dillon 2002, p. 5), characterised by Simon and Benjamin (2001) as 'The Terror', with echoes of the '*grande terreur*' of the French Revolution (Laqueur 2006, pp. 23-24). The modern-day Terror had begun, they maintained, in 1993, with the first attempt to destroy the World Trade Centre in New York. While Hoffman (2006, pp. 30-31) argued that this bloodthirsty new varietal was 'terrorism motivated either in whole or in part by a religious imperative, where violence is regarded by its practitioners as a divine duty or sacramental act', this thesis suggests that in fact it was the natural, indeed inevitable, result of highly motivated terrorists co-evolving with highly potent new information technology with a global reach. In that sense, former CIA director Jim Woolsey was closer to the mark when he observed: 'Today's terrorists don't want a seat at the table, they want to destroy the table and everyone sitting at it' (Morgan 2004, pp. 30-31). In such an atmosphere of psychological fragility, it became clear that the evolution of information technology from the pre-internet world to the internet-enabled world had transformed not just the way terrorists communicated and controlled their messaging, but the way in which they strategised and attacked as well. This was a new level of conflict that demanded not just a more agile response but a new level of understanding of how the attackers functioned. That new understanding was increasingly provided by complexity theory, an overarching view of the world as non-linear, networked, interactive and inherently unpredictable, very much a reflection, in fact, of both the terrorists and the technology whose symbiotic relationship this thesis describes and explains for the first time.

9/11 The Aftermath

The US invasion of Afghanistan in pursuit of Al-Qaeda began in October 2001. The assault forced Al-Qaeda to regroup in Pakistan, where the leaders found themselves 'in a scramble to keep their movement motivated and coherent' (Brachman 2006, pp. 153-154). It used the internet to replace its dismantled training camps and to rebuild its weakened organisational structure. Although combat classrooms online did not render physical training camps obsolete, information technologies do change the nature of education, indoctrination, and participation (Brachman 2006, pp. 153-154). The allies' continued 'pounding' on Al-Qaeda's central command, says Jenkins (2011, p. 2), led to it becoming 'more decentralized' with, as noted earlier, a new emphasis on individual jihad. By now the organisation could be regarded as having four distinct operational dimensions (Hoffman 2006, pp. 285-289): (i) Al-Qaeda Central, the rump of the pre-9/11 organization, including the core leadership who had survived; (ii) Al-Qaeda affiliates and associates from whom Bin Laden aimed to create an unstoppable jihadist 'critical mass'; (iii) local amorphous groups of adherents, usually with some previous terrorist experience; and (iv) homegrown Islamist radicals willing to carry out attacks alone or with support. Within those dimensions were four loosely matching operational styles (Hoffman 2002, pp. 309-310): the professional cadre entrusted with the most high-value attacks; trained amateurs for use in a supporting role; 'local walk-ins' who played to Bin Laden's image as 'a venture capitalist'; and like-minded insurgents, guerrillas, and terrorists providing occasional support. Despite the US-led countermeasures, Al-Qaeda in Pakistan succeeded in reconstituting itself and playing a role in the bombings in Bali, Madrid, and London in the years immediately following. This led Hoffman (2006b) to opine that not alone had the threat from Al-Qaeda not diminished, but, after the migration 'from physical space to virtual space', it was now 'more dangerous than it was on 9/11' (Hoffman 2006b).

Using the terminology of technological evolution to describe the transformation of Al-Qaeda the organization, Chasdi (2014) described the hub which decamped to Pakistan as 'Jihad 1.0'. The emergence of affiliates such as Al-Qaeda in the Islamic Maghreb (AQIM), Al-Qaeda in the Arabian Peninsula (AQAP), and Abu Musab al-Zarqawi's Al-Qaeda in Iraq (AQI), aka Al-Qaeda in Mesopotamia, represented 'Jihad 2.0'. Splinters from the affiliates, such as the AQIM splinter, the so-called 'Battalion of Blood', could be described as 'Jihad 2.5'. With al-Zarqawi's death in June 2006, AQI created a new entity, Islamic State in Iraq, led by Abu Bakr al-

Baghdadi. Then, in April 2013, al-Baghdadi announced a merger of his forces in Iraq and Syria under the banner of Islamic State in Iraq and the Levant (ISIL). In June 2014 that was shortened to 'Islamic State' (Irshaid 2015). Here was 'Jihad 3.0', the first Al-Qaeda affiliate to 'go rogue' (McCormick 2014). It was a highly motivated new terrorist breakaway in search of a new iteration of information technology with which to co-evolve.

Test 4: Estimating the causal credibility of co-evolution

As in Chapter Four, the purpose of this section is to review Tests 1, 2 and 3; to examine the extent to which Al-Qaeda displays the qualities identified in each test as characteristic of a complex adaptive system, and, using the NATO estimative probability yardstick, to assess the degree of causal credibility attached to co-evolution as the most likely explanation for the symbiotic relationship between Al-Qaeda and the internet. Whether that judgment can plausibly be made on the basis of the evidence adduced thus far, and its causal credibility confirmed using the NATO standard, constitutes Test 4.

Test 1 Reviewed: Al-Qaeda as complex adaptive system

In Test 1, it was essential to find in Al-Qaeda: (i) a networked organisational structure that is central to its development, and (ii) convincing traces of CAS behaviour.

Virtually everything written in this chapter about the emergence and development of Al-Qaeda touches on its networked organisational structure, its blood links to the *ummah*, its determination to extend its reach and challenge the 'far enemy', and its view of itself as a mission-orientated hub of resources and experience to which other likeminded jihadist organisations around the world could connect in order to fight a more diffuse global battle, particularly after 9/11 and its flight from Afghanistan. Its development was non-linear, in fact strikingly similar in its organic, interactive, and unpredictable nature to the development of the internet as described by Naughton (2016). Complexity can accommodate contradictions, and they were rampant. From the beginning, it took up a position on 'the extremist fringe' of modern Islamic militancy (Burke 2007, p. xxv). Even so, some of its beliefs could be traced 'to the earliest days of Islam'. It took a tactical decision to employ the latest Western-developed information technology in its battle against America and its allies (Brachman 2006). It then combined that cutting-edge technology with medieval barbarity to shock the world when the

first Al-Qaeda beheadings were posted online, displaying a 'signature method' of Salafi-jihadist terrorism then still new to Western audiences¹⁰² (Cengiz 2021; Maher 2016). The networked nature of the technology (Arthur 2009; Negroponete 1995) and the non-linear trajectory of its development (Naughton 2016), played to Al-Qaeda's naturally networked strengths operationally, as well as specifically in the planning and execution of the 9/11 attacks (Moghadam 2013; Brachman 2006; Thomas 2003), something the 9/11 Commission Report (2004) would underline time out of number.

Beyond that, Marion and Uhl-Bien (2003, pp. 56-57) contend that Islamist terrorist organisations in general are more amenable to complex leadership because, typically, they are 'simply too complex, with too many unique and diverse functions to be tightly led or structured'. In the case of Al-Qaeda specifically, they argue, that that is because – like Hezbollah – it possesses 'numerous loci of leadership bound by common purpose', and leaders, particularly Bin Laden during his tenure, who 'foster and enable' rather than direct and control. This is an organisation where innovation is bottom up rather than top down (Moghadam 2013) and therefore embedded in the grassroots rather than in the leadership only. In that sense, Marion and Uhl-Bien identify Al-Qaeda as 'a complex system'. There were other elements at play as well. Lynch (2006b, p. 1) identified Bin Laden as 'a norm entrepreneur' and Al-Qaeda's broad aim as 'strategic social construction' through actions designed to shape 'the background beliefs and norms of international politics'. This was a new type of terrorist geopolitics driven by the realization that change was generated through interaction with technology driven by strategic mission, which might also be described as co-evolution. Cyberspace had become Al-Qaeda's operating system. The *ummah* had been transformed into a cyber-ummah (Ranstorp 2006, p. 5). Al-Qaeda had become a system without an organisation (Lia 2006, p. 17), a network of networks, a free-floating international terrorism franchise with 'the entire globe as the theatre of war'. In every aspect of its behaviour it functioned as a complex adaptive system.

¹⁰² The word 'audiences' may seem slightly prurient here. However, by virtue of the new scale enabled by the internet, it is also, on reflection, the most accurate. That scale, of course, was the key to its tactical success.

Assessment

While acknowledging that not all terrorist groups may be described as complex adaptive systems at all times, Hayden (2013, pp. 11-19) too finds numerous convincing characteristics in Al-Qaeda, from an organizational structure that favours innovation, to a propensity to display that innovation in its choice of targets and tactics, to the exploitation of safe havens in order to learn, and a tendency to deliberately choose operations that will provoke aggressive countermeasures. In that context, the likelihood that (i) Al-Qaeda's network structure has been central to its development is rated 'highly likely' (more than 90 percent). The likelihood that (ii) this analysis of Al-Qaeda has shown convincing traces of CAS behaviour is also judged highly likely.

Test 2 Reviewed: The internet and autonomous communication

In Test 2, it was essential to find in Al-Qaeda (i) evidence of its pursuit of autonomous communication, specifically (ii) in its adoption of the internet which it used not just to amplify its message but to render its operational preparations for 9/11 effectively invisible.

Given that it was 'perhaps the most transformative invention since Gutenberg' (Healey 2014), it is not surprising that the internet supercharged the communicative capacity of all of its users (Anderson and Rainie 2014). In the more prosperous parts of the planet, it effectively wiped out transnational communications barriers (Meltzer 2014). It is easy, now that it is a general purpose utility (Naughton 2016), to forget what a dramatic development it was to be able to send an instant communication across the world with a single click. The benefits for terrorists were clear and enormous (Hoffman 2006, p. 124) and were immediately identified by Osama Bin Laden who was already in the habit of spending substantial amounts of money on the Al-Qaeda media/propaganda apparatus in pursuit of any additional element of autonomous communication that would give it an operational edge (Lynch 2006b, p. 5). The primary benefit was that anyone who wished to publish online was free to do so, 'directly and unedited' (Jenkins 2006, p. 126). Al-Qaeda, constantly alert to the competitive benefits of new technological developments, realized immediately that this had the potential to revolutionise control of its messaging. As Al-Qaeda core fled Afghanistan in the immediate

aftermath of 9/11, it also saw the potential to replace physical resources with new digital resources online. Just as the internet had supercharged those who were newly affluent as a result of globalisation, it had also supercharged those who were not, and who strategically or instinctively, in a reflexive reconceptualisation worthy of Beck's risk society (Beck 2009, 2006, 2002), turned it back on those who created it.

The internet also allowed the 'deterritorialisation' of terrorism (Lia 2006, p. 17). It became Al-Qaeda's virtual operating system at a time when its new diffuse structure meant it no longer had, or required, a pre-9/11 'organisation' of substance. It learned that its loss of Afghanistan, the unifying 'land of jihad'¹⁰³ (Jones 2006, p. 565), was balanced by a new 'virtual university of jihad' (Ranstorp 2006, p. 1) whose resources were all online. It became 'jihad's franchise', as Weimann (2008) characterised it. Transferring its operations online meant it could 'go dark' at a moment's notice, disappear from view to the point where even the 9/11 Commission Report expressed astonishment at the discipline of its covert tactics while preparing for the Twin Towers attacks (Tenet 2002, p. 4). In that context, the Commission's epic 640-page report may be read as a textbook account of what happens when 'innovative improvisers' such as Al-Qaeda (Jones 2006) identify a new information technology of unprecedented reach and previously unidentified operational potential: co-evolution rendered them operationally 'invisible' and (momentarily) unassailable. The extent to which it was dominant on the digital battlefield resounded across the globe. Conversely, the extent to which Western intelligence agencies had underestimated the powers of adoption and resolve of their networked opponents (Duffield 2002, p. 157) was evident from the scale of the 9/11 carnage.

Assessment

Given its innovative nature and the degree to which Bin Laden and Al-Zawahiri were both clearly convinced by the operational potential of information technology (Hoffman 2006, p. 124), the likelihood that (i) Al-Qaeda was in pursuit of some form of autonomous communication when it first adopted the internet is rated 'highly likely' (more than 90 percent). As regards (ii) convincing evidence that it used the internet not alone to amplify its messaging but to render itself operationally 'invisible', particularly in the run-up to 9/11, that

¹⁰³ Abu Hamza al-Masri referred to Afghanistan as 'the land of jihad' or 'jihad capital' (Gunaratna 2002, p. 132).

is a proposition which must have a high evidentiary bar and which is therefore rated 'likely' (60 to 90 percent).

Test 3 Reviewed: The Internet as a force multiplier

In Test 3, it was essential to trace the manner in which co-evolution with the internet had a force multiplier effect for Al-Qaeda, (ii) culminating on September 11, 2001, in 'the deadliest terrorist attack in history' (Morgan 2009, p. 222).

In terms of its force multiplier effect, the internet enabled Al-Qaeda to become 'the world's first truly global terrorist organization' (Riedel 2011). There were innumerable points along the route to 9/11 where the outcome might have been otherwise. One example was the fortuitous point at which *Maktab al-Khidamat* (MAK) was expanded and incorporated into Al-Qaeda in 1989 (Marion and Uhl-Bien 2003, p. 60). Yet in the end there can be no doubt that the new operational capacities and scale with which the internet provided the 9/11 attackers gave them not just extraordinary new capabilities, but, even more devastatingly, in retrospect, extraordinary new capabilities that were unanticipated by counterterrorism agencies, and that, therefore, were effectively invisible. There is evidence that Al-Qaeda had been collecting intelligence and sending encrypted messages via the internet for 'several years' before the attacks (Jenkins 2002, p.11). When the planning for 9/11 began in earnest, it was online to such a degree that it was convincingly described, also in retrospect, as 'cyberplanning' (Thomas 2003). In a perfect example of co-evolution, the internet was adopted as an online command-and-control system. Likewise, in co-evolutionary terms, the description of it as Al-Qaeda's 'operating system' is highly appropriate. Without rehearsing all that has gone before, email was crucial, and so confident were the attackers that they were totally under the radar of the security services that their online security was often marginal, frequently a series of code words. They found flight schools online, purchased airline tickets online, checked flight times online, and all without once being detected, to the extent that Georgie Tenet, CIA director at the time, had to admit that their tradecraft was perfect. There was 'no major slip in the conspirators' operational security' (Tenet 2002, p. 4). On that basis, there is every likelihood that had the same hijackings been attempted without the availability of the internet, they might not have succeeded. As in every terrorist attack, the force multiplier effect of the tactics used is encapsulated in the number of casualties: 2,977 dead,

apart from the 19 hijackers, and more than 6,000 wounded, many with life-changing physical or mental injuries (The 9/11 Memorial & Museum n.d.), 'the deadliest terrorist attack in history' (Morgan 2009, p. 222).

Before the deaths of 2,977 people in the 9/11 attacks, the worst single terrorist onslaught had claimed the lives of around 380 people (Morgan 2004, p. 29). This thesis proposes that the unprecedented scale of the 9/11 casualties was a direct reflection of the new information-driven scale that kicked in as pre-internet technology and its hard infrastructure was swept away by the internet. As noted by Castells (2004, pp 3-4), networks had always been less efficient than hierarchical command-and-control systems 'under the conditions of pre-electronic communication technology'. However, the emergence of the internet and its co-evolution with the networked jihadists dramatically changed that calculation and gave the terrorists an unprecedented multiplier effect. As one iteration of information technology replaces another, internal barriers are broken down and the interoperability of the systems, their scale and reach, increases. Interoperability allows 'seamless connectivity' between systems (Yocabet and Reijnen 2021). It means those systems can 'work together, communicate, and exchange information without restrictions'. The keys to interoperability are 'open networks' and these too are the backbone of the internet (Kalathil and Boas 2003). A high-performing 'backbone' affects reach, scalability and connectivity. Thus, Hezbollah's Al-Manar TV saw its audience increase from tens of thousands to tens of millions when it switched from terrestrial to satellite broadcasting. In the case of Al-Qaeda, its reach suddenly became limitless and the disruptive impact of the technology extended beyond the potential for communication to operational capability as well.¹⁰⁴ Both were clear cases of co-evolution between the information technology and the terrorists who exploited it.

Assessment

The probability that (i) Al-Qaeda's use of the internet generated new scale, leading to a force multiplier effect, is rated 'highly likely' (higher than 90 percent). As regards (ii) the likelihood that this force multiplier effect led to the historically high 9/11 fatalities, that too is rated 'highly likely'.

¹⁰⁴ Though, of course, both may be seen in philosophical terms as communication.

Conclusion

Having established in Chapter Four, based on continuing advances in complexity theory, that co-evolution provided, on balance, a more convincing explanation for the symbiotic relationship between Hezbollah and satellite technology than previous theories, this chapter set out to establish whether or not the same parameters applied to Al-Qaeda's adoption of the internet. In fact, the assessments above indicate that the underpinning evidence is even stronger. This is because, as Cassells (2004, pp. 3-4) notes, networks are empowered to a far greater extent than hierarchical systems by information technology. Both case studies indicate that new iterations of information technology increase the interoperability of the systems involved. This, in turn, increases the scale/reach/speed/resilience of the information technology, which benefits all of its users. Because terrorist organisations, particularly mission-orientated jihadist networks of the sophistication of Hezbollah and Al-Qaeda, are typically digital-native early adopters, those benefits of scale and reach inject 'increased network centrality and power' (Burkhardt and Brass 1990, p. 107) and translate into formidable force multipliers. Co-evolution is then in full flight. 'Terrorism is par excellence a strategy of surprise', wrote Martha Crenshaw (1987). On 9/11, the full existential horror of that simple observation became apparent.

CHAPTER SIX

Deadly Embrace 3 – How Islamic State ‘microstructures’ mimicked the decentralised architecture of social media by choosing unilaterally how and when to attack

Introduction

This third case study examines Islamic State and its rapid adoption of social media in the months leading up to its capture of the city of Mosul in Northern Iraq at the height of its insurgency on June 10, 2014 (Hassan 2017) and continuing until the Barcelona attack on August 17 and 18, 2017, in which 16 civilians were killed and 152 were injured (Iguualada 2021; Bourekba 2018; Tremlett et al. 2017). That protracted attack, three linked incidents over a period of two days, was the largest in Spain since the Madrid train bombings in 2004. While ploughing a van into the busy pedestrian precinct of the Ramblas was effective rather than spectacular, this was a sophisticated attack to the extent that none of the eight attackers had known terrorist connections, their recruitment and planning was invisible to the authorities in advance, and the casualties and media shock value were high. Even so, Islamic State’s impact was beginning to fade. The trend in European attacks, according to the policing agency, Europol, was towards a ‘decrease in sophistication’ (Europol 2019, 2018). The annual number of arrests was also falling, having increased each year between 2013 and 2016 (Europol 2019). There was an overall decrease too in failed, launched, and completed attacks (Nesser 2019). At the same time, Islamic State was being decisively pushed back in its Middle East caliphate (Chulov 2019), online (Conway 2017a), and in Europe and the US (Bergen et al. 2019, pp. 21-36 and 37-44). Even so, never before had there been so many jihadist terrorist plots in Europe as in the period between 2014 and 2018 (Nesser 2019, p. 15). For that reason, one ‘major strategic challenge’ remained as pressing for the West as it had been on 9/11: understanding how Al-Qaeda ‘and its progeny’ shaped their narratives and delivered them ‘innovatively through modern technologies’ (Ranstorp 2006, p. 18). Islamic State, a Salafi jihadist breakaway from Al-Qaeda, was that ‘progeny’.

To answer Ranstorp coherently means to look at Islamic State from the standpoint of complexity theory, its co-evolution with information technology, and specifically with social media. This thesis contends that, like Hezbollah and then Al-Qaeda, Islamic State shaped its

narrative and delivered it innovatively as a result of the co-evolutionary relationship between high-performing terrorist networks and networked information technology, both of which function as complex adaptive systems, one of whose core characteristics is mutually beneficial co-evolution. In the case of Hezbollah, satellite technology had enabled it to tell its story of oppression and defiance far beyond the borders of Lebanon and to ratchet up its psychological war against Israel. In the case of Al-Qaeda, the networked nature of the internet swept away all barriers to global one-to-one communication and allowed it to plan and execute 9/11 while remaining invisible to Western intelligence services. For Islamic State, internet-enabled social media offered another radical departure. It allowed terrorist users to form their own networks and then generate and share their own jihadist content. Its interactivity allowed followers to influence the direction of the organisation, a new structural development that would lead to a blizzard of 'microstructural' (Knorr Cetina 2005) single-actor attacks in Europe from the end of 2014 until mid-2017 and beyond. As Castells (2004, p. 9) had predicted, information technologies were being 'diffused throughout the entire realm of human activity' as a result of 'growing miniaturisation'. That more diffuse technology was then being mimicked by the more diffuse nature of its networked terrorist users. That is why the operational period under examination in this case study stretches from the build-up to the fall of Mosul in 2014 to the Barcelona attack in mid-2017. During that period, Islamic State had the power to generate social contagion half a world away 'without the loss of intimacy that once attended such great distances' (Berger 2015, p. 65).

In this chapter, the same four tests will be applied to Islamic State's leveraging of social media as were applied earlier to Hezbollah and Al-Qaeda. Those tests will (i) examine its origins and background and ask to what extent it has a networked organisational structure that shows evidence of behaviour consistent with a complex adaptive system; (ii) look for evidence of its pursuit of autonomous communication in its adoption of social media, and of co-evolution with the new information technology; (iii) trace the extent to which that co-evolution had a force-multiplier effect, culminating in its capture of Mosul at the high point of its insurgency, and continuing through a long series of bloody attacks across Europe that lasted sporadically to the end of the decade (Bergen et al. 2019, pp. 21-36 and 37-44; Chulov 2019; Nesser 2019; Hassan 2017; Liang 2015, p. 6; Cuthbertson 2014); and (iv) ask whether the logic of co-evolution 'sufficiently explains' (Beach and Pedersen 2012, p. 8) that dramatic and multi-

faceted interaction of Islamic State with social media, and the manner in which it brought about ‘a sea change in the way we understand modern terrorism’ (Liang 2015, p. 1).

Islamic State in its political setting

Islamic State is a direct descendant of *Jama’at al-Tawhid wal-Jihad*, a militant jihadist group set up in his home country by Jordanian jihadist Abu Mus’ab al-Zarqawi in 1999 (Liang 2015; Zelin 2014; Whitlock 2006). Both he and Osama bin Laden came of age during the Afghan jihad against the Soviet Union in the 1980s. When they first met in Afghanistan in 1999, their different backgrounds, leadership styles, and aims led to ‘major friction’ and ‘distrust’ between the two men (Zelin 2014, p. 1; Weaver 2006). Whereas Bin Laden was a well-educated facilitator, Al-Zarqawi was a street fighter with a criminal past.¹⁰⁵ Even so, they formed a co-evolutionary ‘marriage of convenience’ (Zelin 2014, p. 1) in 2004 when Al-Zarqawi changed the name of his organisation to Al-Qaeda in Iraq (AQI) and pledged *bayat*¹⁰⁶ to resource-rich Bin Laden (Byman and Williams 2015). Al-Zarqawi’s aim was to oppose the American invasion of Iraq (Liang 2015, p. 1) in a setting in which an American-led coalition had taken control of the country and toppled Saddam Hussein’s Ba’athist regime in 2003, dismantled its army and destroyed its civil structures (Tucker 2015). The result was ‘a security and governmental vacuum’. AQI stepped in, launching a campaign of suicide bombings to take advantage of the increasing political and societal alienation of the Sunni population who had been largely excluded by the new Shi’ite regime of prime minister, Nourik al-Maliki (Meir Amit ITIC 2014). AQI’s influence also spread to Syria after the civil war there began in March 2011, by which time Al-Zarqawi had been killed in a targeted US airstrike.¹⁰⁷ The war caused strategic tensions between the new organisation and Al-Qaeda’s leadership and the marriage ended in February 2014 (Byman 2015) in a hostile and very public ‘divorce’ (Hoffman and Ware 2019), though with AQI’s ranks significantly bolstered. The group changed its name to Islamic State of Iraq and Syria (ISIS) in 2013. In June 2014, it launched an insurgent offensive against Tikrit and Mosul. On June 29, its leader, Abu Bakr al-Baghdadi, announced the establishment of a ‘caliphate’ stretching from Aleppo in Syria to Diyala, north-east of

¹⁰⁵ Al-Zarqawi was known as ‘the sheikh of the slaughterers’ for his legendary brutality (Weiss and Hassan 2015).

¹⁰⁶ Allegiance

¹⁰⁷ On June 7, 2006.

Baghdad, in Iraq, with its capital in Raqqa, and renamed the group Islamic State,¹⁰⁸ to reflect its expansionist ambitions (Irshaid 2015).¹⁰⁹ To demonstrate that this caliphate was more than symbolic, it bulldozed a remote stretch of border between the two countries, at the point where Nineveh in Iraq meets Al-Hassaka in Syria (Black 2014). To mark the occasion, it issued a number of videos, among them one called *End of Sykes-Picot* (Tran and Weaver 2014). Images of the bulldozed border were tweeted to followers using the hashtag, #SykesPicotOver. Al-Qaeda had faded. 'The world' was becoming 'fixated' on the sudden rise of Islamic State (Liang 2015, p. 1).

Islamic State in its technological setting

In terms of technology, Al-Qaeda set the scene for Islamic State. From the first, Bin Laden and his deputy, Ayman Al-Zawahiri, had shown themselves alert to the potential of developments in information technology (Hoffman 2006; Lynch 2006b, 2006a; Ranstorp 2006). They understood, noted Kepel (2004, p. 9) that 'rhetoric and satellite propaganda' could be 'on an equal footing with unmanned bombers and cruise missiles' (Kepel 2004, p. 119). That awareness carried through from Al-Qaeda to Islamic State in the gruesome form of the videotaped decapitations (Harrow 2011) which began in 2002 with the death of *Wall Street Journal* bureau chief Daniel Pearl at the hands of Khalid Sheikh Mohammed (The Centre for Public Integrity 2011), fresh from his role as 'mastermind' of the 9/11 attacks (The 9/11 Commission Report 2004, p. 115). According to the CIA (BBC News 2004), Abu Musa'ab Al-Zarqawi, newly appointed *emir* of AQI, the precursor of Islamic State, is believed to have beheaded 26-year-old US contractor Nick Berg in May 2004, allegedly in retaliation for abuses by American forces at Baghdad's Abu Ghraib prison, with the aim of driving up recruitment, particularly among those with the strongest anti-American sentiment (Pape et al. 2014). In terms of its online propaganda value, decapitation was a tactic, noted Harrow (2011, p. 21), that exploited 'technologies of the information age better than older forms of terrorism', adding matter-of-factly, 'when broadband internet access is made available to the global south, it will be possible to cater for a much wider audience with video-recorded

¹⁰⁸ For a tabulated history of IS names, see Zelin (2014, p. 1) at <https://www.washingtoninstitute.org/media/2714>

¹⁰⁹ The new Islamic State leader since March 2022 has been Abu Hassan al-Hashimi al-Qarayshi (Ajjoub 2022).

decapitations'. Similarly, Lynch (2006a, p. 53) interprets Al-Zarqawi's 'dismissal of satellite television' in favour of the internet as indicating that while Bin Laden and Al-Zawahiri aimed at reaching out to the vast previously unreachable uncommitted middle ground of Arab Muslims, Al-Zarqawi's focus was on 'the mobilization of already-committed jihadists', indicating that these had already moved online. His aim was 'terror marketing' (Mosendz 2014). There is no doubt that, by this point, the internet had become the leading means of jihadist communication (Weimann 2008). Al-Qaeda alone was behind some 5,600 websites, with another 900 or so appearing every year, replete with blogs, forums, chat rooms, and electronic notice boards, frequently carrying calculated disinformation, including false stories about a new 9/11 in the planning. Watching this growth, jihadists became rightly wary of infiltration of websites by intelligence services and began to look for alternatives (Weimann 2014). As a result, 'the turn to social media followed' (Weimann 2014, p. 2). The new terrorist landscape was one where Facebook, Twitter, YouTube, Instagram, Surespot, and content-sharing systems like JustPaste.it allowed jihadist groups to network, to fragment into ever-smaller special interest microsystems, and to generate and exchange their own content. By March 2015, supporters of Islamic State were operating at least 46,000 Twitter accounts generating roughly 90,000 tweets every day, according to a Brookings survey (Berger and Morgan 2015, p. 7). As a result, content production was decentralised: it was now being generated by 'autonomous production units from West Africa to the Caucasus' (Koerner 2016). So while the internet had been 'a facilitative tool' increasing the opportunities for liaison, radicalisation, and attack planning (Conway 2017), social media platforms had the potential to go much further, acting as 'digital replicators' (Gillings et al. 2016, p. 7; LaBar et al. 2016), capable of propagating rather than simply amplifying the messages they carried, and empowering even arms-length followers to decide which tactics would constitute its next 'strategy of surprise' (Crenshaw 1988).

Test 1: Islamic State – linear tacticians or complex network?

In Test 1, it is essential to find in Islamic State: (i) a networked organisational structure that is central to its development; (ii) convincing traces of CAS behaviour.

The emergence of Islamic State, networked 'progeny' of Al-Qaeda

As Chapter Four demonstrated, Hezbollah was self-evidently a networked organisation by virtue of its multiple personalities, its multiple constituencies, and its multiple aims, rendered even more complex by its covert nature (Carley et al. 2003). Its exploitation of satellite technology was also the start of a process of digitisation that was about to lead terrorism online. The same was true of Al-Qaeda in Chapter Five, only more so. Its roots in the Soviet Afghan war, Bin Laden's links to Saudi Arabia, Al-Zawahiri's links to the Muslim Brotherhood in Egypt, and the organisation's foundational links to Palestinian cleric Aldallah Azzam and MAK, meant it was predisposed to networking and to operating across borders. That was its non-linear nature. Its adoption of the internet matched that organisational imperative almost exactly, plugging it into a formidable new technology whose co-evolutionary impact Western intelligence services had not even begun to understand. That lack of understanding continued and grew more dangerous as Islamic State emerged from Al Qaeda in Iraq (AQI), reflecting its founder Abu Musa'ab Al-Zarqawi's belief in the power of medieval violence, always amplified and marketed using the very latest in information technology. As the 'progeny' of Al-Qaeda (Ranstorp 2006, p. 18), all of the complex interactions that had created Al-Qaeda had also created Islamic State. More than that, the environment from which it emerged and drew strength comprised two adjacent civil wars involving a multitude of state and non-state actors, the first in Iraq and the second in Syria, in both of which it engaged with a mission-driven fervour supercharged by the idea of 'apocalyptic time' (Berger 2015, pp. 63-64), temporal acceleration leading to the spread of the caliphate and ultimately the arrival of 'end times'. That was its regional context. In a geopolitical context, it set itself up immediately in the jihadist mind as nothing less than a challenger to the global hegemon, the United States, a challenger that was already reclaiming Muslim lands in the Middle East. What was not clear in the initial stages of its ascent was the force multiplier effect that would be generated by its leveraging of social media, or how – had intelligence services understood what to expect or watch for, even in theoretical terms – that effect would manifest itself. In the event, the terror generated by its well-flagged beheadings, floggings, and crucifixions cleared the way for its seizure of territory to an international chorus of social media support, mainly on Twitter, as the Iraqi army fled before it. It had branded itself as 'the "pure" Islamic utopia that necessitates cruel warfare against its enemies, but ensures social justice, proper

administration, and a righteous and authentic moral life for its faithful' (Hoffman 2017, p. 102). What was still unrealized was that the capacity of social media to allow arms-length followers to feed back into and therefore to influence the direction of a debate, would also allow radicalised followers to launch a series of independent attacks without the need for sanction from any organizational authority. As in the cases of Hezbollah and Al-Qaeda, the architecture of Islamic State's new technology of choice, social media, enabled new unforeseen behaviour by its terrorist users.

Just as Hezbollah's capacity to use satellite technology to broadcast into Israel and thus to open a new psychological front in the 2006 war went unanticipated (Jorisch 2004c, 2004b, 2004a), and just as Al-Qaeda's 19 operatives were invisible as they planned and executed the 9/11 attacks (Tenet 2002, p. 4), so Islamic State's emergence, as Al-Qaeda began to fade, passed unnoticed by American forces in Iraq. As Duffield (2002, p.157) notes, it is typical of a hierarchical actor when confronted with a networked opponent that 'it tends to underestimate and misunderstand the powers of adaption and longevity of the resistance it confronts'. At the point at which American forces withdrew from Iraq in 2011, Islamic State did not yet exist under that name. American generals believed that Al-Qaeda had been 'licked' (Fordham 2015). Their intelligence, the results of their 2007 'surge' (Duffy 2008), information from detainees and from sources on the ground, all 'indicated that Al-Qaeda in Iraq was defeated', leaving no residual issues of substance (Fordham 2015). Yet that was not the case. Al-Qaeda in Iraq was in phase transition to Islamic State, gauging how best to position itself on a complex battlefield with multiple actors and competing loyalties. When it re-emerged in 2011, its aggressive posture signalled an immediate challenge to the US and the Obama White House (Byman and Williams 2015). It posed a direct challenge too to Al-Qaeda whose own ultimate goal of a caliphate now looked unlikely at best. Despite the global scale of the 9/11 attacks, Al-Qaeda now seemed 'sclerotic' in comparison to the dynamic and unpredictable newcomers (Liang 2015, pp. 3-4). Bin Laden's successor, Ayman al-Zawahiri, was 'slow to react about the new caliphate'. Al-Qaeda's future at the vanguard of militant Islam looked doubtful (Liang 2015, pp. 3-4). This was confirmed by the perception that Islamic State not alone adopted social media as its communications technology of choice but took it 'by storm' (Liang 2015, p. 1). Across the globe, other terrorist groups were watching and waiting. The balance of influence was tilting from Al-Qaeda to Islamic State. In July 2014, Al-Qaeda in the Islamic

Maghreb (AQIM) and Boko Haram both swore allegiance to Islamic State. In August 2014, the Egyptian group, Ansar Baytal-Maqdis, followed suit. For Western governments, 'the IS crisis' had become 'one of the most socially mediated conflicts in history' (Liang 2015, p. 10). 'The terror experience' had become 'globalised' and 'democratised'. Potential jihadist recruits were invited to 'set a virtual foot into the battlefield, within a safe and encrypted domain in the comfort of their homes'. Social media was training them to participate.

Islamic State: From local breakaway to global jihadist threat

For as long as it lasted – until the bitter and hard-fought end on Friday, March 22, 2019, according to the Syrian Democratic Forces (SDF), Kurdish-led fighters supported by the US (NPR 2019)¹¹⁰ – Islamic State created a pseudo-caliphate that stretched continuously across 33,670 square kilometres of Iraq and Syria, an area with a population of at least six million and substantial captured oil reserves (Solomon et al. 2015). In parallel with that land-grab came a sophisticated 'digital caliphate' that announced itself by declaring 'cyber war' on the US government and its Western allies (Atwan 2015, p. 1). What was unexpected about the caliphate, notes Liang (2015, p. 4) was that Islamic State 'worked hard' from the moment the caliphate was declared to legitimise its 'new pseudo state'. This, she enumerates, involved 'setting up Shura councils and courts, designing school curricula and immigration policies, increasing security, banking, policing, establishing a currency, and enforcing taxation'. Within those broad social parameters, religion was exploited both as a tool for indoctrination and as 'a means of control' once recruits had arrived. Those recruits were shown a propaganda film entitled *A State, not a Group!*, which outlined how the caliphate ideally worked and listed 16 of its key functions, including 'consumer protection' and 'public health'. In the background played its unofficial anthem, emphasising the 'khilafah'¹¹¹ as a place of 'safety and peace', in contrast to its key magazine, *Dabiq*, published in a range of languages including Arabic, English, French, German and Russian, which calculated its military success in terms of the mutilated corpses of 'infidels' (Liang 2015, p. 4). The psychological impact of the new power balance was clear. 'The overriding point is that success breeds success', said former CIA analyst Emile Nakhleh (Shane and Hubbard 2014). 'The perception of quick victories and

¹¹⁰ For a minutely detailed timeline of the rise and fall of Islamic State see Wilson Centre 2019.

¹¹¹ Caliphate. See also Bin Adam (2001)

territory and weapons and bases, means they don't need to try hard to recruit ... Young people look at ISIS and say, "By gosh, they're doing it!". Charles Lister of Brookings agreed: 'Taken globally, the younger generation of the jihadist community is becoming more supportive of Isis, largely out of fealty to its slick and proven capacity for attaining rapid results through brutality' (Tran and Weaver 2014). As Knorr-Cetina (2006, p. 217) observed about transition in complex systems: 'Continual disintegration creates the space for successor elements and this increases the complexity and the chances of survival of the overall system'.

Spurred on by its social media cheerleaders, the litany of Islamic State killings continued. American freelance journalist James Foley, in August 2014, was the first Western hostage to be beheaded by UK-born executioner 'Jihadi John'¹¹². Maher (2014) opined that the killing was framed so as to present a direct challenge to the United States and to President Obama personally, demanding that America disengage militarily and end humanitarian assistance to Iraq. 'It is the sense of belligerence and brazen defiance that is shocking', he said, noting there was no intention to negotiate. The beheading of James Foley was followed by those of Steven Sotloff; David Haines; Alan Henning; Peter Kassig; Croatian Tomislav Salopek, killed in Egypt; French national Herve Gourdel, killed in Algeria; and Japanese nationals Haruna Yukawa and Kenji Goto. American humanitarian worker Kayla Mueller, who'd apparently been forced into marriage to the Islamic State leader, Abu Bakr al-Baghdadi, and repeatedly raped, was beheaded on February 6, 2015 (Iqbal and Cabral 2022). Just as the 9/11 attacks were designed by Al-Qaeda to provoke overreaction by the US, so the relentless beheadings of 2014 and 2015 reversed the trajectory of American public opinion, which switched from opposing the deployment of fresh US troops in order to challenge Islamic State to supporting it (Mueller and Stewart 2020, p. 25; 2016, p. 32). Equally horrific, not least because of its sophisticated motion picture skills, was the video entitled *Healing of the Believer's Chest*, which showed captured Jordanian pilot Mu'adh al-Kasasiban being burned alive in February 2015. His death followed an IS Arabic Twitter campaign asking followers how to kill 'the Jordanian pilot pig' (Griffin 2014). Of a lesser order in terms of shock, perhaps, but an extraordinary example of a Western journalist being used to propagandize against his own culture, was the series of videos made using British hostage John Cantlie to extol the virtues of his captors (Loyd 2022;

¹¹² 'Jihadi John', killed in a drone strike in 2015, was one of four Islamic State members known as The Beatles because of their English accents (Euronews 2022).

Masters 2015). These, says Maher (2015) – the staged killings, in particular – were examples of IS ‘leveraging its power to asymmetrically shock its enemies’. ‘Even when violence is isolated and sporadic, social media ensures that it is never far from people’s minds’, warned Brooking and Singer (2016). ‘That in turn encourages ugly stereotyping and harmful overreactions by citizens, media, and politicians. The result is a widening of divisions and the spread of anger and fear.’

Islamic State: the ‘caliphate’ that came ‘out of nowhere’

Bunzel (2015, p. 4) notes about Islamic State’s emergence in 2013 and 2014 that it ‘seemed to come out of nowhere’. The reasons were two-fold: because the conventional wisdom among some Western analysts was that Islamic State was nothing more than Al-Qaeda under yet another name, and because other analysts regarded Al-Qaeda as beaten (Fordham 2015) and saw nothing yet emerging in its place. Even when Islamic State did emerge there was scepticism. Many groups, not least Al-Qaeda itself (El Damanhoury 2020)¹¹³, had romanticized about the caliphate and this was no different, went the logic. As a result, the extent of its zeal and ambition went ‘largely unnoticed’ or ignored in the West (Bunzel 2015, p. 4). Where it was noticed was by downtrodden Muslims in Iraq and Syria who had traditionally been forced to emigrate to Europe or America because only two out of the 57 Muslim-majority countries, Turkey and Malaysia, offered formal paths for immigrants to become naturalised citizens. Now there was a viable alternative. Islamic State offered immigrants ‘citizenship’ upon arrival and issued caliphate ‘passports’ on the spot, inculcating a strong sense of belonging (Liang 2015, p. 3). The conflict in Syria and Iraq was now ‘the largest mobilization of foreign fighters in Muslim majority countries since 1945’, larger even than Afghanistan in the 1980s (Neumann 2015). Almost overnight it had ‘turned US policy in the Middle East upside down’ (Byman and Williams 2015). Even in Arab countries where Islamic State did not have a significant presence, its rise was radicalising the poorer population and fomenting sectarianism. In the end, it was a struggle for power and authority that split Al-Qaeda in Iraq from Al-Zawahiri’s Al-Qaeda core. Al-Zawahiri proclaimed Jabhat al-Nusra to be the official Al-Qaeda affiliate in Syria and AQI to be the official affiliate in Iraq. Baghdadi refused to accept

¹¹³ El Damanhoury (2020) talks about ‘a branding competition over the caliphate’ between Islamic State and Al-Qaeda.

that decision and declared Jabhat al-Nusra subordinate to him. In response, Al-Zawahiri publicly disavowed Al-Baghdadi's group in February 2014. So, when Abu Bakr al-Baghdadi declared the caliphate on June 29, 2014, he 'split the fractious jihadist movement' and sparked 'jihadism's global civil war' (Byman and Williams 2015). 'The two are now competing for more than the leadership of the jihadist movement', wrote Byman and Williams. 'They are competing for its soul'.

Even in such a complex setting, the reasons for the defeat of the Islamic State insurgency are 'relatively straightforward' (Phillips 2018, p. 258). Despite the breathless media coverage driven by its calculated barbarity, it remained no more than a well-resourced non-state actor. Most importantly, it had no air power, which tactically 'enhances military firepower and manoeuvrability and is critical to battlefield success' (Saunders and Souva 2020). So while it 'thrived in the chaos in Iraq and Syria in 2013-2015 when the state governments were disunited and distracted' (Phillips 2018, p. 258), this changed significantly when first the US and later Russia refocused and built the on-the-ground alliances necessary to challenge and finally defeat it in 2019. By now, the Western allies were beginning to understand the chameleon-like nature of the network they were dealing with, and realized that even defeat left open 'the possibility that in the right circumstances, ISIS, or a variation of it, might return'. It had already transformed itself from a terrorist group into a proto-state and thence into an insurgent force. The US Department of Defence estimated that as many as 30,000 fighters remained at large in Iraqi and Syrian 'cells' ready to 'launch hit-and-run terror attacks' (Phillips 2018, p. 259). In fact, such attacks were to become 'a common occurrence'. For instance, in May 2018, a year after Islamic State had been forced out, an attack on Mayadin in eastern Syria killed 26 Syrian and nine Russian soldiers. Similarly, in January 2019, 15 civilians and four Americans were killed in an Islamic State suicide bomb attack in Manbij, which was controlled by the SDF. Ironically, the Manbij attack came just a few weeks after President Donald Trump tweeted that Islamic State was 'defeated'. At the same time, European cities continued to live in fear of unpredictable single-actor attacks. On December 11, 2018, the year was brought to a close when a man with a revolver and a knife killed five and wounded 11 at the Christmas market in Strasbourg. He was killed in a shootout with police two days later. A high-performing mission-driven complex adaptive system, Islamic State continued to transform itself in response to its changing environment.

Test 2: Islamic State – social media and autonomous communication

In Test 2, it is essential to find (i) evidence of its pursuit of autonomous communication by Islamic State, specifically (ii) in its adoption of social media which it used not alone to amplify its messaging but to empower loosely affiliated jihadists to launch lethal attacks independently, thereby influencing the strategic direction of the organisation through co-evolution.

Islamic State and the emergence of social media

Internet-based social media emerged at around the turn of the millennium. They began in the form of blogging and initially seemed like little more than a novel offshoot of the ‘usernets’ of the late 1970s (WDD 2009), with – in an extraordinary architectural reflection of the jihadist networks themselves – no centralised servers or dedicated administrators. They began to develop more rapidly in 2006 with the arrival in earnest of Facebook, Twitter, and YouTube. Social media were web-based, mobile-first technologies that turned communication into an interactive dialogue (Cohn 2011). In technical terms, they were Web 2.0 applications, websites based solely on interactive user-generated content (Dean et al. 2012, p. 4; Kisselburgh et al. 2010; Sharma 2008). The production, sharing, and viewing of that content led frequently to collaboration among users based on common interests, political ideologies, or often something as simple as a shared geographical location (Wooley et al. 2010). In that sense, with 2.8 billion users worldwide at the end of 2018, social media enabled and amplified social networking, giving it global reach and the capacity to disaggregate endlessly. Mark Zuckerberg, for instance, saw Facebook as an ‘open social utility’ (Murphy 2020). He was correct that in marketing terms social media were something new: a cheap and effective tool of mass communication, and, in particular, a highly effective method of targeting specific demographics (Hindman 2018; Dean et al. 2012, p. 5; Earl and Kimport 2011, pp. 63-120). This was the lesson of social media that terrorist users learned even more rapidly than they had learned to adopt the internet. Social media, essentially ‘made of’ interaction, its users comprising an ever-expanding non-linear constellation of nodes with no discernible patterns of use, constantly changing and therefore totally unpredictable, amounted to a whole new array of weapons for digital-native terrorist networkers.

Here again, scale and speed came into play. Having been confined initially to students, Facebook opened to all comers in September 2006. By January 2009, it had 175 million users, rising to 500 million by July 2010, just 18 months later. By January 2018, that figure had risen to 2.2 billion users (Facebook 2018; Constone 2017). Twitter was launched in March 2006. The following year, an average of 5,000 tweets was posted every day. In 2008, that number was 300,000 a day, rising to 340 million tweets a day by 100 million users in 2010. On November 8, 2016, the day of the US presidential election that returned Donald Trump, Twitter was the largest single source of breaking news, with 40 million election-related tweets sent by 10 pm, far exceeding the 31 million sent on election day 2012 (Isaac and Ember 2016; Beaumont 2010). The rush was not just to Facebook and Twitter. By January 2009, every minute of every day 10 hours of fresh content was being uploaded to the video-sharing platform, YouTube, while Flickr users were already sharing a total of more than three billion photographs. By the second quarter of 2008, such was the stampede to the new technology that 75 percent of internet-surfers used social media in one form or another, up from an already-impressive 56 percent in 2007, according to US analysts, Forrester Research (Kaplan and Haenlein 2010, p. 59). By McLuhan's measure of the 'new scale' introduced into users' affairs by this evolving technology (McLuhan 1967, p. 15), social media were, as the internet had been, transformative. There were initial concerns among terrorist networks about the operational security of social media on the grounds that 'user-generated content imperils message control' and that 'social networking renders jihadists vulnerable to detection, surveillance, and arrests' (Kimmage 2010, p. 15). On both counts, they were correct (Holden 2017; Price and Al-'Ubaydi 2017; Weimann 2010, p. 49). That caution, however, was short-lived. By April 2006, former FBI counterterrorism expert Evan Kohlmann reported that 'more than 90 percent of terrorist activity on the Internet now takes place using social media networking tools' (Noguchi 2006). This was to some extent to evade countermeasures, but primarily because the terrorists' audience had already followed the trend to social media.

Islamic State: the weaponisation of social media

One of the little-known effects of constant interaction with more and more powerful technology is that time appears to speed up. This is partly a function of the evolutionary facts that (i) the brains of 'digital natives' (Tamturk 2017) are becoming more efficient at processing information, and that (ii) faster technology does indeed, in many ways, mean a faster more technocentric world (Macdonald 2015). In its co-evolution with information technology, Islamic State capitalised on the combination of those facts by using powerful new social media to 'activate a sense of "apocalyptic time" among its supporters online' (Berger 2015, p. 61). Berger acknowledges a debate about whether Islamic State leaders were inclined to this way of thinking because they were 'true believers' or because they were employing apocalyptic ideas instrumentally. He takes the view that while it is not possible to answer the question in relation to the leadership with any certainty, it is possible to say that at 'at footsoldier level' a significant number of adherents believe in its apocalyptic aspects and that these are 'an important component of its multifaceted appeal'. Either way, it activates that sense of apocalyptic time by

instilling a sense of temporal acceleration and imminent arrival of end-times scenarios, leveraging the dynamics of social contagion and remote intimacy on beliefs that have an inherently viral appeal, and providing a vehicle for supporters outside its territories to immerse themselves in a highly idealized version of its millenarian project, the so-called caliphate. The Islamic State is the first group to employ these amplifying tactics on social media at an industrial scale, but it will likely not be the last. (Berger 2015, p. 61)

Interestingly in terms of his description of apocalyptic beliefs in their historical setting, Berger (2015, p. 62) says they have been 'historically understood as viral, or more specifically contagious', where 'viral' is a word more usually used nowadays as in relation to information technology. He notes that apocalyptic beliefs are particularly significant in the case of Islamic State for three main reasons: because (i) they have a tendency to spread swiftly through well-defined social networks (Landes 2011, p. 9 and p. 55); because (ii) the most committed apocalyptic believers can be extremely fanatical, 'with a high tolerance for violence and heightened will to act' (Robbins and Palmer 1997, p. 16), and because (iii) apocalyptic believers are frequently unwilling to abandon their beliefs in the face of contradictory evidence and may become even more committed, and potentially violent, when their movement is faced with setbacks (Festinger et al. 1964, p 8). Landes (2011) gives this strikingly complex description of the phenomenon:

These voluntary apocalyptic communities are temporal hothouses, brief moments when a self-selecting group of strangers comes together in circumstances where all 'normal existence' ceases and a series of interlocking and energizing paradoxes come to life ... The shorter the temporal horizon, the more intense the apocalyptic expectations become. (Landes 2011, p. 13-17)

In terms of *how* social media amplifies and facilitates the transmission and inculcation of apocalyptic beliefs, Berger (2015, pp. 62-68) identifies three key mechanisms. *The first is temporal compression*, the belief that prophesied events preceding or accompanying the end of history are imminent or already underway, and that the clock is literally running out. Social media helps to accomplish this through the pace of postings and updates relative to older forms of media. 'The pace of posting on Twitter', for example, 'serves as a kind of metronome', says Berger (2015, p. 63). By following even a modest number of Islamic State supporters online, an individual can receive thousands of messages a day promoting its accomplishments. The pace accelerates around significant developments, stepping up the intensity of the experience. Deceleration occurs after such events. Account suspensions also limit the growth of the network, but the pace of output never approaches zero. 'Thanks to the overall volume of activity, a sense of immanence is easy to achieve' (Berger 2015, p. 63). *The second mechanism is social contagion*, which results when 'intense social contact and prolonged interaction spreads apocalyptic memes in an impactful, life-changing manner'. References to the 'contagion' of Christianity can be found in the Roman writings of the second century CE. In the case of Islamic State, it is possible because social media empowers rapid contact over wide geographical areas. 'The most significant factors empowering this speed are technological – the vastly increased mobility allowed by modern transportation, the rise of socially networked global communities via cheap, instantaneous and easy-to-use communication technologies' (Berger 2015, p. 64). *The third mechanism is immersion*, 'the diminishment and eventual replacement of normal existence with a heightened experience of an alternate interpretation of reality' (Berger 2015, p. 62). This is achieved by combining the sheer volume of Islamic State's media output with its 'always-on' online transmission, and gives a sense of 'remote intimacy'. This thesis argues, however, that while all three – temporal compression, social contagion, and immersion – are certainly fascinating to-the-point descriptions of how Salafi jihadists use millenarianism to their benefit, the key relationship at work is co-evolution. Berger (2015, p. 65) maintains that social media are more effective at promoting millenarianism than previous technologies because they allow both 'community

discovery' and peer-to-peer communication. Also into this mix goes the fact they 'may also be organically suited to advancing extremist indoctrination among vulnerable audiences', because (a) its length limitations lend themselves structurally to the simplification of narratives, and (b) 'the always-on mobile technology of the 21st century allows for a continuous connection to others who share the same extremist views, providing reinforcement and personal validation' (Berger 2015, pp. 68-69). While all of these are undoubtedly aspects of the complex set of relationships Berger describes, what is fundamentally at play here is (i) the co-evolutionary relationship between Islamic State and social media as a new iteration of information technology; (ii) the evolution of that technology from 'facilitative tool' (Conway 2017) to 'digital replicator' (Gillings et al. 2016, p. 7; LaBar et al. 2016) explaining, by virtue of the greater interoperability that that phase transition allows, the extraordinary new scale of the social media networks or 'communities' it generates, and (iii) the co-evolutionary 'symbiotic relationship' between that powerful new technology and scale and the mission-driven network-structured millenarian terrorists of Islamic State.

Islamic State and autonomous communication

Islamic State came into being with autonomous communication – in the limited sense of the capacity to control its own messaging – as an operational priority in the genes it inherited from Al-Qaeda. This thesis argues, however, that autonomous communication in its fullest sense, in the context of Islamic State and social media, entails not alone the amplification of messaging but the empowerment of followers with only marginal links to the network to launch attacks autonomously without reference to Islamic State core. In that sense, the capacity of terrorists to strike reflects the architecture of the information technology by which they are linked and empowered, in this case social media. In the case of Islamic State, this explains the rash of largely single-actor or single actor-instigated attacks across Europe attributed to Islamic State between 2014 and 2018. It also underlines the meaning of acts of terrorism as acts of communication (Jenkins 2015). However, while senior Islamic State commanders such as Abu Muhammad al-Adnani (Cluskey 2016) were certainly conscious of the imperative to maximise the competitive edge available from any new iteration of information technology, it must be likely that this was the limit of their understanding of the co-evolutionary mechanism between them and their technology. Certainly, Abu Mus'ab al-

Zarqawi realised from the start that ‘reality is no match for perception’ (Singer and Brooking 2018, p. 153). For that reason, as *emir* of AQI, he developed his trademark brutality, even in the face of opposition from Osama bin Laden and Ayman al-Zawahiri who did not wish to alienate the Muslim mainstream, as a means of amplifying his message of dominance. It was for this reason too that his brutality in Iraq specifically was aimed strategically at fomenting civil war between Iraq’s Shia and Sunni populations, and that the beheading of James Foley in August 2014, in an orange Guantanamo Bay-style jumpsuit whose symbolism was clear to all, was staged as a direct challenge – in actual fact, a taunt – to the Obama White House, whose medium-term aim was withdrawal from Iraq. When a video clip of the killing, entitled ‘A Message to America’ and addressing Obama by name, went viral on the internet, propelled by some 60,000 social media accounts, almost overnight American public opinion shifted back to favouring further intervention. That tweet, observe Singer and Brooking (2018, p. 151) was ‘among the cheapest, most effective, declarations of war in history’. Through this carefully planned stratagem, enabled by social media, Islamic State had reversed US public opinion and to an extent reversed the clearly enunciated policy of the White House, which launched its first airstrikes against Islamic State on September 23 (Wilson Centre 2019). This constant search by the jihadists for the latest and most effective iteration of information technology is underlined too by the fact that Al-Zarqawi ‘dismissed’ satellite technology immediately there was a better option with virtually unlimited reach in the form of the internet (Lynch 2006, p. 53).

That constant scanning of the technological horizon for powerful new co-evolutionary partners made it inevitable that Islamic State would encounter and become early adopters of social media, taking full advantage of the ‘increased network centrality and power’ which that investment gave them (Burkhardt and Brass 1990, p. 107). It employed the amplifying tactics of social media on ‘an industrial scale’ (Berger 2015, p. 51). This contributed significantly to the fact that it was able to mobilise an estimated 40,000 nationals from 110 countries to join its ranks (Ward 2018). Such an unprecedented rush of support gave European intelligence services more jihadists and potential jihadists to monitor than ever before, and raised new concerns about domestic radicalisation (Europol 2016). While historical data shows that only about 11 percent of European fighters who travelled to join various conflicts in Muslim countries, such as Bosnia in the 1990s and Afghanistan, Iraq, Somalia and Yemen in the 2000s,

became international terrorists, those who did tended to be the more capable and committed who 'contributed to making the threat higher' (Nesser 2019, p. 16). Because of those characteristics, 'many of them played roles as terrorist entrepreneurs: recruiting, organizing, training, and directing attack cells'. Such operatives frequently had important roles in staging high-profile attacks, such as the Bataclan attack by Islamic State in Paris in November 2015, or directing attacks via encrypted messaging apps, as happened in the truck attack by 39-year-old Uzbek asylum seeker Rakhmat Akilov in Stockholm in April 2017, in which five people were killed and 14 seriously injured (Reuters 2017). At the same time, Islamic State was flexible. It modified its attacks so as to avoid detection, which is why, between 2014 and 2017, a higher proportion of attacks involved simple weapons such as cars and knives. Similarly, in the same period, nearly half of plots involved single actors rather than groups. 'Single actors with simple weapons are notoriously difficult to stop' (Nesser 2019, p. 17). The strength and nature of links between plotters and Islamic State networks have varied, but plots without contacts to networks are 'very rare in European jihadism'. The reason countries such as France, Belgium, Germany, and Britain have had so many Islamic State plots is that they have had jihadist networks of varying degrees of substance since the 1990s when the first foreign fighters left for Syria. The main recruitment platform for Islamic State in Europe was a network that grew out of UK-based Al-Muhajiroon, which initially supported Al-Qaeda and mobilised a new generation of European jihadists during the 2000s (Lowles and Mulhall 2013). Each of those fighters had the potential to become a lone attacker loosely affiliated via social media with an unprecedented reservoir of jihadist inspiration.

Test 3: Islamic State and the force multiplier effect of social media

In Test 3 it is essential to trace the manner in which co-evolution with social media had a force multiplier effect for Islamic State, (ii) particularly in the period from its capture of Mosul on June 10, 2014 and continuing through its blizzard of attacks in Europe between 2014 and 2018.

Islamic State's capture of Mosul: 'blitzkrieg' in northern Iraq

In terms of its force multiplier effect, each of the social media developed a distinct terrorist purpose (Dean et al. 2012, pp. 5-10). Facebook was used primarily for recruitment

(Department of Homeland Security 2010; Torok 2010), deploying the 'groups' function to attract sympathisers from all over the world without any significant threat to the organization. From the group, potential recruits were then directed to the organization's website or to forums used for indoctrination and training (Al-Shishani 2010; Weimann 2010). Twitter, by contrast, was used for instant messaging during the 2008 Mumbai attacks by Lashkar-e-Taiba, which left 164 people dead (O'Rourke 2010; Rabasa et al. 2009; Leggio 2008). Interviews with the sole surviving attacker, combined with telephone intercepts, showed that the terrorists' controllers in Pakistan were able to provide them with a constant flow of information from public Twitter posts, including tactical information about Indian counter-terrorism units planning an assault on the hotel at the centre of the attacks (Dean et al. 2012, p. 8). It was similarly used by Al-Shabaab during the Westgate attack in Nairobi in 2013 (Mair 2016). Its immediacy meant it emerged at its height as 'terrorists' favourite Internet service' (Weimann 2014, p. 8). Because of the attractiveness of video as a means of communication, YouTube also became popular, featuring, for instance, bomb-making videos and videos demonstrating the use and field-stripping of an AK47 (Dean et al. 2012, pp. 9-10; Department of Homeland Security 2010). In terms of proselytizing, Yemeni-American imam Anwar al-Awlaki¹¹⁴ posted more than 5,000 videos carrying extremist messages on YouTube alone, while he was also active on Facebook (Meleagrou-Hitchens 2011; Barclay 2010; Madhani 2010; Torok 2010; Shephard 2009; Smith 2009). All of these operational activities would have been incalculably more dangerous, more time consuming, and more demanding of manpower prior to social media. To place social media in its jihadist context, Yelin (2013, p. 4) identifies four phases in jihadists' use of media, and traces the arc of that evolution. Phase 1, beginning in 1984, comprised *khutbas* (sermons), essays and pamphlets, magazines/newsletters, and videotaped lectures or battle scenes. Phase 2, in the mid-1990s, was the move to websites, centralized endeavours with a monopoly on content and distribution. Phase 3, in the mid-2000s, brought interactive online forums which could 'steer' an online community. Phase 4, in the late 2000s, were social media platforms, where '... individuals, not the organization, decide what is important and what they believe should be given the most attention'. This last was the rapid disaggregation of jihadist networks into the impromptu army of individual attackers, supported where necessary, who would claim hundreds of lives in Europe from

¹¹⁴ In Yemen, Al-Awlaki became the first US citizen killed by a US drone on September 30, 2011 (BBC News 2011).

2014 to 2018. The terrorists were acting in the likeness of their preferred information technology, social media. Once again, the medium was the message.

Nothing exemplified Islamic State's brazen exploitation of social media, specifically Twitter, as much as its 'blitzkrieg-like advance' across northern Iraq (Price and Al-'Ubaydi 2017) towards Mosul, a 3,000-year-old metropolis of 1.8 million people. Far from keeping their advance secret, it was accompanied by a highly choreographed social media campaign using the promotional hashtag #AllEyesOnISIS. An army of Twitter bots posted images of black-clad militants with AK47s, grenades and occasionally even swords (Singer and Brooking 2018, pp. 4-7). Its capture shocked the world, largely because while the Iraqi army had some 30,000 men and roughly an equal number of police, they were confronted by just 1,500 or so Islamic State fighters. Between June 4 and June 10, the Iraqi forces 'turned and ran' (Chulov et al. 2014). Their morale had been undermined by images on Twitter and Instagram showing mass killings of their comrades, a forceful example of 'gaming' social media to magnify their message (Berger 2014). On June 10, when the jihadists marched into the city, they emptied the Al-Qayara army base – the fourth largest in the country – of weapons and ammunition, Humvees and rockets, seized its helicopters, opened the gates of the city's jail, and stole a reputed \$480 million in banknotes (Chulov et al. 2014). They immediately posted images of their spoils online. Their victory was marked by almost 40,000 supporters' tweets in a single day (Berger 2014). This was made possible by its Dawn of Glad Tidings Twitter app, which posted tweets, together with hashtags, links, and images, to the accounts of those supporters, who then tweeted them on. The 'Dawn' app spaced its mass posts in order to avoid triggering Twitter's spam detection algorithms (Berger 2014). In a 'lightning' campaign accompanied by followers 'loud and noisy, tweeting, streaming and Instagramming their exploits' (Liang 2015, p.2), they also encircled the city of Deir el-Zour in Syria, took the city of Tikrit, Saddam Hussein's birthplace, in Iraq, and halted at Iraq's largest oil refinery at Baiji, whose power stations supply the region. Crucifixions¹¹⁵ posted on Twitter became routine as a warning to local people not to oppose them. 'The advance of an army used to be marked by war drums', wrote Berger (2014). 'Now it's marked by volleys of tweets'. Singer and Brooking (2018, p.4) reported that 'the invasion was launched with a hashtag', adding (2018, p. 219): 'There's no

¹¹⁵ This image is of the crucifixion by Islamic State fighters in Deir el-Zour, Syria, of a policeman with the Assad regime: <https://twitter.com/conflicts/status/528182391349972993>

historical analogue to the speed and totality with which social media platforms have conquered the planet.’ At this point, the fall of Baghdad seemed imminent. It did not happen. In that case at least, reality was no match for perception. On July 4, 2014, Islamic State leader, Abu Bakr al-Baghdadi, ascended the pulpit of Mosul Grand Mosque, declared victory and underlined the dominance of the restored caliphate (Maher 2017, p. 3).¹¹⁶ This was co-evolution between Islamic State and social media in full flower. As if gauging its force multiplier effect, Liang (2015, p. 2) observed: ‘Terror is now being transmitted across the globe in real time’. In his analysis of the pros and cons of why the US finally authorized air strike against Islamic State, Phillips (2018, p. 207) writes simply: ‘Obama hadn’t believed that ISIS were equivalent to the al-Qaeda network but the Mosul takeover changed his mind’.

How social media enabled Islamic State’s reign of terror in Europe

Islamist terrorism propagated in Europe now had Europe in its sights. In line with the initial tendency to underestimate Hezbollah (Cordesman 2006, pp. 38-39), and the glaring underestimation of Al-Qaeda by Western intelligence services before 9/11 (Duffield 2002, p. 157), the jihadist threat in Western Europe, and Belgium in particular, was also ‘largely underestimated’ before what would transpire to be multiple lethal attacks on European soil (Van Ostaeyen 2019, pp. 10-11). Although the idea that these attacks were so-called lone wolf attacks, perpetrated by individuals, sometimes self-radicalised, with no logistical or other support, has turned out to be ‘a myth’ (Gaub 2017, p. 2), the importance of social media in projecting violent extremist propaganda and recruiting fighters is well documented (Ward 2018). Its force multiplier effect in terms of (i) what may almost be described as auto-recruitment, in the sense that social media are by nature interactive and motivational among networks that attract individuals in search of a mission-driven radical community (Hosen et al. 2021), and (ii) its psychological impact in terms of engendering not just fear but terror on both the real and the virtual battlefields, cannot be overestimated. Time after time, Islamic State-inspired attacks shook entire countries to their core. These attackers were not alone frequently born in Europe but ‘truly European’ in the sense that ‘terrorists form networks, exchange funds and information across borders, and can live in one European country,

¹¹⁶ Mosul was recaptured by Iraqi government forces on July 10, 2017 (Sahay and Garge 2017).

perpetrate an attack in a second, and hide in a third' (Gaub 2017, p.2). Although radical groups such as Sharia4Belgium were openly exploiting what they called 'recruitment labs' such as Brussels, they were largely ignored by government and media (Van Ostaeyen 2019, p. 7). Rather than regarding their presence as evidence of the need for a pan-European counterterrorism response to the conflicts in Iraq and Syria, one Belgian official referred to these radicals as 'clowns in white gowns whom we should ignore' (Knack 2016 cited in Van Ostaeyen 2019, p. 7). On May 24, 2014, just one month before the capture of Mosul, the first attack happened in Brussels when a lone gunman opened fire at the Jewish museum of Belgium, killing four. A second man was subsequently convicted of supplying him with weapons. The gunman was later identified in court as an Islamic State member who had imprisoned and tortured two French journalists in Syria in 2013 (Rawlinson 2014).

Reviewing the main European attacks gives some idea of that scale and the multiplier effect they provided for Islamic State. There had been two Islamic State attacks in the Middle East – the Metrojet bombing with the loss of 224 lives as it left Sharm el-Sheikh airport on October 31, 2015, en route to St Petersburg, and the double suicide bombing in a Shia suburb of Beirut on November 12, in which 43 people died, the worst such attack since the end of the Lebanese Civil War – before the three co-ordinated Paris attacks on November 13, with a death toll of 130 and 416 injured. The first group of three suicide bombers struck outside the Stade de France. The second opened fire on crowded cars and restaurants and the third carried out a mass shooting and took hostages at a concert attended by 1,500 people at the Bataclan theatre. In just one example, video footage filmed from a nearby apartment was posted on YouTube and received 2.1 million views in less than 20 hours (Mercier 2015). This gives one tiny example of the enormous scale of the amplification online. There followed on March 22, 2016, the Brussels metro and airport attacks in which 34 people were killed and 340 injured. A French police officer was stabbed on June 13, and on July 14 the Nice truck attack killed 86. On December 19, a copycat Berlin truck attacked killed 12 and injured 56. Similarly, on March 22, 2017, a car ploughed into pedestrians at Westminster in London and the assailant stabbed a policeman to death. In all, six were killed and 49 injured. The following month, on April 7, a Stockholm truck attack killed five and injured 15. In that attack, for example, Rakhmat Akilov, shared images of his target beforehand and received the green light from his Islamic State contacts via encrypted message (Bergen et al. 2019). In the meantime, there had been the

Würzburg train attack in Germany on July 18 in which five people were stabbed and injured by a 17-year-old Afghan refugee, and the Normandy church attack on July 26 in which two men killed an 85-year-old priest and critically wounded an 86-year-old man before being shot by police. On April 20, three policemen were shot on the Champs-Élysée in Paris; one died. On May 22 came the Manchester Arena suicide bombing with 22 dead and 59 wounded. On June 3, the London Bridge attacked left eight dead and 48 wounded. On August 17/18, 2017, in Barcelona, 16 were killed and 152 injured when a 22-year-old jihadist drove a van into pedestrians in the Las Ramblas precinct of Barcelona (Igalada 2021; Bourekba 2018; Tremlett et al. 2017). He escaped but was subsequently shot dead. Nine hours later, five more from the same cell drove into pedestrians in the nearby town of Cambrils. All five were shot dead by police and two more were killed, including the imam believed to have been the mastermind, when a bomb they were preparing accidentally detonated. They were the deadliest attacks in Spain since the 2004 Madrid train bombings directed by Al-Qaeda in Iraq. There were other attacks in 2018, 2019 and 2020, but it is not possible to list them all here, and the death toll has diminished over time. However, in terms of force multiplier effect, attacks have been amplified and digitally replicated time out of number, and the psychological impact is imprinted on the global psyche. 'The extensive coverage of terrorist attacks through multiple media and social media channels has led to an exponential growth of eyewitnesses to terror attacks', write Hafner et al. (2018) in their analysis of the 'cost' of jihadist terrorism in Europe. 'This means that even those not directly involved in attacks may be psychologically affected.'

Islamic State: The aftermath and what has changed

Islamic State's social media high was in 2014 and 2015, the launch pad from which it was poised firstly to capture Mosul and then to terrorise Europe with its relentless series of arms-length attacks. In response, the US began airstrikes in Iraq in August 2014 and in Syria the following month (Wilson Centre 2019). By December 2017, Islamic State had lost 95 percent of its 'caliphate', including its two largest cities, Mosul in Iraq, and its nominal capital, Raqqa, in northern Syria. On December 9, Iraqi prime minister Haider Al-Abadi declared victory over the insurgents. However, the reality was that even at this stage Islamic State-inspired attacks were a frequent occurrence. The last in Europe was in Marseilles, on October 1, 2017, when

two women, cousins of 20 and 21, were stabbed to death by an illegal immigrant from Tunisia in his twenties. The last in the United States was in New York, where eight died and 12 were injured when a rented pick-up truck was driven through cyclists and joggers for 1.6 kilometres along the Hudson River. The attacker's mobile phone was found to contain some 90 videos and 4,000 images of Islamic State-related propaganda, which he told police had 'inspired' him. It was the fifteenth vehicular attack by jihadists in America and Europe since 2014, with a total death toll of 142. It was the deadliest attack in New York city since 9/11 (Chavez, Yan, Levenson and Almasry 2017).

As Islamic State was forced to relinquish its territory and the inspiration for its campaign of individual attacks unwound, so the scale of its production and posting of propaganda content began to fall off. That was due to the direct targeting by Western forces of its cyber apparatus and, particularly, of its social media strategists during the summer of 2016, when Abu Mohammed al-Adnani and Wa'il al-Fayad, both senior figures, were killed in US strikes. Internet and social media companies also came under increasing pressure to prevent Islamic State from using their platforms. The effect was striking: between September and December 2014, there were somewhere between 46,000 and 90,000 active pro-Islamic State Twitter accounts, whereas between February and April 2017 there were fewer than 1,000 accounts with a minimum of one follower (Conway 2017). Islamic State's previously strong and vibrant Twitter community was by then 'virtually non-existent'. There followed migration to WhatsApp and to Telegram channels where, interestingly in terms of autonomous communication, 'owners' have more control over who joins. What this evolutionary trajectory begins to reveal in terms of the technological footprints from satellite to online to social media, is that each new iteration represents a step towards 'complex global microstructures' (Knorr Cetina 2005, p. 215), 'new terrorist societies' that 'cannot simply be reduced to networks' because they are 'more textured' and 'exhibit temporal complexity'. While microstructures are on some level organised or co-ordinated systems, Knorr Cetina (2005, p. 215) says, the co-ordinating elements are not of the kind associated with formal authority, complex hierarchies, rationalised procedure, or deep institutional structures. This is perhaps the level of microstructure represented by Islamic State-inspired independent attackers, and reflects the much-analysed complex relationship – or lack of it – they have with Islamic State core.

Test 4: Estimating the causal credibility of co-evolution

The purpose of this section is to review Tests 1, 2 and 3; to examine the extent to which Islamic State displays the qualities identified in each test as characteristic of a complex adaptive system, and, using the NATO estimative probability standards, to assess the degree of causal credibility attached to co-evolution as the most likely explanation for the symbiotic relationship between Islamic State and social media. Whether that judgment can plausibly be made on the basis of the evidence adduced thus far, and its causal credibility confirmed using the NATO standard, constitutes Test 4.

Test 1 Reviewed: Islamic State as complex adaptive system

In Test 1, it was essential to find in Islamic State (i) a networked organisational structure that is central to its development, and (ii) convincing traces of CAS behaviour.

If Al-Qaeda was a networked non-linear organisation, Islamic State was even more so (Clarke et al. 2017). It shared the same roots with Al Qaeda in the mujahideen of Afghanistan, but came of age as a hybrid force independent of its predecessor by earning a well-justified reputation for strategic brutality in the highly unstable battlefields of Iraq and Syria, always pursuing its overarching aim of a Sunni theocracy (Laub 2021). In an environment whose worst excesses were characterised by a UN spokesman as ‘a complete breakdown of humanity’ (Barnard 2016), Islamic State was utterly at home and motivated, thriving on chaos, on unbridled violence, and on rapidly transmuted and often short-lived alliances. There could not have been a more appropriately hellish setting for its millenarian project, driven by its Salafist belief in ‘progress through regression, where the perfect life is realised by reviving the Islam of its first three generations’ (Maher 2017, p. 207). War is ‘a non-linear phenomenon’ (Solvit 2012, p. 73) and as a non-linear organism, Islamic State matched it as the perfect co-evolutionary partner. Its networked architecture, and the speed with which that enabled it to adapt and evolve, marked it as a high performing complex adaptive system, where ‘ideas from outliers can be quickly assessed and assimilated and exogenous shocks can be distributed’ (Hayden 2013, p. 20). Such a shock was the targeted killing of its leader.

By the time Abu Mus’ab al-Zarqawi was removed, his network had grown agile and unpredictable, key qualities of complex adaptive systems which are resilient enough to

survive the removal of any individual node. It had built its brand on brutality, and now it strengthened that brand by switching from its trademark suicide bombings to beheadings of foreign hostages in order to reach into centres of Western power, including the Obama White House, to monopolise the political agenda. Leveraging the reach of social media to amplify the shock of those killings, it learned that it could project its rampant power across the globe with minimal effort, even though the reality of that threat was no match for the perception. This carefully cultivated illusion is what led Iraqi troops to flee as black banners engulfed Mosul in June 2014 to a global chorus on Twitter. Another complex illusion of power was created by the ability of lone actors with only marginal contact with Islamic State core through social media to act on its behalf in a manner reflecting the architecture of the technology.

Assessment

While Hayden (2013) does not include Islamic State in her analysis of terrorist networks as complex adaptive systems, she does – as noted in Chapter Five – find numerous convincing characteristics in its predecessor, Al-Qaeda (Hayden 2013, pp. 11-19). However, given the complex relationships just described, in particular its oneness with such an unpredictable battlefield and its mission-driven leveraging of interactive social media, the likelihood that (i) its networked structure has been central to its development is rated ‘highly likely’ (more than 90 percent). The likelihood that (ii) this analysis of Islamic State has shown convincing traces of CAS behaviour is also judged highly likely.

Test 2 Reviewed: Social media and autonomous communication

In Test 2, it was essential to find in Islamic State (i) evidence of its pursuit of autonomous communication, specifically (ii) in its adoption of social media, which it used not alone to amplify its messaging but to empower arms-length sympathisers to launch independent, almost unforeseeable, attacks in the name of the organisation.

There is no doubt about the power of the commitment to the potential of new iterations of information technology shared by the leaders of Al-Qaeda, Osama bin Laden and Ayman Al-Zawahiri, and by Abu Mus’ab al-Zarqawi when he became emir of Al-Qaeda in Iraq (Lynch 2006, pp. 50-51). All three, along with others at a senior level within what would become Islamic State, in particular Abu Muhammad al-Adnani, were fully aware of the force multiplier effect to be gained by exploiting media technology to its fullest. What was new as a result of

the internet was that jihadist groups were able to distribute video of beheadings around the globe at the press of a 'send' button. This immediately allowed them to bypass the editorial safeguards that would have been – and remain – in place in traditional media. So that while (i) satellite television granted some autonomy in that Hezbollah was able for the first time to broadcast its propaganda over the border into Israel, and (ii) the internet went hugely further in that it wiped out Al-Qaeda's dependence on traditional media almost overnight, now (iii) social media went a step further again and enabled Islamic State followers all over the world to redistribute the clips of video among their own networks, creating an unstoppable cascade that piggybacked atop the already-formidable power of the internet. Not alone was the reach of social media new and unprecedented, as each successive iteration of information technology typically is, but the content went one step further than the internet in terms of being unmediated: it remained unmediated at every point as it was replicated through social media users' networks. What was posted was what was seen, shock value intact. Each and every social media user was now 'a potential target of postmodern conflict' (Fukuyama 2018).

Given that terrorism is fundamentally about communication, one can see the blizzard of attacks by lone operatives that swept across Europe with a ferocious intensity from the end of 2014 until the end of 2017 and beyond, as a new and emerging species of autonomous communication as well. A high percentage of those attacks appear to have been staged without significant input from Islamic State core. In the relatively large-scale Barcelona attack, for example, none of the eight attackers¹¹⁷ was a known terrorist. Despite this, or perhaps because of it, they succeeded where others had been intercepted by the Spanish intelligence services (Igalada 2021). These attacks marked, in effect, the disaggregation of jihadist networks into an impromptu army of individual attackers, supported where necessary to a greater or lesser degree by Islamic State core. They were a reflection of the last of Yelin's four phases in jihadists' use of media, their use of social media platforms, where '... individuals, not the organization, decide what is important and what they believe should be given the most attention' (Yelin 2013, p. 4). Not alone had terrorist networks achieved autonomy of communication, but newly radicalised individual terrorists themselves now had the autonomy to plan, strike and inflict multiple fatalities without any reference to a directing organisation.

¹¹⁷ Known as 'the Ripoll cell' after the town where the imam leading the Barcelona attackers settled after leaving prison in 2014 (Igalada 2021, p. 66).

Assessment

Given the well-documented stress placed by Islamic State on information technology, first the internet and then social media, and the manner in which they openly used it to recruit, inspire and sometimes direct new followers and to cheerlead attacks, the likelihood that it was in pursuit of autonomous communication is rated 'highly likely' (more than 90 percent). The likelihood that its pursuit of autonomous communication explains its leveraging of social media is also judged 'highly likely'.

Test 3 Reviewed: Islamic State and the force multiplier effect of social media

In this test, it is essential to trace the manner in which co-evolution with social media had a force multiplier effect for Islamic State, (ii) particularly in the period from its capture of Mosul on June 10, 2014, and continuing through its blizzard of attacks in Europe until the Barcelona attack in August 2017, in which 16 civilians and eight terrorists died.

The force multiplier effect of social media for Islamic State was self-evident to the extent that it occurred, quite calculatedly, in the public domain. Terrorism apart, while telegraphy had taken at least two generations to develop (Hurdeman 2003, pp. 67-69), and even the internet had been in gestation for decades in various US government technology laboratories, there was 'no historical analogue' to the 'speed and totality' with which social media platforms 'conquered the planet' (Singer and Brooking 2018, p. 219). 'Social media was something that simply *wasn't* – until suddenly it was'. Constantly on the lookout for new information technology that might amplify its 'terror marketing' (Mosendz 2014), it was inevitable that Islamic State would gravitate towards social media, just as Al-Zarqawi had switched from satellite to the internet when its game-changing power became apparent (Lynch 2006, p. 53). The same speed was evident when Islamic State followers cheered its fighters' 'blitzkrieg-like advance' across northern Iraq towards Mosul (Price and Al-'Ubaydi 2017). Speed and reach were exceptional qualities of social media, and speed and reach were the new characteristics that made the Islamic State insurgency apparently unstoppable.

There is no doubt that the co-evolution of Islamic State with social media was rapid and dramatic, so rapid and dramatic, in fact, that it brought about 'a sea-change in the way we understand modern terrorism' (Liang 2015, p. 1). The expansion of the new physical caliphate

was paralleled by the expansion of the Islamic State media operation, the increased strategic importance of that operation within the councils of the organisation, and a realization that success and the amplification of success were not just inextricably linked but were becoming a self-fulfilling prophecy. To some extent that was in fact the case: networking via social media allowed previously unknown Islamic State followers to become radicalised, to plan, and to carry out an extraordinary series of attacks across Europe, and to a lesser extent in the Middle East and the US, with minimal support. Whereas intelligence services had been in awe of the forensic planning capabilities of the 9/11 Al-Qaeda attackers, here many of the smaller attacks seemed verging on the opportunistic, and the larger leant heavily on the resolve of a few. However, just as the beheadings had shocked the world, and the apparently effortless taking of Mosul and other cities had compounded that shock, so those attacks, amplified to the remarkable extent that they were, reinforced the terrible idea that Islamic State and its 'war-like slaughters' (Black 2004, p. 24) might be a new and permanent reality. In sociological terms, here – as on 9/11 – was co-evolution between terrorism, 'a phenomenon of the modern age', and 'modern technology' which 'twists the shape of global space':

Terrorism by and against civilians requires physical contact between enemies separated by huge chasms in social space – a combination of physical and social geometry uncommon in human history. Enter modern technology, including rapid transportation, electronic communications, and new weapons that offer the possibility of mass violence between people separated by both physical and social space, those of different regions and nations with different religions, languages, and customs. Social geology shifts and the ground trembles. (Black 2004, p, 23)

Assessment

The probability that (i) Islamic State's relentless leveraging of social media generated new scale, leading to a force multiplier effect, is rated 'highly likely' (higher than 90 percent). As regards (ii) the likelihood that this force multiplier effect was particularly impactful in the period leading up to the capture of Mosul, that was self-evident given the disappearance of the Iraqi army. However, as regards the force multiplier effect continuing on through the blizzard of attacks across Europe using a *modus operandi* that reflected the architecture of

the technology, that is more problematical because the disaggregation of terrorist networks into microstructures is a largely unexplored area. To allow for that newness, it is rated 'likely' (60 to 90 percent).

Conclusion

Having established in Chapters Four and Five that co-evolution provided, on balance, a more convincing explanation than traditional analyses for the symbiotic relationship between, first, Hezbollah and satellite technology, and then Al-Qaeda and the internet, this chapter confirms that co-evolutionary relationship for a third time in the rapidly evolving interaction between Islamic State and social media. What has become clear across the three case studies is that, as complex adaptive systems, what makes co-evolution work is the networked match between technology and terrorist organisation, underpinned by a period of mutually beneficial interaction/data exchange, leading to the evolution of both along parallel trajectories and thus to co-evolution. Culturally, jihadist organisations are naturally networked and non-hierarchical, and it is for this reason that they have been particularly empowered in their terrorist campaigns by the information revolution, empowerment that earned them the descriptor of 'the new terrorism'. There is a point during the process of co-evolution where the balance of influence between terrorist organisation and information technology is reversed: at first, the terrorists leverage and influence the technology, but after a quantum of interaction, the technology begins to influence the shape of the terrorist network by virtue of the new operational features it allows. However, by the time a particular iteration of information technology has brought a terrorist network as far as its mission-driven exploitation can bring it, the phase transition is already underway to a new iteration with the potential to be taken up by another group. What the progressions from one iteration of information technology to another have in common is the breaking down of internal technological barriers and a consequent increase in interoperability, which allows greater interaction, scale and reach, as illustrated by the trajectory: satellite broadcasting, the internet, and social media. In the case of Islamic State, that new social media architecture enabled new microstructures (Knorr Cetina 2005) and therefore a new type of terrorist: the successful lone attacker with little or sometimes no contact with the organisation on whose behalf he kills. This is an iterative process which will inevitably continue to change the nature

of twenty-first century networked terrorism. This is because, as the biological and digital worlds move towards symbiosis (Gillings et al. 2016), and as other terrorists become as networked as Islamist terrorists have become since the end of the Cold War, the same co-evolutionary mechanism will take effect. Because each new iteration will increase interoperability, a significant new question arises: is it therefore reasonable to anticipate that the force multiplier effect terrorists experience will be even greater than heretofore, increasing the threat at an exponential rate?

CONCLUSIONS

Introduction

This thesis began by investigating the possibility of describing a simple mechanism (Conitzer and Sandholm 2014) – in the sense of a consistent series of interacting elements – that would ‘sufficiently explain’ (Beach and Pedersen 2012, p. 8) how terrorism so successfully exploits new iterations of information technology. It has gone on to identify that mechanism, describe its structure, and test its theoretical application rigorously in three case studies – Hezbollah and its migration from terrestrial to satellite broadcasting, Al-Qaeda and its leveraging of the internet, and Islamic State and its adoption of social media – which have found it to be logically coherent. More than that, it has revealed the inherent historicity of the mechanism by tracing how it has evolved in line with the trajectory of information technology over a period of more than 20 years. In addition, it has shown, using the NATO Allied Joint Doctrine for Intelligence Procedures (NATO-AJP-2.1) estimative probability standard, how that assessment links directly to the data it has adduced (Irwin and Mandel 2020). It ends by challenging some of the prevailing assumptions in the discipline of terrorism studies, arguing that they are better explained from the standpoint of complexity theory, the guiding ontology of the thesis, than by using a more traditional linear world view. Prior knowledge provides ‘ideational anchorage’ during new learning experiences (Langer and Nicolich 1981) but only to the point where it is finally subsumed in a process of ‘creative destruction’ (Perez 1983, p. 3). Nowhere more than in science, and arguably nowhere in science more than in the broad realm of information-related technologies, are preconceptions dismissed with such relentless regularity. This is a good thing. It is a reflection of the fact that science as a complex body of information is in a perpetual state of flux (Börner et al. 2012, pp. 3-4), and of the dizzying speed with which existing knowledge is aggregated and the attendant search for new directions leads to significant leaps in understanding. However, as veteran RAND terrorism researcher Brian Jenkins (2015) illustrated by his early failure to identify the internet as a weapon, understanding is invariably and frustratingly a lagging indicator.

As the preceding chapters have shown in relation to terrorism and information technology and how they co-evolve, one such paradigm shift in understanding was, and remains,

complexity science (Holland 2014, 1995, 1992b, 1992a, 1975; Lemm and Vatter 2014; Mitchell 2009, 2006, 1995; Kauffman 1993, 1992, 1991b, 1991a), which re-interprets life as non-linear rather than linear and reductionist, and which focuses on biopolitical systems as interactive in the sense of networked, emergent in the sense of changing constantly in response to that interaction, and unpredictable in that they sometimes vary by chance, without a cause (Cresser 2011, p.1). It does not, it is worth noting again, set out to replace the canon of knowledge that already exists in disciplines to which it is applied, but rather provides a new way of looking at them that has the potential to explain countless underlying connections whose existence is frequently hypothesised, if not always fully understood. Due largely to the revolutionary development of mathematical computation and the non-linear concepts it has shown itself capable of modelling, the computer has become 'the instrument of the sciences of complexity' (Pagels 1989, p. 36) and complexity has become dominant as a means of modelling and interpreting physics and the life sciences, technological evolution, and, increasingly, 'biological-digital fusion' (Gillings et al. 2016, p. 2). In the humanities, however, siloed thinking in many disciplines remains largely unaffected, although the switch away from 'functionalist sociology' and the structure and agency dichotomy to a new 'network sociology' (King 2010, p. 258) has placed productive new emphasis on interaction and its downstream evolutionary implications, such as co-evolution. In relation to terrorism, it recalls Crenshaw's prescient view (2010, p. 2) that in attempting to understand the evolution of terrorist organizations, focusing on them 'in isolation addresses the issue of agency but misses the significance of interactions'. Without further rehearsal of what has gone before, this chapter will (i) set out the key findings of the thesis, (ii) identify the degree to which they lead to a re-interpretation of key concepts in the discipline of terrorism studies; (iii) examine their implications for twenty-first century counterterrorism, and (iv) preview areas which suggest themselves as a logical continuation of this research.

Key findings of this thesis

This thesis identifies a novel mechanism which explains how certain high-performing terrorist networks co-evolve with new iterations of information technology. It does so initially simply by describing that mechanism, and subsequently by examining in more detail the structure and function of its various elements and the consequences of their interaction. It shows that

the co-evolutionary mechanism comprises three elements: a networked terrorist organisation with a track record as an innovative user of information technology, a new iteration of information technology packed with the disruptive power that comes with novelty, and evidence of a substantial force multiplier effect in line with the evolutionary function of their co-evolution. Why does co-evolution happen in the case of this particular pairing? The thesis shows that both terrorism and some networked terrorist groups with particular organisational structures (Hayden 2013) may reasonably be described as complex adaptive systems, a feature of which is that they co-evolve with similar systems in pursuit of augmented performance (Holland 1992b, p. 11). That augmented performance is the basis of co-evolution (Kauffman 1991a, p. 6), which works only when it brings mutual benefits to both partners. In the case of this pairing there are clear operational gains for both terrorists and technology. In the case of the terrorists: The design of the new technology allows terrorist networks to evolve operationally, while the increased interoperability amplifies their messaging, enables greater autonomy of communication (Conway 2005, p. 9), and increases the threat they pose. In the case of the technology: Mission-driven adoption by terrorists catalyses evolution. Each new iteration leads to greater interoperability which gives it greater scale/reach (Elkhodr et al. 2016; Heubusch 2006, pp. 26-30).

The rudimentary structure of the co-evolutionary mechanism is that of a classic information system, defined as ‘a set of interrelated components that collect (or retrieve), process, store, or distribute information in support of decision-making and control in an organisation’ (Laudon and Laudon 2000, pp. 44-45). System design is widely replicated in nature and this follows a basic three-stage input-processing-output logic typical of information systems, not unlike the much-studied relationship, for example, between DNA, RNA and proteins and the process by which genetic information moves between them, described by Crick (1972) as ‘the central dogma’ of molecular biology. However, it is important to realize that information is not simply transferred from one element to the other. In the case of DNA-RNA-Protein, DNA contains the genetic code which is *transcribed* into RNA. RNA then processes that code by *translating* it into proteins (Clancy and Brown 2008; Isaacson 2021, pp. 43-44). The co-evolutionary mechanism mirrors that design. In the case of input, the system architecture of the new iteration of information technology, essentially its code, will determine how the force multiplier effect will ultimately express itself. In relation to processing, the terrorist network

in its interaction with the technology acts as a catalyst for the force multiplier effect. The output is 'communication' (Jenkins 2015a) in the form of the terrorist attack. 'The process of translation can be seen as the decoding of instructions' (Clancy and Brown 2008). In the detail of its structure, the co-evolutionary mechanism sits comfortably with social systems as defined by Luhmann (1995, 1987, 1986), who, uniquely in sociology, promotes communication to the dominant position in the pantheon of life systems, reflecting the central position it also occupies in terrorism studies (Jenkins 2015; Nacos 2007, p.14; Hoffman 2006, p. 198), while relegating human actors to the role of catalysts. That relative prominence of communication also reflects the degree to which online communications platforms act as significant social disruptors, and, more broadly, the degree to which the gradual symbiosis between biological and digital information is already being expressed through artificial intelligence, with the potential in future for 'virtually limitless recombination' (Gillings et al., 2016).

The mechanism shows how co-evolution accounts for the dramatic increase in the threat posed at their height by each of the three case studies – Hezbollah and satellite broadcasting, Al-Qaeda and the internet, and Islamic State and social media – examined in Chapters Four, Five and Six respectively. In the case of Hezbollah and satellite broadcasting, it allowed Hezbollah to broadcast propaganda on the progress of the 2006 war directly into the homes of Israelis, despite repeated Israeli attempts to block its transmitters (Jorisch 2004c, 2004b, 2004a). This was the impact of an increased satellite footprint. In the case of Al-Qaeda and the internet, the internet was global, many to many, acknowledging no boundaries, and this was the remarkable scale of the benefit it delivered for Al-Qaeda, allowing it to communicate globally and covertly from behind a phalanx of computers, and to 'cyberplan' (Thomas 2003) as if invisible in the run-up to 9/11. In the case of Islamic State and social media, co-evolution enabled the spate of lone attacks, predominantly in Europe, from 2014 until 2018 (Nesser 2019, p. 15), by attackers with marginal links to the core organisation. This displayed the reflexive capacity of social media to allow individuals to feed back into its operating system and influence the organisation and its direction, an extraordinary new level of autonomous communication (Conway 2005, p. 9). An examination of the three case studies also indicates that, in line with the change in power balance (Burkhardt and Brass, 1990, p. 105) that typically accompanies the 'exogenous shock' (Barley 1986, p. 80) caused by adoption of new

technology, it is the terrorists who initially control the innovative new manner in which the technology is applied, for example in the case of pre-9/11 cyberplanning by Al-Qaeda (Thomas 2003), until a tilt occurs after which the technology begins to influence the operational 'shape' of the terrorist network as a result of having been successfully diffused through its systems, in the case of Al-Qaeda underpinning it as leaderless and global at once, and in the case of Islamic State, empowering individual followers to attack on behalf of the network as a whole. This is less obvious in the case of Hezbollah and satellite broadcasting because the evolutionary step from terrestrial to satellite broadcasting was not as great a sea-change as the step from satellite to the internet or that from the internet to social media.

What this illustrates is that each new iteration of information technology allows a more complex architecture for the terrorist networks. As information technology becomes more complex over time (satellite, internet, social media), terrorism too is becoming more complex (Hezbollah, Al-Qaeda, Islamic State). Even leaving aside the chronologically accurate connections to the three terrorist organisations, Hezbollah, Al-Qaeda, Islamic State, the evolutionary trajectory of the technology, from satellite to internet to social media, is beyond dispute. As previously noted, satellites have three types of communications function: telecommunications, broadcasting, and data transmission, all of which are varieties of electronic information diffusion (NASA 2020; Orbital Today 2020; Maini and Agrawal 2014). The progression from terrestrial to satellite technology meant a significant increase in speed and power, so that data was now transferred in gigabytes per second rather than megabits per second. At the same time, the breaking down of barriers between terrestrial and satellite technology increased interoperability, scale, and therefore force multiplier effect. That transformed Hezbollah's global presence. In the case of Al-Qaeda and the internet the process was similar. The internet was originally developed as a system that would allow the US military to link satellite systems and to transmit information to and from the front lines of distant conflict. Again, enabling satellite systems to work together increased interoperability, scale and force multiplier effect. So too with Islamic State and its early adoption of internet-based social media, which allowed users to form 'microstructures' (Knorr Cetina 2005, p. 216), in the sense of social networks that could generate their own new material and feed it into the system, multiplying its reach once again and taking ownership of the process far more than in the case of the internet.

The significance of this evolution towards microstructures (Knorr Cetina 2005) is that these are networks but 'not simply networks'. 'The term "microstructure" is intended to point to the richness and diversity of elements and practices that layer global social forms' (Knorr Cetina 2005, p. 216). Salafi-jihadists are a perfect example, as powerfully illustrated by Maher 2017 and Ranstorp 2007, among others. As a result of that evolution towards microstructures, hard infrastructure has disappeared in terms of information technology (satellite uplinks, down links, etc.), with a move to 'socio-technical' terminology, such as 'communications protocols', 'platforms', 'algorithms', etc. (Lash 2003, p. 54). At the same time, organisations have disappeared in terms of the terrorism, leaving leaderless de-territorialised 'systems' (Lia 2006, p. 17) and a zone of conflict that is potentially global and always unpredictable. In terms of both terrorism and information technology, cyberspace has become 'a form of central nervous system' (Ranstorp 2007, p. 38). 'Continual disintegration creates the space for successor-elements and this increases their complexity and the chances of survival of the overall system' (Knorr Cetina 2006, p. 217; Luhmann 1984, pp. 76-81; Zeleny 1981, pp. 4-17). The logic of the three case studies suggests that the same co-evolutionary mechanism will take effect when a terrorist network to succeed Islamic State become early adopters of a new iteration of information technology to follow social media. It indicates how the next co-evolutionary pairing will happen, but not what that pairing will be.

What that logic does reveal, significantly, is that this co-evolutionary mechanism is by no means an exclusively Islamist terrorist phenomenon. Because, as the biological and digital worlds move towards symbiosis (Gillings et al. 2016), and as other terrorist groups become as networked as Islamist terrorists have become since the end of the Cold War, the same mechanism will take effect. Because each new iteration increases interoperability, it is reasonable to expect that the force multiplier effect that results will be even greater than heretofore. However, because the architecture of the technology is certainly difficult, if not impossible, to anticipate, it is equally difficult, if not impossible, to anticipate how that force multiplier effect will play out.

What is inevitable is that the potential symbiosis between biological information and digital information will reach a critical point where the two can compete 'via natural selection' (Gillings et al. 2016, p. 1). Already, digital information technology, self-organizing and autopoietic, is in the ascendent, to the extent that human activity has generated information

storage and replication systems that are on track ‘to contain more information than the combined information content of the cells and genes in the biosphere’ (Gillings et al. 2016, p. 4). Despite that competitive characterisation, information storage and translation/computation/replication (Flack 2017) is, in fact, an evolutionary process that is common to biological and, increasingly, technological systems. It is a value-neutral process, although it does lead to change in the power relationships between and within the systems involved. As McLuhan (1967) anticipated when he referred to certain types of information technology as ‘extensions of man’, it has indeed developed to the point where it is extending human cognition ‘beyond the brain’ (Zlotnik and Vansintjan 2020). In that context, information technology already provides storage and translation/computation for social systems in the form of online social networks¹¹⁸, increasing at an exponential level as a result of replication. Co-evolutionary interaction between technological systems and social systems catalyses and prioritises communication, as set out by Luhmann. In the same way, co-evolutionary interaction between technological systems and terrorism catalyses and prioritises communication, as long held by Jenkins. In terms of co-evolution between technological systems and biological systems the route ahead remains unclear, and this perhaps explains the inclusion of gene editing in the US national threat assessment list once CRISPR was developed in 2016 (Regalado 2016) in all its mould-breaking accessibility.

Twenty-first century terrorism: a new interpretation

Identifying both information technology and certain high-performing terrorist organisations as complex adaptive systems, which, in line with their evolutionary trajectories, co-evolve with other systems whose interaction they find mutually beneficial, allows a fundamental re-interpretation of key concepts in the discipline of terrorism studies. That re-interpretation should begin with the foundational analysis by the RAND team, when it started terrorism research 1972, that ‘terrorism evolves’ (Jenkins 1999, p. iv). Instead, in line with the realization that ‘the world we live in is a complex socio-technical system’ (Carley et al. 2002, p. 79), a more appropriate twenty-first century analysis would be not that terrorism evolves, but that it co-evolves, as this thesis has shown.

¹¹⁸ The term ‘social network’ was coined in 1954 by Australian social anthropologist John Arundel Barnes in ‘Class and Committees in a Norwegian island Parish’. See Barnes 1954.

In the same way, the ‘symbiotic relationship’ (Wilkinson 2006, p. 145) between terrorists and the media, at the centre of the discipline for 50 years, is, in reality, a co-evolutionary relationship between terrorism and information technology catalysed by the identities of both as complex adaptive systems that ‘evolve through differential fitness’ (Gillings et al. 2016) and augment one another’s performance for as long as it is mutually beneficial (Holland 1992a, p. 11). That being so, imperatives frequently attributed to terrorists, such as the ‘imperative to act’ (Hoffman 1999, p. 35), the ‘religious imperative’ (Hoffman 1994, p. 3), and the ‘imperative to succeed’ (Hoffman 1994, p. 11), are, similarly, instinctive responses driven by co-evolution rather than imperatives driven by some unspecified form of mission-driven Salafist rationale.

What is new about ‘new terrorism’ is the increase in scale – as a result of seamless technological interoperability (Yocabet and Reijnen 2021) – available to networked terrorists who successfully co-evolve with new iterations of information technology. As Castells (2004, pp. 3-4) points out, networks are substantially more effective than hierarchical command-and-control systems when combined with electronic technology. In relation to the ‘increasing lethality’ (Jenkins 2001, pp. 4-5) of ‘new terrorism’, the reason for this phenomenon is not that it is becoming more and more difficult to shock, although that may indeed be true. The reason, in the case of 9/11, for example, was that such was the open field for ‘cyberplanning’ (Thomas 2003) presented by the internet that Al-Qaeda successfully carried out a well-nigh impossible co-ordinated suicide attack using multiple passenger aircraft trained on several targets while betraying no operational hints to the intelligence services (Tenet 2002, p. 4). The result was 2,977 deaths, apart from the 19 hijackers. In the case of Islamic State and social media, the attacks in Europe, largely by individuals with only peripheral links to the core organisation, were also virtually impossible to anticipate and difficult to stop when they came. In the case of Hezbollah and satellite broadcasting, the impact during the 2006 war with Israel was largely psychological, both in terms of Hezbollah’s new global reach and in terms of its new ability to broadcast into Israeli households.

While complexity theory, and co-evolution specifically, provides a much more logically compelling twenty-first century explanation than has hitherto been available for how terrorism and information technology interact and develop ‘a symbiotic relationship’ (Wilkinson 2006, p. 145), it does not – as noted in Chapter Two – provide an explanation which

similarly underpins the pervasive view in the discipline that terrorism is fundamentally all about communication (Jenkins 2015; Nacos 2007, p. 14; Hoffman 2006, p. 198). Looking at the co-evolution of terrorism and information technology from the viewpoint of Luhmannian systems theory, however, yields confirmation of that missing link: the primacy of communication. Luhmann promotes communication to the dominant position among social systems, reflecting the central position it also occupies in terrorism studies (Jenkins 2015; Nacos 2007, p.14; Hoffman 2006, p. 198), while relegating human actors to the role of catalysts. This also sits comfortably with the co-evolutionary mechanism as a classic information system, where a new iteration of information technology is catalysed by the terrorists and the code contained in its architecture is translated, in the form of a multiplier effect, into communication. 'The more one considers terrorism as a phenomenon, the less it resembles other forms of violence and the more it looks like a form of communication' (Decker and Rainey 1980, p. 2).

In relation to the most lethal attack in the history of terrorism and the conclusion of The 9/11 Commission Report (2004, p. 9) that the September 11 attacks represented a 'failure of imagination' in that intelligence agencies simply failed to anticipate, detect or pay adequate attention to forewarnings of what was about to happen, this thesis disagrees. It takes the view that 9/11 was, instead, a failure to see the elements of what was unfolding from the point of view of complexity theory, the most holistic and cutting-edge means of interpreting fast-changing, multi-faceted, interactive terrorism risk scenarios. As a result, the plotters – working online often without any significant professional security precautions – were operationally invisible. It is therefore reasonable to conclude that 9/11 was, in fact, a failure of understanding.

Implications for counterterrorism

That lesson of invisibility is one which runs through all three of the case studies in this thesis. Hezbollah's switch from terrestrial to satellite television was not regarded as operationally significant by Israel until the 2006 war and repeated failed attempts to jam its broadcasts (Jorisch 2004c, 2004a) enabled it to launch a new campaign of psychological warfare against the Israeli population. In a similar vein, Al-Qaeda's adoption of the internet was largely overlooked while counterterrorism experts focused instead on what weapons technology it

was likely to adopt next (Jenkins 2015), with the result that pre-9/11 online planning went undetected and invisible. In the case of Islamic State and social media, Al-Qaeda in Iraq essentially became invisible as it transitioned into Islamic State simply because the consensus among American military leaders was that the jihadists had been 'licked' (Fordham 2015) following the 2007 'surge' in Iraq (Duffy 2008). When Islamic State did emerge, it was initially dismissed as no more than Al-Qaeda in Iraq by another name. By the time Islamic State had captured Mosul and lone actors across Europe had begun to launch a blizzard of independent attacks between 2014 and 2019, its prowess was attributed to its skill in leveraging social media rather than to psychological warfare, though how exactly this was being achieved at such scale was never satisfactorily explained at that time. Islamic State walked into Mosul largely because of the fear engendered through social media. 'Obama hadn't believed that ISIS were equivalent to the al-Qaeda network but the Mosul takeover changed his mind' (Phillips 2016, p. 207). The weapons order was psychological warfare first, social media second. That being so, in terms of lessons for counterterrorism, it is worth considering that, in effect, American foreign policy was being significantly influenced as a result of an illusion generated through social media by a terrorist network with endless quantities of militant fervour but relatively little in the way of firepower compared with the US, and, crucially, no air force. Beyond that, the striking fact appears to remain that military and intelligence agencies, by their nature hierarchical, seem incapable of finding a means of countering the asymmetrical tactics of terrorism, again despite the huge imbalance of manpower and resources. This is typical of a hierarchical actor when faced with a networked terrorist opponent: 'It tends to underestimate and misunderstand the powers of adaption and longevity of the resistance it confronts' (Duffield 2002, p. 157). In other words, it consistently fails two key tests: it is less agile and less resilient.

It is also the case that the co-evolutionary mechanism identified in this thesis, may, with further study, have interesting implications for counterterrorism. As noted above, the logic of the three case studies suggests that the same co-evolutionary mechanism will take effect when terrorists who succeed Islamic State become early adopters of a new iteration of information technology to follow social media. It indicates how the next co-evolutionary pairing will happen, but not what that pairing will be. On the other hand, it goes further by making clear that this is emphatically not a mechanism which is confined to jihadist groups

because of their networked nature. As other terrorist groups become as networked as Islamist terrorists have become since the end of the Cold War, the same mechanism will take effect. Because each new iteration increases interoperability, it is reasonable to expect that the force multiplier effect that results will be even greater than heretofore. However, because the architecture of the technology is difficult, if not impossible, to anticipate, how that force multiplier effect will play out remains unpredictable. Even so, on the basis of the three case studies examined here, one might reasonably expect that it may follow the route anticipated in the development of complex microstructures (Knorr Cetina 2005) towards greater diffusion (Castells 2004, p. 9) and even more autonomy for individual terrorist network nodes or members. What this thesis does make clear in relation to this broad point is that – as argued by Jackson (2001, p. 5) – it is the pursuit of the *processes* which make terrorism the complex adaptive system that it is, rather than the persistent analysis of the political *effects* of terrorism, that leads to enhanced understanding.

Areas for further study

This thesis has underlined repeatedly the critical role of information and information technology in twenty-first century terrorism and counterterrorism. It has shown strikingly how, in contemporary society, ‘information, cultural expression, and language are now being replicated at multiple points around the globe via interconnected digital systems’ (Gillings et al. 2016, p. 2). Humans and digital technology share the same universal language built on the syntactic basis of information society and its universal grammar (Sudkamp and Cotterman 1988; Chomsky 1957). Technological progress ‘shows signs of being super-exponential when examined across technological paradigms’ (Nagy et al. 2011). Digital technology has ‘infiltrated the fabric of human society to a degree of undisputable and often life-sustaining dependence’ (Gillings et al. 2016, p. 11). Given such facts, it is clear, maintain Gillings et al. (2016, p. 11) that ‘we are already in the midst of a major evolutionary transition that merges technology, biology, and society’. In that context, ‘we’ includes terrorist networks as a subset of wider society. So, in the context of potential information terrorism, it is hard to regard the phrase ‘life-sustaining dependence’ as anything other than a very large moving target.

As noted in the introduction, there was a dramatic new focus in counterterrorism in 2016 when the US Director of National Intelligence, James Clapper, added gene editing as a

potential weapon of mass destruction to the annual Worldwide Threat Assessment report (Regalado 2016). Gene editing established human beings definitively as reprogrammable information systems, and it was the only biotechnology with the potential to be used as a 'bioweapon' that was listed as a threat. Although it is not mentioned by name in the intelligence assessment, it is believed the security concerns refer, in particular, to the gene editing system, CRISPR (Doudna 2020; Doudna and Charpentier 2014), because of its relative ease of use and low cost. Margaret Kosal (2020) goes as far as to suggest that systems such as CRISPR 'may enable capabilities that challenge nuclear weapons in terms of strategic stability', observing that:

The rate and broad diffusion of emerging technology matters. There has not been sufficient time for institutions to form mechanisms that respond to and monitor the ways that humans combine gene editing and security challenges. Mechanisms include, but are not limited to, exploitation of advances in the life sciences and biotechnology for biological (as well as chemical) proliferation. As such, this field needs more study in order to assess its level of threat to international security. (Kosal 2020)

These developments underline the degree to which the gradual symbiosis between biological and digital information already being expressed through artificial intelligence has the potential for 'virtually limitless recombination', sometimes for malign purposes. Less dramatic perhaps than gene editing, but also with pervasive potential for harm are information systems such as the fledgling Internet of Things (Ashton 2009); the computer networks linking critical infrastructure of the type already being targeted by Russian state hackers in Ukraine (Yürük 2022), and, in global finance, the automated trading algorithms used by high-frequency trading firms which represent just two percent of all financial trading companies in the US but account for 73 percent of all equity trading volume (Kenett et al. 2013).

Of concern too in the context of the move towards self-directing terrorist microstructures (Knorr Cetina 2005), is militant accelerationism (Kriner 2022) which has been responsible for dozens of attacks worldwide in the past two decades as it attempts to accelerate the demise of 'capitalist and liberal civilization' and speed 'social rejuvenation'. The most recent attack apparently associated with this loose framework was the shooting at a supermarket in Buffalo, New York, on May 17, 2022, in which 10 people were killed and three wounded by an 18-year-old gunman who streamed the attack live online (Milman 2022). The attacker described himself as an 'eco-fascist' and a believer in the 'great replacement theory' which

holds that whites are in danger of losing their position in society as a result of immigration. That belief was also held by the white nationalist who killed 51 people in Christchurch, New Zealand, in March 2019, killings which were also live-streamed (Royal Commission Report 2020). Adherents of militant accelerationism typically self-identify, frequently self-radicalise, and sometimes coalesce around a solitary figure such as Ted Kaczynski, more popularly known as The Unabomber, who produced the 35,000-word anti-technology manifesto *Industrial Society and its Future* (Kaczynski 1995). The same document was also referenced by Norwegian far-right domestic terrorist Anders Breivik (Farrell-Molloy and Macklin 2022).

In terms of online technology, Telegram has long been a favourite of far-right extremists for digital organising and community building (Shadnia et al., 2022, p. 2), including adherents of the broad neo-fascist strain of militant accelerationism. The most prominent to date has been the so-called Atomwaffen¹¹⁹ Division (Newhouse 2021), which was unveiled in October 2015 and which was heavily networked from the start. Many of its most influential members have been arrested on suspicion of crimes ranging from possession of illegal weapons to murder. Some, including its founder, Brandon Russell, are in jail, indicating that the attention of the authorities has had the desired effect. Some members, however, openly suggest on Telegram that ‘the age of public brands and propaganda is over’ and that its focus is now turning instead to ‘small-cell, clandestine, in-person organisation’, as Newhouse (2021) warns in his analysis, ‘The Threat is the Network’:

The biggest risk ... is that a network of recruitment, radicalisation and organisation is already established and so a focus on any specific group may not tackle the root of the issue. Enforcement against individuals and groups is necessary but not sufficient for mitigating the threat posed by neo-fascist accelerationists ... Atomwaffen was one node in a dynamic network spanning the globe, and treating it as such may allow for more comprehensive preventative action.

The danger is that by abjuring brands and propaganda, for example, militant accelerationism may enter a period of operational invisibility during which, counterintuitively, its potential threat increases rather than diminishes, in line with the three case studies tracked in this thesis. Indeed, given the propulsive power of co-evolution, combined with the new and very real speed imbued by a hyperconnected world, it may seem that ‘apocalyptic time’ (Berger

¹¹⁹ *Atomwaffen* means nuclear weapons in German.

2015) is no longer an environment that must be calculatedly generated, but is becoming a reflexive risk routinely ignited not just by terrorism but by society as a whole. In such circumstances, it may be that it is therefore being intuitively identified by militant accelerationists as a 'residual risk' (Beck 2009, p. 15), a potential weapon which need only be sporadically magnified in order to paralyse modern society, causing it to 'freeze in panic'. The co-evolutionary trajectory continues.

REFERENCES

- Abbott, A., 1988. 'Transcending General Linear Reality'. *Sociological Theory*, 6 (2), pp. 169-186. Available from: <https://dokumen.tips/documents/abbott-transcending-general-linear-reality.html> [Accessed 6 September 2020].
- Abernathy, W. and Utterback, J., 1978. 'Patterns of Industrial Innovation'. *Technology Review*, 80 (7), pp. 40-47. Available from: https://www.academia.edu/23341473/Patterns_of_Industrial_Innovation [Accessed 24 December 2019].
- Abuza, Z., 2004. 'Learning by Doing: Al Qaeda's Allies in Southeast Asia'. *Current History*, 103 (672), pp. 171-176.
- Achen, C. H. and Snidal, D., 1989. 'Rational Deterrence Theory and Comparative Case Studies.' *World Politics*, 41 (2), pp. 143-169. Available from: http://www.robertthomson.info/wp-content/uploads/2010/11/achen_snidal_RDT_WP89.pdf [Accessed 5 November 2020].
- Adami, C., 2012. 'The Use of Information Theory in Evolutionary Biology'. *Annals of the New York Academy of Sciences*, 1256 (1), pp. 49-65. Available from: <https://arxiv.org/ftp/arxiv/papers/1112/1112.3867.pdf> [Accessed 1.2.2023].
- Addis, C. and Blanchard, C., 2011. Hezbollah: Background and Issues for Congress. CRS (Congressional Report Service) Report for Congress, 3 January. Available from: <https://fas.org/sgp/crs/mideast/R41446.pdf> [Accessed 5 November 2020].
- Ahmed, E., Elgazzar, A. and Hegazi, A., 2008. 'On Complex Adaptive Systems and Terrorism'. *Physics Letters A*, 337 (1&2), pp. 127-129. Available from: <https://arxiv.org/pdf/nlin/0501032.pdf> [Accessed 30 March 2018].
- Ajjoub, O., 2022. ISIS has a new leader. It's important to understand their operational capacity. Atlantic Council, 18 March. Available from: <https://www.atlanticcouncil.org/blogs/menasource/isis-has-a-new-leader-its-important-to-understand-their-operational-capacity-%EF%BF%BC/> [Accessed 25 August 2022].
- Alali, A. and Eke, K., 1991. *Media Coverage of Terrorism: Methods of Diffusion*. Newbury Park, CA: Sage.
- Aldrich, R., 2005. 'The New Terrorism: The problem is balancing security, freedom and the globalising quest for luxury'. *The Independent*, 10 July. Available from: <https://www.independent.co.uk/voices/commentators/richard-aldrich-a-global-battlefield-5528316.html> [Accessed 11 June 2018].
- Alexander, Y. and Picard, R., 1991. *In the Camera's Eye: News Coverage of Terrorism Events*. Washington DC: Brassey's.
- Al-Shishani, M. B., 2010. 'Taking al-Qaeda's Jihad to Facebook'. *The Jamestown Foundation. Terrorism Monitor*, 8 (5), 4 February. Available from: <https://jamestown.org/program/taking-al-qaedas-jihad-to-facebook/> [Accessed 15 February 2020].

Anderson, J. and Rainie, L., 2014. 'Digital Life in 2025'. Pew Research Center, 11 March. Available from: <https://www.pewresearch.org/internet/2014/03/11/digital-life-in-2025/> [Accessed 25 April 2022].

Anderson, P. and Tushman, M., 1990. 'Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change'. *Administrative Science Quarterly*, 35 (4), pp. 604-633.

AP News, 2013. A Look at Recent Assassinations in Lebanon. 27 December. Available from: <https://apnews.com/article/01aa3d3bfa944bfd960d250ebd528061> [Accessed 19 November 2021].

Archer, M., 2010 [1982]. 'Morphogenesis Versus Structuration: On Combining Structure and Action'. *The British Journal of Sociology*, 61 (s1), pp. 225-252. Special Issue: The BJS – Shaping Sociology over 60 Years. [Originally published in 1982. *The British Journal of Sociology*, 33 (4), pp. 455-483]. Available from: <https://onlinelibrary.wiley.com/doi/10.1111/j.1468-4446.2009.01245.x> [Accessed 23 August 2021].

Arlen, M., 1997. *Living-Room War*. Syracuse, NY: Syracuse University Press.0

Arquilla, J. and Ronfeldt, D., 2001. 'The Advent of Netwar (Revisited)'. In: J. Arquilla and D. Ronfeldt, eds, *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, CA: RAND, pp. 1-25. Available from: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch1.pdf [Accessed 2 February 2020].

Arquilla, J. and Ronfeldt, D., 1999. *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica, CA: RAND. Available from: https://www.rand.org/pubs/monograph_reports/MR1033.html [Accessed 8 October 2021].

Arquilla, J. and Ronfeldt, D., 1997. 'A New Epoch – and Spectrum – of Conflict'. In: J. Arquilla and D. Ronfeldt, eds, *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, pp. 1-20. Available from: https://www.rand.org/pubs/monograph_reports/MR880.html [Accessed 11 October 2021].

Arquilla, J., Ronfeldt, D. and Zanini, M., 1999. 'Networks, Netwar, and Information-Age Terrorism'. In: Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D. and Zanini, M., *Countering The New Terrorism*. Santa Monica, CA: RAND, pp. 39-84.

Arthur, W. Brian, 2009. *The Nature of Technology: What it is and How it Evolves*. London: Penguin.

Ashton, K., 2009. 'That "Internet of Things" Thing'. *RFID Journal*, 22 June. Available from: <http://www.rfidjournal.com/articles/pdf?4986> [Accessed 12 July 2018].

Atkinson, S. R. and Moffat, J., 2005. *The Agile Organization: From Informal Networks to Complex Effects and Agility*. Washington DC: CCRP (Command and Control Research Programme) Publication Series. Available from: http://www.dodccrp.org/files/Atkinson_Agile.pdf [Accessed 13 October 2021].

Atwan, A. B., 2015. *Islamic State: The Digital Caliphate*. London: Saqi Books.

Axelrod, R. and Cohen, M. D., 1999. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York: The Free Press.

- Axtell, R., 2004. 'The New Co-Evolution of Engineering Systems and the Social Sciences'. Paper presented at engineering systems symposium, Cambridge, 31 March.
- Azani, E., 2006. 'Hezbollah, A Global Terrorist Organization'. Testimony to the House Committee on International Relations, Sub-committee on International Terrorism and Non-Proliferation, Washington DC. September. Available from: <https://www.ict.org.il/Article/960/Hezbollah-a-Global-Terrorist-Organization#gsc.tab=0> [Accessed 5 March 2021].
- Ayubi, N., 1990. 'Arab Bureaucracies: Expanding Size, Changing Roles'. In: G. Luciani, ed., *The Arab State*. Berkeley and Los Angeles, CA: University of California Press.
- BAAD, 2012. Big, Allied And Dangerous. A Department of Homeland Security online database, led by the University of Maryland. Available from: <https://www.start.umd.edu/baad/database.html> [Accessed 1 February 2023].
- Baddarin, B., 2005. 'Al-Qaeda Draws up its Working Strategy to the Year 2020'. *Al-Quds al-Arabi*, 11 March.
- Baetu, T., Barwich, A.S., Brooks, D., Dutreuil, S. and German, P.L., 2013. 'Model Thinking in the Life Sciences: Complexity in the Making'. Second European Advances Seminar in the Philosophy of the Life Sciences, Hermance, Switzerland, 10-14 September. *Biological Theory*, 8 (1), pp. 121-124.
- Bakker, E. and Boer, L., 2007. 'The Evolution of Al-Qaedaism: Ideology, Terrorists, and Appeal'. Netherlands Institute of International Relations The Hague. Available from: <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/67702.pdf> [Accessed 2 June 2022].
- Balanis, C. A., 2015. *Antenna Theory: Analysis and Design*. Fourth edition. Hoboken, NJ: John Wiley & Sons.
- Bale, J. and Ackerman, G., 2009. 'Profiling the WMD Threat'. In: S. Maurer, ed., *WMD Terrorism: Science and Policy Choices*. Cambridge, MA: The MIT Press, pp. 11-46.
- Ball, D., Hair, L., McVey, T. and Nacht, M., 2009. 'Preventing WMD Terrorism'. In: S. Maurer, ed., *WMD Terrorism: Science and Policy Choices*. Cambridge, MA: The MIT Press, pp. 483-510.
- Barclay, J., 2010. 'Challenging the Influence of Anwar Al-Awlaki'. The International Centre for the Study of Radicalisation and Political Violence, King's College, London, September. Available from: http://icsr.info/wp-content/uploads/2012/10/1283965345ICSR_ChallengingtheInfluenceofAnwarAlAwlaki.pdf [Accessed 15 December 2017].
- Barley, S., 1986. 'Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments'. *Administrative Science Quarterly*, 31 (1), pp. 78-108.
- Barnard, A., 2016. Battle Over Aleppo is Over, Russia says, as Evacuation Deal Reached. *The New York Times*, 13 December. Available from: <https://www.nytimes.com/2016/12/13/world/middleeast/syria-aleppo-civilians.html> [Accessed 22 August 2022].
- Barnes, J. A., 1954. 'Class and Committees in a Norwegian Island Parish'. *Human Relations VII* (1954), pp. 39-58.

Barth, A., 1943. *The New Republic: A Journal of Opinion*, Volume 108. Letters, p. 667. Available from: https://books.google.nl/books?id=cDgQAAAAIAAJ&q=%22draft+of+history%22&redir_esc=y [Accessed 30 June 2021].

Bar-Yam, Y., 2004. *Making Things Work: Solving Complex Problems in a Complex World*. Cambridge, MA: NECSI Knowledge Press.

Bar-Yam, Y., 1997. *Dynamics of Complex Systems*. Reading, MA: Addison-Wesley.

Basu, A., 2014. 'Social Network Analysis: A Methodology for Studying Terrorism.' In: M. Panda, S. Dehuri and G.N. Wang, eds, *Social Networking: Mining, Visualization, and Security*. Intelligent Systems Reference Library, Volume 65. Cham, Switzerland: Springer, pp. 215-242.

Bazin, A., 2017. 'Complex Adaptive Operations on the Battlefield of the Future'. Modern War Institute at West Point, 28 February. Available from: <https://mwi.usma.edu/complex-adaptive-operations-battlefield-future/> [Accessed 26 October 2021].

BBC News, 2015. Europol chief warns on computer encryption. BBC News online, 29 March. Available from: <http://www.bbc.com/news/technology-32087919> [Accessed 27 November 2017].

BBC News 2015a. The Day Iran Buried Ayatollah Khomeini. French photojournalist, Eric Bouvet, recalls covering the funeral. Available from: <https://www.bbc.com/news/av/magazine-32938264> [Accessed 31 October 2021].

BBC News, 2011. Islamist Cleric Anwar al-Awlaki Killed in Yemen. BBC News online, 30 September. Available from: <https://www.bbc.com/news/world-middle-east-15121879> [Accessed 16 February 2020].

BBC News 2001. History of Airliner Hijackings. BBC News online, 3 October. Available from: http://news.bbc.co.uk/2/hi/south_asia/1578183.stm [Accessed 21 April 2018].

Beach, D., 2017. 'Process-Tracing Methods in Social Science'. *Oxford Research Encyclopaedia of Politics*. Available from: <http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-176?print=pdf> [Accessed 29 November 2017].

Beach, D. and Pedersen, R., 2012. 'Case Selection Techniques in Process Tracing and the Implications of Taking the Study of Causal Mechanisms Seriously'. Paper prepared for annual meeting of APSA 2012. Available from: <http://dpsa.dk/papers/Case%20selection%20in%20PT%20-%20Beach%20and%20Pedersen%20-%202nd%20draft.pdf> [Accessed 29 November 2017].

Beach D. and Pedersen, R., 2011. 'What is Process Tracing Actually Tracing? The Three Variants of Process Tracing Methods and Their Uses and Limitations.' Paper prepared for annual meeting of APSA 2011. Available from: https://pure.au.dk/portal/files/40422940/APSA_paper_Beach_and_Pedersen_final.pdf [Accessed 3 November 2020].

Beauchamp, T. and Rosenberg, A., 1981. *Hume and the Problem of Causation*. Oxford: Oxford University Press.

Beaumont, C., 2010. Twitter users send 50 million Tweets per day. *The Telegraph*, Technology, 23 February. Available from: <https://www.telegraph.co.uk/technology/twitter/7297541/Twitter-users-send-50-million-tweets-per-day.html> [Accessed 20 July 2018].

- Beck, U., 2009. 'Critical Theory of World Risk Society: A Cosmopolitan Vision'. *Constellations*, 16 (1), pp. 3-22. Available from: <https://www.jus.uio.no/smr/om/aktuelt/arrangementer/2015/urlich-beck-cosmopolitan-view.pdf> [Accessed 3 February 2019].
- Beck, U., 2006. 'Living in the World Risk Society'. *Economy and Society*, 35 (3), pp. 329-345.
- Beck, U., 2002. 'The Terrorist Threat: World Risk Society Revisited'. *Theory, Culture & Society*, 19 (4), pp. 39-55.
- Beck, U., 1992. *Risk Society: Towards a new Modernity*. London: Sage.
- Beckett, C., 2016. Fanning the Flames: Reporting on Terror in a Networked World. Tow Centre for Digital Journalism, Columbia Graduate School of Journalism, September 22. Available from: https://www.cjr.org/tow_center_reports/coverage_terrorism_social_media.php [Accessed 23 September 2020].
- Bedau, M., 2008. 'Is Weak Emergence Just in the Mind?' *Minds and Machines*, 18 (4), pp. 443-459.
- Bell, J. Boyer, 1978. 'Terrorist Scripts and Live-Action Spectaculars'. *Columbia Journalism Review*, 17 (1), pp. 47-50.
- Bellhouse, D. R., 2004. 'The Reverend Thomas Bayes, FRS: A Biography to Celebrate the Tercentenary of his Birth'. *Statistical Science*, 19 (1), pp. 3-43. Available from: <https://www.york.ac.uk/depts/maths/histstat/bayesbiog.pdf> [Accessed 27 October 2020].
- Benbya, H. and McKelvey, B., 2006a. 'Towards a Complexity Theory of Information Systems Development'. *Information Technology & People*, 19 (1), pp. 12-34.
- Benbya, H. and McKelvey, B., 2006b. 'Using Co-evolutionary and Complexity Theories to Improve IS Alignment: A Multi-level Approach'. *Journal of Information Technology*, 21 (4), 284-298.
- Benjamin, D. and Simon, S., 2003. *The Age of Sacred Terror: Radical Islam's War Against America*. New York: Random House.
- Bennett, C. H., 1988. 'Logical Depth and Physical Complexity'. In: R. Herken, ed., *The Universal Turing Machine: A Half-Century Survey*. Oxford: Oxford University Press.
- Bennett, A. and Checkel, J., 2014. *Process Tracing: From Metaphor to Analytical Tool*. Cambridge: Cambridge University Press.
- Bennett, A. and George, A., 1997. 'Process Tracing in Case Study Research'. MacArthur Foundation Workshop on Case Study Methods, October 17-19, 1997. Available from: https://www.uzh.ch/cmsssl/suz/dam/jcr:00000000-5103-bee3-0000-000059b16b9d/05.19.bennett_george.pdf [Accessed 5 October 2017].
- Bergen, P., Sterman, D. and Salyk-Virk, M., 2019. *Terrorism in America 18 years after 9/11*. Washington, DC: New America. Available from: https://d1y8sb8igg2f8e.cloudfront.net/documents/Terrorism%20in%20America%2018%20Years%20After%209/11_2019-09-16_183612.pdf [Accessed 22 June 2022].
- Berger, J. M., 2014. How ISIS Games Twitter. *The Atlantic*, 16 June. Available from: <http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/> [Accessed 20 April 2018].

Berger, J. M. and Morgan, J., 2015. 'The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter'. Analysis Peter No. 20, Brookings, March. Available from: https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf [Accessed 29 July 2022].

Berners-Lee, T. and Fischetti, M., 1999. *Weaving the Web: The Original Design and Ultimate Destiny of the Worldwide Web, by its Inventor*. New York: Harper. Available from: <https://www.scribd.com/document/371687132/Tim-Berners-Lee-Weaving-the-Web-The-Original-Design-and-Ultimate-Destiny-of-the-World-Wide-Web-PDF-TKRG> [Accessed 2 February 2023].

Binder, L., 1966. *Politics in Lebanon*. New York: Wiley.

Bin Adam, F., 2001. 'The Concept of Khilāfah According to Selected Sunni and Shia Qur'anic Commentaries'. PhD thesis. University of Leeds, April. Available from: <https://core.ac.uk/download/43666.pdf> [Accessed 31 July 2022].

Bin Laden, O., 2004. 'God knows it did not cross our minds to attack the towers'. Text of videotaped address by Osama bin Laden, translated by Reuters and first aired by Al Jazeera. *The Guardian*, 30 October. Available from: <https://www.theguardian.com/world/2004/oct/30/alqaida.september11> [Accessed 1 February 2023].

Bishwas, S. K., 2011. 'Conceptualization of Organisation Vitality based on Strategic Knowledge Management'. *Global Journal of e-Business and Knowledge Management*, 7 (1), pp. 45-52. Available from: https://www.researchgate.net/publication/278031191_Conceptualization_of_Organization_Vitality_based_on_Strategic_Knowledge_Management [Accessed 15 November 2020].

Black, D., 2004. 'The Geometry of Terrorism'. *Sociological Theory*, 22 (1), pp. 14-25.

Black, I., 2014. Isis breach of Iraq-Syria border merges two wars into one 'nightmarish reality'. *The Guardian*, 18 June. Available from: <http://www.theguardian.com/world/2014/jun/18/isis-iraq-syria-two-wars-one-nightmare> [Accessed 21 July 2018].

Blanford, N., 2017. 'Hezbollah's Evolution: From Lebanese Militia to Regional Player'. Middle East Institute Counterterrorism Series, Policy Paper 4, November. Available from: https://www.mei.edu/sites/default/files/publications/PP4_Blanford_Hezbollah.pdf [Accessed 8 November 2021].

Blanford, N., 2006. *Killing Mr Lebanon: The Assassination of Rafik Hariri and its impact on the Middle East*. London: I. B. Tauris.

Blatter, J. and Haverland, M., 2014. 'Case Studies and (Causal-) Process Tracing'. In: I. Engeli and C. Rothmayr, eds, *Comparative Policy Studies: Conceptual and Methodological Challenges*. Basingstoke, UK: Palgrave Macmillan, pp. 59-83. Available from: https://www.researchgate.net/publication/304869549_Case_Studies_and_Causal-Process_Tracing [Accessed 3 September 2020].

Blatter, J. and Haverland, M., 2012. *Designing Case Studies: Explanatory Approaches in Small-N Research*. Basingstoke, UK: Palgrave Macmillan.

Bodetti, A., 2016. 'The Taliban's Latest Battlefield: Social Media'. *The Diplomat*, 8 September. Available from: <https://thediplomat.com/2016/09/the-talibans-latest-battlefield-social-media/> [Accessed 19 October 2019].

Börner, K., Boyack, K., Milojevic, S. and Morris, S., 2012. 'An Introduction to Modelling Science: Basic Model Types, Key Definitions, and a General Framework for the Comparison of Process Models'. In: A. Scharnhorst, K. Börner and P. van den Besselaar, eds, *Models of Science Dynamics: Encounters Between Complexity Theory and Information Sciences*. Berlin/Heidelberg, Germany: Springer-Verlag, pp. 3-22.

Boucek, C., 2007. 'Saudi Arabia Aligns with US to Rout Al-Qaeda Operatives'. Royal United Services Institute (RUSI), 19 November. Available from: <https://rusi.org/publication/saudi-arabia-aligns-us-rout-al-qaeda-operatives> [Accessed 31 January 2022].

Bourekba, M., 2018. 'Revisiting the Barcelona Attacks: Reactions, Explanations and Pending Discussions'. Barcelona, Spain: CIDOB (Barcelona Centre for International Affairs), February. Available from: https://www.cidob.org/en/content/download/68601/2078803/version/32/file/CIDOB%20REPORT_02_ENGLISH.pdf [Accessed 5 July 2022].

Bowie, N., 2021. '40 Terrorism Databases and Data Sets: A New Inventory'. *Perspectives on Terrorism*, 15 (2), pp. 147-161. Available from: <https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2021/issue-2/bowie.pdf> [Accessed 27 June 2021].

Box, G., 1979. 'Robustness in the Strategy of Scientific Model Building'. In: R. L. Launer and G. N. Wilkinson, eds, *Robustness in Statistics*. Academic Press, Cambridge, MA, pp. 201-236.

Boyd, D. and Ellison, N. 2007. 'Social Network Sites: Definition, History, and Scholarship'. *Journal of Computer-Mediated Communication*, 13 (1), pp. 210-230. Available from: <https://academic.oup.com/jcmc/article/13/1/210/4583062/> [Accessed 5 October 2019].

Boyle, A., 2013. Sputnik started space race, anxiety. NBCNews.com. Available from: http://www.nbcnews.com/id/3077890/ns/technology_and_science-space/t/sputnik-started-space-race-anxiety/#.WhhRU1WnHIU [Accessed 24 November 2017].

Brachman, J., 2006. 'High-Tech Terror: Al-Qaeda's Use of New Technology'. *The Fletcher Forum of World Affairs*, 30 (2), pp. 149-164. Available from: <http://www.dtic.mil/dtic/tr/fulltext/u2/a458499.pdf> [Accessed 26 April 2018].

Brady, H. E., 2011. 'Causation and Explanation in Social Science'. In: R. E. Goodin, ed, *The Oxford Handbook of Political Science*. Oxford: Oxford University Press, pp. 1005-1053. Available from: <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199604456.001.0001/oxfordhb-9780199604456-e-049> [Accessed 12 June 2021].

Bremer, L., P., 2001. 'A New Strategy for the New Face of Terrorism'. *The National Interest*, Thanksgiving, Special 9/11 Issue. Available from: <http://nationalinterest.org/article/a-new-strategy-for-the-new-face-of-terrorism-843> [Accessed 11 June 2018].

Bresnahan, T., 2010. 'General Purpose Technologies'. In: B. Hall and N. Rosenberg, eds, *Handbook of the Economics of Innovation*, Vol 2. Amsterdam: Elsevier, pp. 761-761.

Brocardus, 1906 [1332]. 'Directorium ad Passagium Faciendum'. In: *Receuil des Historiens des Croisades* (RHC), E, Documents Arméniens, ii. Paris 1906, pp. 496-497. Available from: <https://gallica.bnf.fr/ark:/12148/bpt6k51558x/f4.image.r=.langEN> [Accessed 5 November 2019].

Brooking, E. and Singer, P., 2016. 'War Goes Viral: How Social Media is being Weaponized Across the World'. *The Atlantic*, November. Available from: <https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/> [Accessed 21 July 2018].

Bryden, J., 2019. Karina Gould, Democratic Institutions Minister, Says 'Wild West Online Era' Can't Continue. *Huffpost*, 27 May. Available from: https://www.huffingtonpost.ca/entry/karina-gould-social-media_ca_5cec5442e4b0512156f65875?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xllmNvbS8&guce_referrer_sig=AQAAAMJPDh8qwbIGd26yHyJ6xCyp8C7taRPYavpmar2iBDO7j8o4psJN4BIDYNpPtwm18e2xwAJBdMvk-18rf54Exef0UcUoOWIRUXHqdTBAKfdqr5OM9NTpcOoovri47FX6hTNxCqprBheH5gSTd1xfjaW0MM0Y1ZRadxw1SXTWSmH [Accessed 21 June 2020].

Brzezinski, M., 2002. Operation Bojinka's Bombshell. *Toronto Star*, 2 January. Available from: https://web.archive.org/web/20020614124327/http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar%2FLayout%2FArticle_PrintFriendly&c=Article&cid=1009926464027 [Accessed 2 June 2022].

Bunt, G., 2003. *Islam in the Digital Age*. London: Pluto Press.

Bunzel, C., 2015. 'From Paper State to Caliphate: The Ideology of the Islamic State'. The Brookings Project on US Relations with the Islamic World, Analysis Paper No. 19, March. Available from: <https://www.brookings.edu/wp-content/uploads/2016/06/the-ideology-of-the-islamic-state.pdf> [Accessed 19 June 2022].

Burke, J., 2007. *Al-Qaeda: The True Story of Radical Islam*. Third edition. London: Penguin Books.

Burkhardt, M. and Brass, D., 1990. 'Changing Patterns or Patterns of Change: The Effects of a Change in Technology on Social Network Structure and Power'. *Administrative Science Quarterly*, 35 (1), pp. 104-127. Available from: https://pdfs.semanticscholar.org/3c2e/975382ec7f61116d275f5b56ade0189971df.pdf?_ga=2.180835175.1372907413.1605455818-697649069.1598700249 {accessed 15 November 2020}.

Burnett, J. and Whyte, D., 2005. 'Embedded Expertise and the New Terrorism'. *Journal for Crime, Conflict and the Media*, 1 (4), pp. 1-18. Available from: https://www.diplomatie.gouv.fr/IMG/pdf/expertise_terrorisme.pdf [Accessed 20 September 2020].

Byman, D., 2015. Comparing Al Qaeda and ISIS: Different Goals, Different Targets. *Brookings*, 29 April. Available from: <https://www.brookings.edu/testimonies/comparing-al-qaeda-and-isis-different-goals-different-targets/> [Accessed 10 November 2020].

Byman, D., 2003. 'Should Hezbollah Be Next?' *Foreign Affairs*, 82 (6), pp. 54-66. Available from: <https://www.brookings.edu/wp-content/uploads/2016/06/byman20031101.pdf> [Accessed 2 March 2021].

Byman, D. and Williams, J., 2015. ISIS vs. Al Qaeda: Jihadism's Global Civil War. *Brookings Institution*, 24 February. Available from: <https://www.brookings.edu/articles/isis-vs-al-qaeda-jihadisms-global-civil-war/> [Accessed 24 June 2018].

Byrne, D., 1998. *Complexity and the Social Sciences: An Introduction*. London: Routledge.

- Caldarelli, G. and Catanzaro, M., 2012. *Networks: A Very Short Introduction*. Oxford: Oxford University Press.
- Cambanis, T., 2010. Grand Ayatollah Fadlallah Dies, Shiite Cleric, Dies at 75. *The New York Times*, 4 July. Available from: <https://www.nytimes.com/2010/07/05/world/middleeast/05fadlallah.html> [Accessed 3 February 2021].
- Campbell, D., 1966. 'Pattern Matching as an Essential in Distal Knowing'. In: K. Hammond (ed.), *The Psychology of Egon Brunswik*. New York: Holt, Rinehart & Winston, pp. 81-106.
- Carley, K., 2002. 'Inhibiting Adaptation'. In: Proceedings of the 2002 Command and Control Research and Technology Symposium held at the Naval Postgraduate School, Monterey, CA. Available from: http://www.casos.cs.cmu.edu/publications/papers/carley_2002_inhibitingadaptation.pdf [Accessed 24 April 2018].
- Carley, K., Diesner, J., Reminga, J. and Tsvetovat, M., 2004. 'An Integrated Approach to the Collection and Analysis of Network Data'. Centre for Computational Analysis of Social and Organizational Systems, Carnegie Mellon University, Pittsburg, PA. Available from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.445.7368&rep=rep1&type=pdf> [Accessed 16 July 2020].
- Carley, K., Dombroski, M., Tsvetovat, M., Reminga, J. and Kamneva, N., 2003. 'Destabilizing Dynamic Covert Networks'. *Proceedings of the 8th International Command and Control Research and Technology Symposium*. Washington, DC: National Defense War College. Available from: http://www.casos.cs.cmu.edu/publications/papers/a2c2_carley_2003_destabilizing.pdf [Accessed 10 April 2018].
- Carley, K., Lee, J.S. and Krackhardt, D., 2002. 'Destabilizing Networks'. *Connections*, 24 (3), pp. 79-92. Available from: <https://www.andrew.cmu.edu/user/krack/documents/pubs/2001/2001%20Destabilizing%20Networks.pdf> [Accessed 24 April 2018].
- Carnegie Council 2016. The Symbiotic Relationship between Western Media and Terrorism. Carnegie Council for Ethics in International Affairs, 24 May. Available from: https://www.carnegiecouncil.org/publications/ethics_online/0117 [Accessed 9 April 2018].
- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J. and Neville, A., 2014. 'The Use of Triangulation in Qualitative Research'. *Oncology Nursing Forum*, 41 (5), pp. 545-547.
- Castells, M., 1996. *The Information Age: Economy, Society and Culture. Volume 1. The Rise of Network Society*. Oxford: Blackwell.
- Castells, M., 2010. *The Rise of the Network Society*. Second edition with a new preface. Malden, MA: Wiley-Blackwell.
- Castells, M., 2004. 'Informationalism, Networks, and the Network Society: A Theoretical Blueprint'. In: M. Castells, ed., *The Network Society: A Cross-Cultural Perspective*. Northampton, MA: Edward Elgar Publishing, pp. 3-45. Available from: <https://annenbergl.usc.edu/sites/default/files/2015/04/28/Informationalism%2C%20Networks%20and%20the%20Network%20Society.pdf> [Accessed 15 February 2018]. Page numbers refer to online version.
- Castells, M., 1997. *The Power of Identity*. Oxford: Blackwell.

- Caston, L., Leonard, R., Mouton, C., Ohlandt, C., Moore, C., Conley, R. and Buchan, G., 2014. The Future of the US Intercontinental Ballistic Missile Force. Santa Monica, CA: RAND. Available from: <https://www.rand.org/pubs/monographs/MG1210.html> [Accessed 9 October 2022].
- Castrodeza, C., 1978. 'Evolution, Complexity, and Fitness'. *Journal of Theoretical Biology*, 71 (3), pp. 469-471.
- Cengiz, M., 2021. 'Beheading as a Signature Method of Jihadist Terrorism from Syria to France'. Terrorism, Transnational Crime and Corruption Centre (TraCCC), Schar School of Policy and Government, George Mason University. Available from: <https://tracc.gmu.edu/wp-content/uploads/2021/04/BEHEADING-AS-A-SIGNATURE-METHOD-OF-JIHADIST-TERRORISM-FROM-SYRIA-TO-FRANCE-ESJ-4.pdf> [Accessed 21 April 2022].
- Cerny, P., 2005. 'Terrorism and the New Security Dilemma'. *Naval War College Review*, 58 (1), pp. 11-33. Available from: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1950&context=nwc-review> [Accessed 5 February 2019].
- Chaliand, G. and Blin, A., 2007a. 'From 1968 to Radical Islam'. In: G. Chaliand and A. Blin, eds, *The History of Terrorism: From Antiquity to Al Qaeda*. Berkeley, CA: University of California Press, pp. 221-254.
- Chaliand, G. and Blin, A., 2007b. 'Zealots and Assassins'. In: G. Chaliand and A. Blin, eds., *The History of Terrorism: From Antiquity to Al Qaeda*. Berkeley, CA: University of California Press, pp. 55-78.
- Chan, S., 2001. 'Complex Adaptive Systems'. ESD.83 Research Seminar in Engineering Systems, MIT, 31 October. Available from: <http://web.mit.edu/esd.83/www/notebook/Complex%20Adaptive%20Systems.pdf> [Accessed 10 August 2018].
- Chandler, A., Jr., 1977. *The Visible Hand: The Managerial Revolution in American Business*. Cambridge, MA: Harvard University Press.
- Chen, G., Wang, X. and Li, X., 2015. *Fundamentals of Complex Networks: Models, Structures and Dynamics*. Singapore: Wiley.
- Chasdi, R., 2014. 'Al-Qaeda 3.0': Fusion of terrorism and Guerrilla Warfare. The World Post, 10 June. Available from: http://www.huffingtonpost.com/dr-richard-chasdi/alqaeda-30-fusion-of-terr_b_5923264.html [Accessed 6 April 2016].
- Chitty, N., Rush, R. and Semanti, M., 2003. *Studies in Terrorism: Media Scholarship and the Enigma of Terror*. Penang, Malaysia: Southbound.
- Choi, T., Dooley, K. and Rungtusanatham, M., 2001. 'Supply Networks and Complex Adaptive Systems'. *Journal of Operations Management*, 19 (3), pp. 351-366.
- Chomsky, N., 2002. *Media Control: The Spectacular Achievements of Propaganda*. Second edition. New York: Seven Stories Press.
- Chomsky, N., 1957. *Syntactic Structures*. 'S-Gravenhage, Netherlands: Mouton & Co.

Chulov, M., 2019. The Rise and Fall of the Isis 'caliphate'. *The Guardian*, 24 March. Available from: <https://www.theguardian.com/world/2019/mar/23/the-rise-and-fall-of-the-isis-caliphate> [Accessed 21 June 2022].

Chulov, M., Hawramy, F. and Ackerman, S., 2014. Iraq Army Capitulates to ISIS Militants in Four Cities. *The Guardian*, 12 June. Available from: <https://www.theguardian.com/world/2014/jun/11/mosul-isis-gunmen-middle-east-states> [Accessed 3 July 2022].

Clancy, S. and Brown, W., 2008. 'Translation: DNA to mRNA to Protein'. *Nature Education*, 1 (1). Available from: <https://www.nature.com/scitable/topicpage/translation-dna-to-mrna-to-protein-393/#> [Accessed 9 November 2022].

Clapper, J. R., 2016. *Worldwide Threat Assessment of the US Intelligence Community*. Statement to Senate Armed Services Committee, 9 February. Available from: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf [Accessed 29 February 2020].

Clarke, C., 2017. 'How Hezbollah Came to Dominate Information Warfare'. *The RAND Blog*, 19 September. Available from: <https://www.rand.org/blog/2017/09/how-hezbollah-came-to-dominate-information-warfare.html> [Accessed 19 October 2021].

Clarke, C., Serena, C. and Amarasingam, A., 2017. Beware the New Mujahideen: The Threat from Future Jihadist Networks. *TheRANDblog*, 14 March. Available from: <https://www.rand.org/blog/2017/03/beware-the-new-mujahideen-the-threat-from-future-jihadist.html> [Accessed 6 July 2022].

Cluskey, P., 2016. Killing of Abu Muhammad al-Adnani Silences Influential Islamic State Voice. *The Irish Times*, 31 August. Available from: <https://www.irishtimes.com/news/world/middle-east/killing-hbv-bcof-abu-muhammad-al-adnani-silences-influential-islamic-state-voice-1.2774720> [Accessed 21 July 2018].

Cochrane, P., 2007. 'Bombs and Broadcasts: Al Manar's Battle to Stay on Air'. *Arab Media & Society*, February. Available from: https://www.arabmediasociety.com/wp-content/uploads/2017/12/20070312145543_AMS1_Paul_Cochrane-2.pdf [Accessed 10 November 2021].

Cohen, J., 2015. 'Digital Counterinsurgency: How to Marginalize the Islamic State Online'. *Foreign Affairs*, November/December issue. Available from: <https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency> [Accessed 20 April 2018].

Cohen-Almagor, R., 2005. 'Media Coverage of Acts of Terrorism: Troubling Episodes and Suggested Guidelines'. *Canadian Journal of Communication*, 30 (3). Available from: <http://www.cjc-online.ca/index.php/journal/rt/prnterFriendly/1579/1734> [Accessed 19 April 2018].

Cohn, M., 2011. Social Media vs Social Networking. Available from: <https://www.compukol.com/social-media-vs-social-networking/> [Accessed 13 February 2020].

Cohn, N., 2004. *The Pursuit of the Millennium: Revolutionary Millenarians and Mystical Anarchists of the Middle Ages*. London: Pimlico.

- Coleman, J, Katz, E. and Menzel, H., 1957. 'The Diffusion of an Innovation among Physicians'. *Sociometry*, 20 (1), pp. 253-270. Available from: https://www.suz.uzh.ch/dam/jcr:ffffff-f952-f950-ffff-ffffd58273/03.18_coleman_et-al_57.pdf [Accessed 13 November 2021].
- Coll, S. and Glasser, S., 2005. Terrorists Turn to the Web as Base of Operations. *The Washington Post*, 7 August. Available from: <https://www.washingtonpost.com/archive/politics/2005/08/07/terrorists-turn-to-the-web-as-base-of-operations/4e52c8f9-b42b-4100-817b-09e206b3f816/> [Accessed 30 October 2022].
- Collier, D. and Mahoney, J., 1996. 'Insights and Pitfalls: Selection Bias in Qualitative Research'. *World Politics*, 49 (1), pp. 56-91.
- Collins, S., 2010. 'Indigenous Rights and Internal Wars: The Chiapas Conflict at 15 Years'. *The Social Science Journal*, 47 (4), pp. 773-788. Available from: <http://whereareyouquetzalcoatl.com/RioHondo/humn125/Collins2010.pdf> [Accessed 5 February 2020].
- Combs, C. and Slann, M., 2007. *Encyclopedia of Terrorism*. Revised edition. Facts on File Library of World History. New York, NY: Facts on File.
- Conitzer, V. and Sandholm, T., 2014. 'Complexity of Mechanism Design'. Proceedings of the Eighteenth Conference on Uncertainty in Artificial Intelligence, August. Available from: <https://arxiv.org/ftp/arxiv/papers/1408/1408.1486.pdf> [Accessed 2 November 2022].
- Constine, J., 2017. Facebook now has 2 billion monthly users ... and responsibility. *Techcrunch.com*, 27 June. Available from: <https://techcrunch.com/2017/06/27/facebook-2-billion-users/> [Accessed 20 July 2018].
- Conway, M., 2017a. 'Researching violent extremism and terrorism online: challenges and directions'. *Terrorism and Social Media: An International Conference*, keynote address. Swansea University Bay Campus, 27-28 June.
- Conway, M., 2017b. 'Islamic State's Social Media Moment has Passed'. *Demos Quarterly*. November 1.
- Conway, M., 2008a. 'Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures'. Working Papers in International Studies, Paper No. 2008-5. Centre for International Studies, Dublin City University, Ireland. Available from: <http://doras.dcu.ie/2142/1/2008-5.pdf> [Accessed 24 February 2021].
- Conway, M., 2008b. 'Terror TV? An Exploration of Hizbollah's Al-Manar Television'. In: J.F. Forest, ed., *Countering Terrorism and Insurgency in the 21st Century*. Westport, CT: Greenwood Publishing Group, pp. 401-419. Available from: <http://doras.dcu.ie/2147/1/2008-10.pdf> [Accessed 5 October 2019].
- Conway, M., 2007. 'Terrorism and the Making of the "New Middle East": New Media Strategies of Hizbollah and al Qaeda'. In: P. Seib, ed., *New Media and the New Middle East*. New York: Palgrave Macmillan, pp. 235-258. Available from: http://doras.dcu.ie/503/1/new_media_2007.pdf [Accessed 12 December 2017].
- Conway, M., 2005. 'Cybercortical Warfare: Hizbollah's Internet Strategy'. In: S. Oates, D. Owen and R. Gibson, eds, *The Internet and Politics: Citizens, Voters and Activists*. London: Routledge, pp. 100-

117. Available from: <http://doras.dcu.ie/2145/1/2008-8.pdf> [Accessed 6 August 2017]. Page numbers refer to online version.

Conway, M., 2004. 'Terrorism and (Mass)Communication: From Nitro to the Net'. *The World Today*, 60 (8/9), pp. 19-22.

Conway, M., 2003. 'Terrorism and IT: Cyberterrorism and Terrorist Organizations Online'. Paper presented at International Studies Association (ISA) annual international convention, Portland, Oregon, USA, 25 February- 1 March. Available from: http://doras.dcu.ie/502/1/terrorism_it_2003.pdf [Accessed 18 July 2018].

Conway, M., 2003a. 'Cybercortical Warfare: The Case of Hizbollah.org'. Paper prepared for the European Consortium for Political Research (ECPR) Joint Sessions of Workshops, Edinburgh, 28 March – 2 April. Available from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.189.2457&rep=rep1&type=pdf> [Accessed 23 February 2018].

Conway, M. and McInerney, L., 2008. 'Jihadi Video and Auto-Radicalisation: Evidence from an Exploratory YouTube Study'. In: *Intelligence and Security Informatics*, proceedings of the first European conference, EuroISI, Esbjerg, Denmark, December 3-5. Berlin: Springer, pp. 108-118. Available from: http://doras.dcu.ie/2253/2/youtube_2008.pdf [Accessed 21 July 2018].

Copeland, T., 2001. 'Is the "New Terrorism" Really New? An Analysis of the New Paradigm for Terrorism'. *The Journal of Conflict Studies*, 21 (2), pp. 7-27.

Cordesman, A., 2006. 'Preliminary "Lessons" in the Israeli-Hezbollah War'. Working draft, second edition. Washington, DC: Centre for Strategic and International Studies. Available from: <http://www.mafhoum.com/press9/286P6.pdf> [Accessed 4 July 2022].

Correll, C., Stetka, B. and Harsinay, A., 2018. Rare and Unusual Psychiatric Syndromes: A Primer. Medscape.com, 23 July. Available from: https://www.medscape.com/viewarticle/899520_5 [Accessed 2 January 2021].

Crelinsten, R. D., 1987. 'Power and Meaning: Terrorism as a Struggle over Access to the Communication Structure'. In: P. Wilkinson and A. M Stewart, eds, *Contemporary Research on Terrorism*. Aberdeen: Aberdeen University Press, pp. 419-450.

Crenshaw, M., 2018. 'Time for Peace Talks with ISIS and Al Qaeda?' *Foreign Policy*, 19 September. Available from: <https://foreignpolicy.com/2018/09/19/time-for-peace-talks-with-isis-and-al-qaeda/> [Accessed 24 September 2018].

Crenshaw, M., 2010a. 'Innovation: Decision Points in the Trajectory of Terrorism'. In: M. Rasmussen and M. Hafez, eds, *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators*. The Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Report Number ASCO 2010-019, pp. 35-50.

Crenshaw, M., 2010b. 'Mapping Terrorist Organisations.' Research Project funded by the National Science Foundation as part of the US Department of Defense Minerva Initiative. Available from: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/res/mapping_terrorist_organizations.pdf [Accessed 2 May 2020].

Crenshaw, M., 2007. 'The Debate over "New" vs. "Old" Terrorism'. Paper prepared for the annual meeting of the American Political Science Association, Chicago, Illinois, USA, 30 August – 2

- September. Available from:
http://www.start.umd.edu/sites/default/files/files/publications/New_vs_Old_Terrorism.pdf
 [Accessed 11 June 2018].
- Crenshaw, M., 1987. 'Theories of terrorism: Instrumental and organisational approaches'. *Journal of Strategic Studies*, 10 (4), pp. 13-31.
- Crenshaw, M., 1981. 'The Causes of Terrorism'. *Comparative Politics*, 13 (4), pp. 379-399. Available from: <http://courses.kvasaheim.com/hist319a/docs/Crenshaw%201981.PDF> [Accessed 21 July 2018].
- Cresser, J. D., 2011. *Quantum Physics Notes*. North Ryde, NSW, Australia: Macquarie University.
- Crick, F., 1970. 'Central Dogma of Molecular Biology'. *Nature*, 227 (1), pp. 561-563.
- Crozier, M. and Friedberg, E., 1980. *Actors and Systems: the Politics of Collective Action*. Chicago, IL: University of Chicago Press.
- Culf, A., 1996. The Global News Frenzy. *The Observer*, 2 June, T16.
- Cuthbertson, A., 2014. Iraq Crisis: ISIS Launch Twitter App to Recruit, Radicalise and Raise Funds. *International Business Times*, 18 June. Available from: <https://www.ibtimes.co.uk/iraq-crisis-isis-launch-twitter-app-recruit-radicalise-raise-funds-1453154> [Accessed 27 January 2019].
- Damon, C. and Macy, M., 2007. 'Complex Contagions and the Weakness of Long Ties'. *American Journal of Sociology*, 113 (3), pp. 702-734. Available from: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1603&context=asc_papers [Accessed 13 November 2021].
- Daniş M. F., 2019. 400 Years of Ottoman Rule in Lebanon: An Uneasy Negotiation. *Daily Sabah*, 12 September. Available from: <https://www.dailysabah.com/op-ed/2019/09/12/400-years-of-ottoman-rule-in-lebanon-an-uneasy-negotiation> [Accessed 31 January 2021].
- David, L., 2002. 'Sputnik 1: The Satellite that Started it all.' Space.com, 4 October. Available from: https://web.archive.org/web/20060216013800/http://www.space.com/missionlaunches/sputnik_4_5th_anniversary_021004.html [Accessed 7 October 2021].
- Davidson, J., 1988. *An Introduction to TCP/IP*. New York: Springer Verlag.
- Davies, P., 2019a. Interviewed on *Today*, BBC Radio 4, 12 February.
- Davies, P., 2019b. *The Demon in the Machine: How Hidden Webs of Information are Solving the Mystery of Life*. London: Penguin UK.
- Davies, M. L., 2016. *How History Works: The Reconstitution of a Human Science*. Abingdon, Oxon, UK: Routledge.
- Dawisha, A. I., 1978. 'Syria's Intervention in Lebanon, 1975-1976.' *Jerusalem Journal of International Relations*, 3 (Winter-Spring 1978), pp. 245-263.
- Dean, G., Bell, P. and Newman, J., 2012. 'The Dark Side of Social Media: Review of Online Terrorism'. *Pakistan Journal of Criminology*, 3 (3), pp. 107-126. Available from: v

https://www.researchgate.net/publication/279419560_The_dark_side_of_social_media_review_of_online_terrorism [Accessed 20 July 2018]. Page references relate to online numbering.

Decker, W. and Rainey, D., 1980. 'Terrorism as Communication'. Paper presented at the annual meeting of the Speech Communication Association, New York, November 1980. Available from: <https://files.eric.ed.gov/fulltext/ED196091.pdf> [Accessed 5 December 2022].

Defence Update, 2006. INS Hanit Suffers Iranian Missile Attack. 16 July, 2006, updated 17 July. Available from: <https://web.archive.org/web/20150722010225/http://www.defense-update.com/2006/07/ins-hanit-suffers-iranian-missile.html> [Accessed 10 September 2022].

De Landa, M., 2014. *A Thousand Years of Nonlinear History*. First paperback edition, eighth printing. New York: Zone Books.

Del Cid Gomez, J.-M., 2010. 'A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates'. *Perspectives on Terrorism*, 4 (4), pp. 3-27. Available from: <https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2010/issue-4/a-financial-profile-of-the-terrorism-of-al-qaeda-and-its-affiliates--juan-miguel-del-cid-gomez.pdf> [Accessed 23 May 2022].

Della Porta, D., 2008. 'Comparative Analysis: Case-oriented versus variable-oriented research'. In: D. Della Porta and M. Keating, eds *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective*. Cambridge: Cambridge University Press, pp. 198-222.

De Moraes, L., 1998. Ted Turner, Trying to Put his Spin on Planet Earth. *The Washington Post*, 24 September, B1.

Denning, D., 2009. 'Terror's Web: How the Internet is Transforming Terrorism'. In: Y. Jewkes and M. Yar, eds, *Handbook of Internet Crime*, pp. 1-34. Portland, OR: Willan Publishing. Available from: <http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf> [Accessed 1 February 2023]. Page numbers refer to online version.

Denning, D., 1999. *Information Warfare and Security*. Boston, MA: Addison-Wesley.

Department of Homeland Security 2010. Terrorist Use of Social Networking Sites : Facebook Case Study. Public Intelligence, 5 December. Available from: <https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/> [Accessed 15 February 2020].

Der Spiegel, the reporters, writers and editors, 2001. *Inside 9/11: What Really Happened*. New York: St Martin's Paperbacks.

Deuchars, R., 2010. 'Deleuze, De Landa and Social Complexity: Implications for the "International"'. *Journal of International Political Theory*, 6 (2), pp. 161-187. Available from: https://www.researchgate.net/publication/271240243_Deleuze_DeLanda_and_Social_Complexity_Implications_for_the_'International' [Accessed 16 October 2019].

Dewar, J., 1998. *The Information Age and the Printing Press: Looking Backward to See Ahead*. Santa Monica, CA: RAND. Available from: <https://www.rand.org/pubs/papers/P8014.html> [Accessed 1 February 2023].

Dillon, M. and Lobo-Guerrero, L., 2008. 'Biopolitics of Security in the 21st Century: An Introduction'. *Review of International Studies*, 34 (2), pp. 265-292. Available from:

http://eprints.lanacs.ac.uk/26979/1/Biopolitics_of_security_in_the_21st_century.pdf [Accessed 28 January 2018].

Dillon, M., 2002. 'Network Society, Network-Centric Warfare and the State of Emergency'. *Theory, Culture and Society*, 19 (4), pp. 71-79. Available from:

http://eprints.lanacs.ac.uk/809/1/Microsoft_Word_-_State_of_Emergency_TCS_.pdf [Accessed 24 November 2017]. Page numbers refer to online version.

Dolnik, A., 2007. *Understanding Terrorist Innovation: Technology, Tactics and Global Trends*. London: Routledge.

Don, B., Frelinger, D., Gerwehr, S., Landree, E. and Jackson, B., 2007. *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*. Santa Monica, CA: RAND. Available from:

https://www.rand.org/pubs/technical_reports/TR454.html [Accessed 3 July 2020].

Dooley, K., 2004. 'Complexity Science Models of Organizational Change'. In: S. Poole and A. van de Ven, eds, *Handbook of Organizational Change and Development*. Oxford: Oxford University Press, pp. 354-373. Available from:

https://www.researchgate.net/publication/280645784_Complexity_science_models_of_organizational_change_and_innovation [Accessed 26 February 2019]. Page numbers refer to online version.

Dooley, K., 2002. 'Organizational Complexity'. In: M. Warner, ed., *International Encyclopaedia of Business and Management*. London: Thompson Learning, pp. 5013-5022.

Doudna, J., 2020. 'The Promise and Challenge of Therapeutic Genome Editing'. *Nature*, 578 (7794), pp. 229-236. Author manuscript available from:

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8992613/> [Accessed 9 October 2022].

Doudna, J., and Charpentier, E., 2014. 'The New Frontier of Genome Editing with CRISPR – Cas9'. *Science*, 364 (6213).

Downing, K., 2015. *Intelligence Emerging: Adaptivity and Search in Evolving Neural Systems*. Cambridge, MA: The MIT Press. Available from:

<https://www.idi.ntnu.no/emner/it3105/lectures/intem-short.pdf> [Accessed 29 October 2022].

Doyle, M., 1986. 'Liberalism and World Politics'. *The American Political Science Review*, 80 (4), pp. 1151-1169. Available from:

https://is.muni.cz/el/1423/podzim2009/MVZ200/Doyle_Liberalism_World_Politics_APSR_1986.pdf [Accessed 4 April 2018].

Drucker, P., 1999. 'Beyond the Information Revolution'. *The Atlantic*, October. Available from:

<https://www.theatlantic.com/magazine/archive/1999/10/beyond-the-information-revolution/304658/> [Accessed 29 January 2019].

Duchek, S., Raetzke, S. and Scheuch, I., 2019. 'The Role of Diversity in Organizational Resilience: A Theoretical Framework'. *Business Research*, 13 (1), pp. 387-423. Available from:

<https://link.springer.com/content/pdf/10.1007/s40685-019-0084-8.pdf> [Accessed 4 June 2021].

Duffield, M., 2002. 'War as a Network Enterprise: The New Security Terrain and its Implications'. *Cultural Values: The Journal for Cultural Research*, 6 (1&2), pp. 153-165. Available from:

https://pdfs.semanticscholar.org/348c/aa8d088f9cd1c15551952115532b64f6c668.pdf?_ga=2.137563828.54210042.1497197893-1424573576.1497197893 [Accessed 19 December 2017].

Duffy, M., 2008. 'The Surge at Year One'. *Time*, 31 January. Available from: <http://www.time.com/time/magazine/article/0%2C9171%2C1708843%2C00.html> [Accessed 15 June 2022].

Duggan, J., 2016. *System Dynamics Modelling with R*. Cham, Switzerland: Springer.

Duyvesteyn, I., 2004. 'How New is the New Terrorism?' *Studies in Terrorism & Conflict*, 27 (5), pp. 439-454.

Earl, J. and Kimport, K., 2011. *Digitally Enabled Social Change: Activism in the Internet Age*. Cambridge, MA: The MIT Press.

Eckstein, H., 1975. 'Case Study and Theory in Political Science'. In: F. Greenstein and N. Polsby, eds, *Political Science: Scope and Theory*. Handbook of Political Science, Volume 7. Reading, MA: Addison-Wesley, pp. 94-137. Available from: <https://publishing.cdlib.org/ucpressebooks/view?docId=ft0k40037v&chunk.id=d0e2292&toc.depth=1&toc.id=d0e2292&brand=ucpress> [Accessed 4 November 2020].

Ehrlich, P. and Raven, P., 1964. 'Butterflies and Plants: A study in Coevolution'. *Evolution*, 18, pp. 586-608. Available from: <http://www.bio.miami.edu/horvitz/Plant-animal%20interactions%202013/coevolution/required%20readings/for%20the%20discussion/Ehrlich%20and%20Raven%201964.pdf> [Accessed 21 May 2019].

Einstein, A., 1920. *Relativity: The Special and General Theory*. Translated by R. W. Lawson. London: Methuen & Co., Ltd. Available from: <https://www.marxists.org/reference/archive/einstein/works/1910s/relative/relativity.pdf> [Accessed 2 June 2018].

Eisenstein, E., 1979. *The Printing Press as an Agent of Change: Communications and Cultural Transformations in Early-Modern Europe*. New York: Cambridge University Press.

El Damanhoury, K., 2020. Constructing Place Identity: ISIS and Al-Qaeda's Branding Competition Over the Caliphate. *Place Branding and Public Diplomacy*, 16 (1), pp. 265-278. Available from: https://www.researchgate.net/publication/337299879_Constructing_place_identity_ISIS_and_Al-Qaeda's_branding_competition_over_the_Caliphate [Accessed 11 January 2021].

Eldredge, N. and Gould, S., 1972. 'Punctuated Equilibria: An Alternative to Phyletic Gradualism'. In: T. Schopf, ed., *Models in Paleobiology*. San Francisco, CA: Freeman.

El Hoss, S., 2008. 'Peace in Lebanon and the Middle East'. *Contemporary Arab Affairs*, 1 (2), pp. 149-155. Available from: <https://caus.org.lb/wp-content/uploads/2020/06/Peace-in-Lebanon-and-the-Middle-East-1.pdf> [Accessed 31 January 2021].

El Hourri, W., 2012. *The Meaning of Resistance: Hezbollah's Media Strategies and the Articulation of a People*. Amsterdam: Rozenberg Publishers. Available from: <https://dare.uva.nl/search?identifier=1b3d837f-09e1-4b3f-8cb5-fa0bb47ed7fe> [Accessed 12 February 2021].

El Husseini, R., 2010. 'Hezbollah and the Axis of Refusal: Hamas, Iran and Syria'. *Third World Quarterly*, 31 (5), pp. 803-815. Available from:

<https://www.tandfonline.com/doi/pdf/10.1080/01436597.2010.502695?needAccess=true>
[Accessed 11 October 2021].

Elkhodr, M., Shahrestani, S. and Cheung, H., 2016. 'The Internet of Things: New Interoperability, Management and Security Challenges'. *International Journal of Network Security and Its Challenges*, 8 (2), pp. 85-102. Available from: <https://www.airconline.com/ijnsa/V8N2/8216ijnsa06.pdf>
[Accessed 26 September 2020].

Elwell, F., 2020. Elisabeth Eisenstein: On the Printing Press. Video. Available from: <https://www.youtube.com/watch?v=5cwTLrQNA-g> [Accessed 6 November 2020].

Emery, N., Earl, R. and Buettner, R., 2004. 'Terrorist Use of Information Operations'. *Journal of Information Warfare*, 3 (2), pp. 14-26. Available from <https://www.jstor.org/stable/pdf/26502782.pdf?refreqid=excelsior%3A892ed59337cb2c401728d92ffe6fd15d> [Accessed 15 November 2020].

Emmeche, C., 1997. 'Aspects of Complexity in Life and Science'. *Philosophica*, 59 (1), pp. 41-68. Available from: https://pdfs.semanticscholar.org/553e/967c2dc9e53f11af296baaf5b2d12eeb7ed6.pdf?_ga=2.240001793.300458158.1594294437-295058391.1594294437 [Accessed 9 July 2020].

Erdős, P. and Rényi, A., 1959. 'On Random Graphs 1'. *Publicationes Mathematicae*, 6 (1), pp. 290-297. Available from: https://www.renyi.hu/~p_erdos/1959-11.pdf [Accessed 6 May 2020].

Euronews, 2022. Islamic State 'Beatle' gets life sentence for beheadings. Euronews with AP, 29 April. Available from: <https://www.euronews.com/2022/04/29/islamic-state-beatle-gets-life-sentence-for-beheadings> [Accessed 16 June 2022].

Europol, 2019. *Do criminals dream of electric sheep? How technology shapes the future of crime and Law Enforcement*. European Union Agency for Law Enforcement Co-operation, 18 July. Available from: <https://www.europol.europa.eu/newsroom/news/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement> [Accessed 18 July 2019].

Facebook, 2018. Newsroom, Stats, 31 March. Available from: <https://newsroom.fb.com/company-info/> [Accessed 20 July 2018]. Scroll down to 'History', followed by 'Stats'.

Fairfield, T. and Charman, A., 2015. 'Formal Bayesian Process Tracing: Guidelines, Opportunities and Caveats.' LSE Research Online. Working paper. Available from: http://eprints.lse.ac.uk/62368/1/Fairfield_Formal%20Bayesian%20process%20tracing.pdf [Accessed 15 October 2017].

Fanon, F., [1963] 2001. *The Wretched of the Earth*. Preface by Jean-Paul Sartre. London: Penguin.

Farah, D., 2001. Al Qaeda Cash Tied to Diamond Trade. The Washington Post, 2 November. Available from: <https://www.washingtonpost.com/archive/politics/2001/11/02/al-qaeda-cash-tied-to-diamond-trade/93abd66a-5048-469a-9a87-5d2efb565a62/> [Accessed 5 March 2021].

Farrell-Molloy, J. and Macklin, G., 2022. Ted Kaczynski, Anti-Technology Radicalism and Eco-Fascism. International Centre for Counterterrorism, The Hague, 15 June. Available from: <https://icct.nl/publication/ted-kaczynski-anti-technology-radicalism-and-eco-fascism/> [Accessed 6 December 2022].

Fawaz, M., 2013. 'The Role of the Media in a Precarious Plural Democracy'. Georgie State University, 28 May. Available from: https://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1045&context=communication_diss [Accessed 26 October 2021].

FBI, n/d. 9/11 Investigation. Fbi.gov, History. Available from: <https://www.fbi.gov/history/famous-cases/911-investigation> [Accessed 17 April 2022].

Fellman, P. V., 2010. 'The Complexity of Terrorist Networks'. In: A. Minai, D. Braha and Y. Bar-Yam, eds, *Unifying Themes in Complex Systems*, Vol. VI: Proceedings of the Sixth International Conference on Complex Systems. Cham, Switzerland: Springer, pp. 162-169.

Fellman, P. V., 2009. 'Understanding the Complexity of Terrorist Networks'. American Military University, School of Security and Global Studies. Available from: <https://arxiv.org/ftp/arxiv/papers/0907/0907.1683.pdf> [Accessed 24 April 2018].

Fellman, P. V. and Post, J. V., 2010. 'Complexity, Competitive Intelligence and the "First Mover" Advantage'. In: A. Minai, D. Braha, D. and Y. Bar-Yam, eds, *Unifying Themes in Complex Systems*, Vol. VI: Proceedings of the Sixth International Conference on Complex Systems. Cham, Switzerland: Springer, pp. 114-121.

Feltman, J. and Benjamin, D., 2010. Assessing the Strength of Hezbollah. Joint statement to a hearing of the Sub-committee on Near Eastern and South and Central Asian Affairs of the Committee on Foreign Relations of the US Congress, 8 June. Available from: <https://www.govinfo.gov/content/pkg/CHRG-111shrg62141/html/CHRG-111shrg62141.htm> [Accessed 13 October 2021].

Fenton, N., 2012. 'The Internet and Social Networking'. In: J. Curran, N. Fenton and D Freedman, eds, *Misunderstanding the Internet*. Abingdon, Oxon: Routledge, pp. 123-148.

Festinger, L., Riecken, H. and Schachter, S., 1964. *When Prophecy Fails: A Social and Psychological Study of a Modern Group that Predicted the Destruction of the World*. New York: Harper & Row.

Firro, K., 2012. 'Nationalism and Confessionalism: Shi'is, Druzes and Alawis in Syria and Lebanon. In: A. N. Longva and A. S. Roald, eds, *Religious Minorities in the Middle East: Domination, Self-Empowerment, Accommodation*. Leiden and Boston, MA: Brill, pp. 245-266.

Fisk, R., 2000. Television News is Secret Weapon of the Intifada. *The Independent*, 2 December.

Fitelson, B., 2001. 'Studies in Bayesian Confirmation Theory'. PhD thesis, University of Wisconsin – Madison. Available from: <http://exordio.qfb.umich.mx/archivos%20pdf%20de%20trabajo%20umsh/Aphilosofia/thesis%20bayesian.pdf> [Accessed 21 October 2017].

Fitsanakis, J. and Bolden, M-S, 2012. 'Social Networking as a Paradigm Shift in Tactical Intelligence Collection'. MCIS (Mediterranean Council for Intelligence Studies) Yearbook 2012. Available from: <http://www.rieas.gr/images/mcis2012.pdf> [Accessed 28 January 2018].

Flack, J., 2017. How Nature Solves Problems Through Computation. Video. *Quanta Magazine*, 10 July. Available from: <https://www.youtube.com/watch?v=EoHmzuxKong> [Accessed 12 December 2018].

- Flanigan, S. and Abdel-Samad, M., 2009. 'Hezbollah's Social Jihad: Nonprofits as Resistance Organizations'. *Middle East Policy*, 16 (2), pp. 122-137. Available from: https://www.researchgate.net/profile/Shawn-Flanigan/publication/249391972_Hezbollah%27s_Social_Jihad_Nonprofits_as_Resistance_Organizations/links/5a1c7e0a0f7e9b2a53169c7b/Hezbollahs-Social-Jihad-Nonprofits-as-Resistance-Organizations.pdf [Accessed 1 March 2021].
- Flaxman, A., Frieze, A. and Vera, J., 2007. 'A Geometric Preferential Attachment Model of Networks II'. *Internet Mathematics*, 4 (1), pp. 87-112. Available from: https://projecteuclid.org/download/pdf_1/euclid.im/1243430569 [Accessed 15 May 2019].
- Fleming, L. and Sorenson, O., 2001. 'Technology as a Complex Adaptive System: Evidence from Patent Data'. *Research Policy*, 30 (2001), pp. 1019-1039. Available from: https://s3.amazonaws.com/academia.edu.documents/7233416/technology%20as%20a%20complex%20adaptive%20system%20evidence%20from%20patent%20data.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1515770651&Signature=ooWLbpquIW1Zl9nzwlj9pMSKESE%3D&response-content-disposition=inline%3B%20filename%3DTechnology_as_a_complex_adaptive_system.pdf [Accessed 12 January 2018].
- Fordham, A., 2015. Fact Check: Did Obama Withdraw from Iraq Too Soon, Allowing ISIS to Grow? NPR (National Public Radio, 19 December). Available: <https://www.npr.org/2015/12/19/459850716/fact-check-did-obama-withdraw-from-iraq-too-soon-allowing-isis-to-grow> [Accessed 15 June 2022].
- Foucault, M., 1997. 'The Birth of Biopolitics'. In: P. Rabinow and J. Faubion, eds, *Ethics (Essential Works of Michel Foucault 1954-1984)*. New York: The New Press, pp. 73-79.
- Foucault, M., 1977. *Discipline and Punish*. New York: Vintage Books.
- Fowler, W., 1980. *An Agenda for Quantitative Research on Terrorism*. Santa Monica, CA: RAND. Available from: <https://www.rand.org/pubs/papers/P6591.html> [Accessed 13 June 2021].
- François, C., 1999. 'Systems and Cybernetics in a Historical Perspective'. *Systems Research and Behavioral Science*, 16 (1), pp. 203-219. Available from: http://www.nomads.usp.br/pesquisas/design/objetos_interativos/arquivos/restrito/francois_systemics_and_cybernetics.pdf [Accessed 25 August 2020].
- Friedman, T., 1999. *The Lexus and the Olive Tree*. London: Harper Collins.
- Fukuyama, F., 2018. Review of *LikeWar: The Weaponization of Social Media* by P. W. Singer and E. T. Brooking. Section used on the rear cover of the book.
- Fukuyama, F., 2002. *Our Posthuman Future: Consequences of the Biotechnology Revolution*. New York: Farrar, Straus and Giroux.
- Fussey, P. and Roth, S., 2020. 'Digitizing Sociology: Continuity and Change in the Internet Era'. *Sociology* (54), 4, pp. 659-674. Available from: <https://journals.sagepub.com/doi/pdf/10.1177/0038038520918562> [Accessed 29.10.2022].
- Gaddis, J. L., 2005 [1982]. *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War*. Revised and expanded edition. New York: Oxford University Press.

- Galbraith, J., 1977. *Organization Design*. Reading, MA: Addison-Wesley.
- Garamone, J., 1996. 19 Dead, 80 Hospitalized in Terror Attack in Saudi. American Forces Press Service, 27 June. Available from: https://irp.fas.org/news/1996/n06271996_9606271.html [Accessed 31 January 2022].
- Garton Ash, T., 2006. Lebanon, North Korea, Russia ... here is the world's new multi-polar disorder. *The Guardian*, US News, Opinion, 20 July. Available from: <https://www.theguardian.com/commentisfree/2006/jul/20/comment.usa> [Accessed 30 March 2018].
- Gaub, F., 2017. 'Trends in Terrorism'. Issue Alert 4, March. European Union Institute for Security Studies, Paris. Available from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_Terrorism_in_Europe_0.pdf [Accessed 3 July 2022].
- Gell-Mann, M., 2002. 'Plectics: The study of simplicity and complexity'. *Europhysics News*, January/February, pp. 17-20. Available from: <https://www.europhysicsnews.org/articles/epn/pdf/2002/01/epn02105.pdf> [Accessed 8 August 2018].
- Gell-Mann, M., 1994. 'Complex Adaptive Systems'. In: G. Cowan, D. Pines and D. Meltzer, eds, *Complexity: Metaphors, Models and Reality*. Cambridge, MA: Perseus Books, pp. 17-28. Available from: <https://authors.library.caltech.edu/60491/1/MGM%20113.pdf> [Accessed 22 April 2018].
- Gell-Mann, M., 1988. 'Simplicity and Complexity in the Description of Nature'. *Engineering & Science*, 51 (3), pp. 2-9. Available from: http://tuvalu.santafe.edu/~mgm/Site/Publications_files/MGM%2099.pdf [Accessed 3 October 2018].
- Gerges, F., 2016. *A History of ISIS*. Princeton, NJ: Princeton University Press.
- Gerges, F., 2005. *The Far Enemy: Why Jihad Went Global*. Cambridge: Cambridge University Press.
- Gerring, J., 2007. 'Is There a (Viable) Crucial-Case Method?' *Comparative Political Studies*, 40 (3), pp. 231-253. Available from: <http://people.bu.edu/jgerring/documents/CrucialCaseCPS.pdf> [Accessed 4 November 2020].
- Gerring, J., 2005. 'Causation: A Unified Framework for the Social Sciences'. *Journal of Theoretical Politics*, 17 (2), pp. 163-198. Available from: <https://blogs.kent.ac.uk/ionw/files/2015/03/Gerring-05-Causation-a-unified-framework-for-the-social-sciences.pdf> [Accessed 3 November 2020].
- Gerrits, L., 2008. *The Gentle Art of Coevolution: A Complexity Theory Perspective on Decision Making over Estuaries in Germany, Belgium and the Netherlands*. Rotterdam: Erasmus University. Available from: https://www.researchgate.net/publication/254805429_The_Gentle_Art_of_Coevolution_a_complexity_theory_perspective_on_decision_making_over_estuaries_in_Germany_Belgium_and_the_Netherlands [Accessed 27 August 2020].
- Gershenson, C., 2014. 'Requisite Variety, Autopoiesis, and Self-organization'. Cornell University Library. Available from: <https://arxiv.org/ftp/arxiv/papers/1409/1409.7475.pdf> [Accessed 3 October 2018].

Giddens, A., 2004. 'The Future of World Society: The New Terrorism'. Lecture delivered at London School of Economics, 10 November. LSE Digital Library video. Available from: <https://digital.library.lse.ac.uk/objects/lse:boh708tuk> [Accessed 11 June 2018].

Giddens, A., 1999. 'Risk and Responsibility'. *Modern Law Review*, 62 (1), pp. 1-10. Available from: https://courses.washington.edu/sales09/Handouts/Giddens_Risk_Responsibility.pdf [Accessed 1 February 2023].

Giddens, A., 1979. *Central Problems in Social Theory*. London: Macmillan.

Gilfillan, S. C., 1935. *Inventing the Ship*. Chicago, IL: Follett Publishing Company.

Gillings, M., Hilbert, M. and Kemp, D., 2016. 'Information in the Biosphere: Biological and Digital Worlds'. *Trends in Ecology and Evolution*, 31 (3), pp. 1-16. Available from: <https://escholarship.org/content/qt38f4b791/qt38f4b791.pdf> [Accessed 10 May 2021].

Gleick, J., 1987. *Chaos: The Making of a New Science*. New York: Viking.

Glennan, S., Illari, P. and Weber, E., 2021. 'Six Theses on Mechanisms and Mechanistic Science'. *Journal for General Philosophy of Science*, 53 (1), pp. 143-161.

Global Terrorism Database 2012. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Available from: <http://www.start.umd.edu/gtd/> [Accessed 1 February 2023].

Golburt, Y., 2004. 'An In-depth Look at the Jemaah Islamiyah Network'. *Al Nakhlah: The Fletcher School Online Journal for Southwest Asia and Islamic Civilization*, Article 2. Tufts University. Available from: https://ciaotest.cc.columbia.edu/olj/aln/aln_fall04/aln_fall04b.pdf [Accessed 11 April 2022].

Goldberg, D. E., 1989. *Genetic Algorithms in Search, Optimization, and Machine Learning*. Boston, MA: Addison-Wesley.

Goldberg, J., 2002. 'A Reporter at Large: In the Party of God (Part 1)'. *The New Yorker*, 14 October. Available from: https://web.archive.org/web/20080516070556/http://www.jeffreygoldberg.net/articles/tny/a_reporter_at_large_in_the_par.php [Accessed 24 October 2021].

Goldenfeld, N. and Kadanoff, L., 1999. 'Simple Lessons from Complexity'. *Science*, 284 (1), pp. 87-89. Available from: http://www.profligategrace.com/documents/Grant/Simple_Lessons_Complexity.pdf [Accessed 14 April 2019].

Goldman, A. and Nakashima, E., 2015. CIA and Mossad killed senior Hezbollah figure in car bombing. *The Washington Post*, 30 January. Available from: https://www.washingtonpost.com/world/national-security/cia-and-mossad-killed-senior-hezbollah-figure-in-car-bombing/2015/01/30/ebb88682-968a-11e4-8005-1924ede3e54a_story.html [Accessed 24 October 2021].

Goldschmidt Jr, A., 1991. *A Concise History of the Middle East*. Fourth edition. Boulder, CO: Westview Press.

Goldstein, J., 1999. 'Emergence as a Construct: History and Issues'. *Emergence*, 1 (1), pp. 49-72. Available from: https://www.researchgate.net/publication/243786253_Emergence_as_a_Construct_History_and_Issues [Accessed 26 August 2020].

Goodman, R., 2017. How Would You Explain Shannon's Information Theory in Layman's Terms? Quora, 19 July. Available from: https://www.quora.com/How-would-you-explain-Shannons-information-theory-in-laymans-terms/answer/Rob-Goodman-4?ref=forbes&rel_pos=1 [Accessed 16 June 2018].

Goolsby, R., 2006. 'Combatting Terrorist Networks: An Evolutionary Approach'. *Computational & Mathematical Organization Theory*, 12 (1), pp. 7-20. Available from: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a467322.pdf> [Accessed 4 June 2020].

Grant, C. and Valasek, T., 2007. *Preparing for the Multi-Polar World: European Foreign and Security Policy in 2020*. London: The Centre for European Reform. Available from: http://www.cer.eu/sites/default/files/publications/attachments/pdf/2011/e783_18dec07-1376.pdf [Accessed 30 March 2018].

Granovetter, M., 1973. 'The Strength of Weak Ties'. *American Journal of Sociology*, 78, pp. 1360-1380. Available from: <https://www.cs.umd.edu/~golbeck/INST633o/granovetterTies.pdf> [Accessed 12 July 2020].

Grassberger, P., 1986. 'Toward a Quantitative Theory of Self-Generated Complexity'. *International Journal of Theoretical Physics*, 25 (9), pp. 907-938.

Grassé, P-P., 1959. 'La Reconstruction de la Nid et les Co-ordinations Inter-individuelles Chez Bellicoitermes Natalenis et Cubitermes, sp. La theorie de la Stigmergie: Essai d'interpretation des Termites Constructeurs'. *Insectes Sociaux*, 6, pp. 41-81.

Greenfield, S., 2014. *Mind Change: How Digital Technologies are Leaving their Mark on our Brains*. London: Rider.

Gregorio, J., 2002. Stigmergy and the World-Wide Web. BitWorking, 30 December. Available from: <https://bitworking.org/news/2002/12/Stigmergy> [Accessed 15 May 2019].

Griffin, A., 2014. Isis militants 'using Twitter to ask for suggestions on how to kill Jordanian pilot'. *The Independent*, 30 December. Available from: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/isis-polls-twitter-for-gruesome-suggestions-of-how-to-kill-jordanian-pilot-9949550.html> [Accessed 21 July 2018].

Grobman, G., 2005. 'Complexity Theory: A New Way to Look at Organizational Change'. *Public Administration Quarterly*, 29 (3), pp. 350-382. Available from: <http://www.complexityforum.com/members/Grobman%202005%20Complexity%20theory.pdf> [Accessed 8 August 2018].

Grzymala-Busse, A., 2011. 'Time Will Tell? Temporality and the Analysis of Causal Mechanisms and Processes'. *Comparative Political Studies*, 44 (9), pp. 1267-1297. Available from: https://amgbusse.people.stanford.edu/sites/g/files/sbiybj5521/f/cps_time-2011-grzymala-busse-1267-97.pdf [Accessed 25 October 2020].

Gunaratna, R., 2002. *Inside Al-Qa'ida: Global Network of Terror*. New York: Columbia University Press.

Hacker, F., 1976. *Crusaders, Criminals, Crazyies: Terror and Terrorism in Our Time*. New York: W.W. Norton + Company.

- Hafner, M., Disley, E. and Baruch, B., 2018. 'The Cost of Terrorism in Europe'. RAND Europe, 6 June. Available from: <https://www.rand.org/randeurope/research/projects/the-cost-of-terrorism-in-europe.html> [Accessed 5 July 2022].
- Hall, P., 2013. 'Tracing the Progress of Process Tracing'. *European Political Science*, 1 (1), pp. 20-30. Available from: https://scholar.harvard.edu/files/hall/files/hall2012_eps.pdf [Accessed 2 September 2020]. Page numbers relate to online version.
- Hall, P., 2003. 'Aligning Ontology and Methodology in Comparative Politics'. In: J. Mahoney and D. Rueschemeyer, eds, *Comparative Historical Analysis in the Social Sciences*. Cambridge: Cambridge University Press, pp. 373-404. Available from: https://scholar.harvard.edu/files/hall/files/aligning_ontology_2003.pdf [Accessed 29 August 2020].
- Hall, S., 1973. 'The Determinations of News Photographs'. In: S. Cohen and J. Young, eds, *The Manufacture of News: Deviance, Social problems and the Mass Media*. London: Constable, pp. 176-190. Available from: <https://www.scribd.com/document/352003622/Hall-S-1-The-Determinations-of-News-Photographs-The-Manufacture-of-News-Social-problems-De-pdf> [Accessed 29 August 2020].
- Halverson, J., Corman, S. and Goodall, H. L., 2011. *Master Narratives of Islamist Extremism*. Berlin: Springer.
- Hamilos, P., 2015. From our Own Correspondent. 60th Anniversary Special Edition. Panel discussion presented by Owen Bennett-Jones. BBC Radio 4, 17 September.
- Hamzeh, A. Nizar, 1993. 'Lebanon's Hizbullah: From Islamic Revolution to Parliamentary Accommodation'. *Third World Quarterly*, 14 (2), pp. 321-337.
- Har Shemesh, O., 2017. 'Phase Transitions in Complex Systems: An Information Geometric Approach'. PhD thesis, University of Amsterdam, submitted 13 December. Available from: <https://pure.uva.nl/ws/files/19772829/Thesis.pdf> [Accessed 22 October 2022].
- Harb, Z., 2015. 'Al Manar and Hezbollah: Creative Instances in Propaganda Warfare'. In: A. Hamdar and L. Woods, eds, *Islamism and Cultural Expression in the Arab World*. London: Routledge, pp. 189-205. Available from: <https://openaccess.city.ac.uk/id/eprint/14595/3/Islamism%20Harb%20SUBMITTED.pdf> [Accessed 31 October 2021].
- Harel, A., 2006. Soldier killed, three missing, after Naval vessel hit off Beirut coast. Haaretz.com, 16 July. Available from: <https://web.archive.org/web/20060718032259/http://haaretz.com/hasen/spages/738695.html> [Accessed 10 September 2022].
- Harper, W. and Harris, D., 1975. 'The Application of Link Analysis to Police Intelligence'. *Human Factors*, 17 (2), pp. 157-164. Available from: <https://journals.sagepub.com/doi/pdf/10.1177/001872087501700206> [Accessed 2 January 2021].
- Harrow, M., 2011. 'Video-recorded Decapitations: A Seemingly Perfect Terrorist Tactic that did not Spread'. Danish Institute for International Studies (DIIS) Working Paper 2011:08. Available from: https://www.files.ethz.ch/isn/131372/WP%202011-08_video-recorded-decapitations_web.pdf [Accessed 12 June 2022].

Hassan, H., 2017. Insurgents Again: The Islamic State's Calculated Reversion to Attrition in the Syria-Iraq Border Region and Beyond. *CTC Sentinel*, 10 (11). Available from: <https://ctc.usma.edu/insurgents-again-the-islamic-states-calculated-reversion-to-attrition-in-the-syria-iraq-border-region-and-beyond/> [Accessed 8 November 2020].

Hauben, M., 1994. History of ARPANET: Behind the Net. 19 December. Available from: https://www.bibliotecapleyades.net/sociopolitica/sociopol_DARPA10.htm [Accessed 12 September 2022].

Hawking, S., 2000. "'Unified Theory' is getting closer", Hawking predicts. Interview with *San Jose Mercury News*, 23 January, p. 29A. Cited in Jankowski, A., 2017. *Interactive Granular Applications in Networks and Systems Engineering: A Practical Perspective*. Cham, Switzerland: Springer, p. 45.

Hayden, N., 2013. 'Innovation and Learning in Terrorist Organizations: Towards Adaptive Capacity and Resilience'. Paper presented at the 31st International Conference of the System Dynamics Society, Cambridge, Massachusetts, July 21-25, 2013. Available from: <https://proceedings.systemdynamics.org/2013/proceed/papers/P1407.pdf> [Accessed 29 November 2017]. Page numbers refer to online version.

Hayden, N., 2006. 'The Complexity of Terrorism: Social and Behavioral Understanding Trends for the Future'. In: M. Ranstorp, ed., *Mapping Terrorism Research: State of the Art, Gaps and Future Direction*. London: Routledge, pp. 33-57.

Hazran, Y., 2009. 'The Shiite Community in Lebanon: From Marginalization to Ascendancy'. *Middle East Brief*, 37 (1), pp. 1-8. Crown Centre for Middle East Studies, Brandeis University. Available from: https://www.academia.edu/7274252/The_Shiite_Community_in_Lebanon_From_Marginalization_to_Ascendancy [Accessed 1 February 2021].

Healey, J., 2014. 'The Internet: A Lawless Wild West?'. *The National Interest*, 11 July. Available from: <https://nationalinterest.org/feature/the-internet-lawless-wild-west-10638> [Accessed 19 July 2018].

Hegghammer, T., 2010. *Jihad in Saudi Arabia: Violence and Pan-Islamism Since 1979*. Cambridge: Cambridge University Press.

Helmer, D., 2006. 'Hezbollah's Employment of Suicide Bombing During the 1980s: The Theological, Political, and Operational Development of a New Tactic'. *Military Review*, July-August, pp. 71-82. Available from: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20060831_art012.pdf [Accessed 2 March 2021].

Hess, S. and Kalb, M., 2003. *The Media and the War on Terrorism*. Washington DC: Brookings Institution Press.

Heubusch, K., 2006. 'Interoperability: What it Means, Why it Matters?' *Journal of AHIMA*, 77 (1), pp. 26-30. Available from: <https://library.ahima.org/doc?oid=60942#.YX1a255BxPY> [Accessed 30 October, 2021].

Heylighen, F., 2016b. 'Stigmergy as a Universal Coordination Mechanism 1: Definition and Components'. *Cognitive Systems Research*, 38 (2016), pp. 4-13. Available from: <http://cleamc11.vub.ac.be/Papers/Stigmergy/CognSystems.pdf> [Accessed 15 May 2019].

Heylighen, F., 2002. 'The Global Brain as a New Utopia'. In: R. Maresch and F. Rötzer, eds, *Zukunftsfiguren*. Frankfurt, Germany: Suhrkamp. Available from: <http://pespmc1.vub.ac.be/Papers/GB-Utopia.pdf> [Accessed 25 April 2019].

Heylighen, F. and Lenartowicz, M., 2017. 'The Global Brain as a Model for the Future Information Society: An Introduction to the special issue'. *Technological Forecasting & Social Change*, 114 (1), pp. 1-6. Available from:

https://www.researchgate.net/publication/310799660_The_Global_Brain_as_a_model_of_the_future_information_society_An_introduction_to_the_special_issue [Accessed 21 April 2019].

Heylighen, F., Kingsbury, K., Lenartowicz, M., Harmsen, T. and Beigi, S., 2017. 'Social Systems Programming: Behavioural and Emotional Mechanisms Co-opted for Social Control'. ECCO Working Paper 2017-07. Available from:

https://pdfs.semanticscholar.org/8b4d/9bb4540ea6f5802c1ed17c1b3f6dc845e6fc.pdf?_ga=2.196121769.409404469.1554390967-368132887.1551566424 [Accessed 4 April 2019].

Hindman, M., 2018. How Cambridge Analytica's Facebook Targeting Model Really Worked – According to the Person Who Built It. *The Conversation*, 30 March. Available from:

<http://theconversation.com/how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it-94078> [Accessed 20 July 2018].

Hizballah, 1985. *The Hizballah Programme: An Open Letter*. IDC Herzliya, International Institute for Counter-Terrorism, 16 February. Available from:

<https://www.ict.org.il/UserFiles/The%20Hizballah%20Program%20-%20An%20Open%20Letter.pdf> [Accessed 3 October 2021].

Hoffman, A., 2017. 'The Islamic State's Use of Social Media: Terrorism's Siren Song in the Digital Age'. The Institute for National Security Studies (INSS), Tel Aviv University. Available from:

<https://www.inss.org.il/wp-content/uploads/2017/07/10-The-Islamic-States-Use-of-Social-Media-Terrorism%E2%80%99s-Siren-Song-in-the-Digital-Age.pdf> [Accessed 30 July 2022].

Hoffman, B. and Ware, J., 2020. The Challenges of Effective Counterterrorism Intelligence in the 2020s. *Lawfare*, 21 June. Available from: <https://www.lawfareblog.com/challenges-effective-counterterrorism-intelligence-2020s> [Accessed 10 November 2020].

Hoffman, B. and Ware, J., 2019. After Baghdadi: What Hurts the Islamic State May Help Al-Qaeda. Council on Foreign Relations, 29 October. Available from: <https://www.cfr.org/in-brief/after-baghdadi-what-hurts-islamic-state-may-help-al-qaeda> [Accessed 10 November 2020].

Hoffman, B., 2007. 'A Form of Psychological Warfare'. *eJournalUSA: Countering the Terrorist Mentality*. *Foreign Policy Agenda*, 12 (5), pp. 8-11. Available from:

http://www.au.af.mil/au/awc/awcgate/state/counter_terr_mentality_may07.pdf [Accessed 12 June 2018].

Hoffman, B., 2006a. *Inside Terrorism*. Revised and expanded edition. New York: Columbia University Press.

Hoffman, B., 2006b. 'Al-Qaida is More Dangerous than it was on 9/11'. *Spiegel* Online, 10 October. Available from: <http://www.spiegel.de/international/interview-with-terrorism-expert-bruce-hoffman-al-qaida-is-more-dangerous-than-it-was-on-9-11-a-441695.html> [Accessed 14 December 2017].

Hoffman, B., 2006c. *The Use of the Internet by Islamic Extremists*. Santa Monica, CA: RAND. Available from: <https://www.rand.org/pubs/testimonies/CT262-1.html> [Accessed 12 January 2020].

Hoffman, B., 2004. 'Redefining Counterterrorism: The Terrorist as CEO'. *RAND Review*, 28 (1), pp. 14-15. Available from:

https://www.rand.org/content/dam/rand/www/external/publications/randreview/issues/spring2004/RAND_Review_spring2004.pdf [Accessed 11 January 2022].

Hoffman, B., 2003. 'Al Qaeda, Trends in Terrorism and Future Potentialities: An Assessment'. Santa Monica, CA: RAND. Available from: <https://www.rand.org/content/dam/rand/pubs/papers/2005/P8078.pdf> [Accessed 12 December 2017].

Hoffman, B., 2002. 'Rethinking Terrorism and Counterterrorism Since 9/11'. *Studies in Conflict & Terrorism*, 25 (5), pp. 303-316. Available from: http://home.sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/29/Rethinking%20Terrorism%20and%20Counterterrorism_Hoffman.pdf [Accessed 1 January, 2018].

Hoffman, B., 1999. 'Terrorism Trends and Prospects'. In: Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D. and Zanini, M., *Countering the New Terrorism*. Santa Monica, CA: RAND, pp. 7-38.

Hoffman, B., 1994. *Responding to Terrorism Across the Technological Spectrum*. US Army War College Strategic Studies Institute, 15 July. From paper presented at Fifth Annual Strategy Conference, 26-28 April. Carlisle Barracks, PA: Strategic Studies Institute. Pages are unnumbered. I have numbered them from first page of the text.

Hogg, M., 2018. "'Causal Potency" and contributory negligence.' *Obligations Law Blog*, March 6. The University of Edinburgh Law School. Available from: <https://www.obligations.law.ed.ac.uk/2018/03/06/causal-potency-and-contributory-negligence/> [Accessed 14 June 2021].

Hogg, T. and Huberman, B. A., 1985. *Order, Complexity, and Disorder*. Palo Alto, CA: Palo Alto Research Centre (PARC), Xerox.

Holbrooke, R., 2001. Get the Message Out. *The Washington Post*. WP Opinions, 28 October. Available from: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/13/AR2010121305410.html> [Accessed 6 April 2016].

Holden, M., 2017. Islamic State militants developing own social media platform: Europol. Reuters, World News, 3 May. Available from: <https://www.reuters.com/article/us-security-islamic-state-socialmedia/islamic-state-militants-developing-own-social-media-platform-europol-idUSKBN17Z1KS> [Accessed 20 July 2018].

Holden, R., 1986. 'The Contagiousness of Aircraft Hijacking'. *American Journal of Sociology*, 91 (4), pp. 874-904.

Holland, J., 2014. *Signals and Boundaries: Building Blocks for Complex Adaptive Systems*. Cambridge, MA: The MIT Press.

Holland, J., 1995. *Hidden Order: How Adaptation Builds Complexity*. Reading, MA: Addison-Wesley.

Holland, J., 1992a. 'Complex Adaptive Systems'. *Daedalus*, 121 (1), pp. 17-30.

Holland, J., 1992b. *Adaptation in Natural and Artificial Systems*. Cambridge, MA: MIT Press.

Holland, J., 1975. *Adaptation in Natural and Scientific Systems*. Ann Arbor, MI: University of Michigan Press.

Holland, P. W., 1986. 'Statistics and Causal Inference'. *Journal of the American Statistical Association*, 81 (396), pp. 945-960. Available from: <http://people.umass.edu/~stane/pdffiles/causal-holland.pdf> [Accessed 6 September 2020].

Hook, D., 2004. 'Frantz Fanon, Steve Biko, "psychopolitics" and critical psychology'. London: LSE Research Online. Available from: <http://eprints.lse.ac.uk/961/1/PsychopoliticsMasterPDF.pdf> [Accessed 6 April 2016].

Hosen, M., Ogbeibu, S., Giridharan, B., Cham, T.-H., Lim, W. M. and Paul, J., 2021. 'Individual motivation and social media influence on student knowledge sharing and learning performance: Evidence from an emerging economy'. *Computers & Education*, 172 (1).

Howell, L., 2015. The Space Race and the Advancement of Technology. Washington State University Digital History Project. Available from: <https://history.libraries.wsu.edu/fall2015/2015/09/01/the-roles-economic-hardship-had-in-changing-the-perception-of-women-in-different-countries/> [Accessed 30 March 2018].

Howson, C. and Urbach, P., 2006. *Scientific Reasoning: The Bayesian Approach*. Third edition. La Salle, IL: Open Court Publishing Company.

Huberman, B. A. and Hogg, T., 1986. 'Complexity and Adaptation'. *Physica D: Nonlinear Phenomena*, 22 (1-3), pp. 376-384.

Humphreys, M. and Jacobs, A., 2015. 'Mixing Methods: A Bayesian Approach'. Version 3.0. Available from: <http://www.columbia.edu/~mh2245/papers1/BIQQ.pdf> [Accessed 21 October 2017].

Huntington, S., 1996. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon and Schuster.

Hurdeman, A. A., 2003. *The Worldwide History of Telecommunications*. Hoboken, NJ: Wiley-Interscience.

Igualada, C., 2021. 'International Links and the Role of Islamic State in the Barcelona and Cambrils attacks in 2017'. *Perspectives on Terrorism*, 15 (4), pp. 65-75. Available from: <https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2021/issue-4/igualada.pdf> [Accessed 5 July 2022].

Ilachinski, A., 2005. 'Self-Organized Terrorist-Counterterrorist Adaptive Co-evolutions, Part 1: A Conceptual Design'. Technical Report, February. Alexandria, VA: CNA. Available from: https://www.cna.org/CNA_files/PDF/D0010776.A3.pdf [Accessed 4 April 2019].

Ingram, H., 2017. "'That is What the Terrorists Want": Media as Amplifier or Disrupter of Violent Extremist Propaganda'. Paper prepared for Paris workshop, 15-16 June, entitled 'The Judicial response to Terrorism and the Charter of Fundamental Rights of the EU: Media Treatment of terrorism Cases'. Available from: <https://icct.nl/wp-content/uploads/2017/06/INGRAM-paris-speech.pdf> [Accessed 16 October 2019].

Iqbal, N. and Cabral, S., 2022. Mother 'begged for life' of IS hostage, court hears. BBC News, 5 April. Available from: <https://www.bbc.com/news/world-us-canada-61003674> [Accessed 17 June 2022].

Irshaid, F., 2015. Isis, Isil, IS or Daesh? One group, many names. BBC.com/news, 2 December. Available from: <https://www.bbc.com/news/world-middle-east-27994277> [Accessed 4 July 2022].

Irwin, D. and Mandel, D., 2020. 'Variants of Vague Verbiage: Intelligence Community Methods for Communicating Probability'. In: D. Mandel, ed., *Assessment and Communication of Uncertainty in Intelligence to Support Decision-Making*. Brussels: NATO Science and Technology Organization, pp. 319-348. Available from:

https://www.researchgate.net/publication/335771404_Variants_of_Vague_Verbiage_Intelligence_Community_Methods_for_Communicating_Probability [Accessed 19 August 2021].

Isaac, M. and Ember, S., 2016. For Election Day Influence, Twitter Ruled Social Media. *The New York Times*, Technology, 8 November. Available from:

<https://www.nytimes.com/2016/11/09/technology/for-election-day-chatter-twitter-ruled-social-media.html> [Accessed 20 July 2018].

Isaacson, W., 2021. *Code Breaker: Jennifer Doudna, Gene Editing, and Future of the Human Race*. London: Simon & Schuster.

Isaacson, W., 2007. *Einstein: His Life and Universe*. London: Simon & Schuster.

Isikoff, M., 2010. US Failure to Retaliate for USS Cole attack Rankled then – and now. NBCNews.com, 12 October. Available from: <https://www.nbcnews.com/id/wbna39622062> [Accessed 27 February 2022].

Jaber, H., 1997. *Hezbollah: Born with a Vengeance*. New York: Columbia University Press.

Jacinto, L., 2004. Al-Qaeda's Webmasters Wage a Cyber Jihad. ABC News online, 15 July. Available from: <https://abcnews.go.com/International/story?id=84595&page=1&singlePage=true> [Accessed 29 October 2022].

Jackson, B., 2009. 'Organizational Decision-making by Terrorist Groups'. In: P. Davis and K. Cragin, eds, *Social Science for Counterterrorism: Putting the Pieces Together*. Santa Monica, CA: RAND.

Jackson, B., 2001. 'Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption'. *Studies in Conflict and Terrorism*, 24 (3), pp. 183-213. Available from: <https://www.rand.org/pubs/reprints/RP1248.readonline.html> [Accessed 6 December 2017]. Page numbers refer to online version.

Jakobsen, P. V., 2000. 'Focus on the CNN Effect Misses the Point: The Real Media Impact on Conflict Management is Invisible and Indirect'. *Journal of Peace Research*, 37 (2), pp. 131-143. Available from: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.838.7236&rep=rep1&type=pdf> [Accessed 11 November 2021].

Jantsch, E., 1980. *The Self-Organizing Universe: Scientific and Human Implications of the Emerging Paradigm of Evolution*. Oxford: Pergamon Press. Available from:

<https://monoskop.org/images/9/9e/166495032-The-Self-Organizing-Universe-by-Erich-Jantsch.pdf> [Accessed 2 March 2019].

Jenkins, B., 2015a. Brian M. Jenkins on Countering Terrorism for Four Decades. Los Angeles World Affairs Council. Video: 00.06.13 'We spent ...' – 00.08.55 '...that have changed'. Available from: <https://www.youtube.com/watch?v=Nfttm4LR5uo> [Accessed 29 November 2017].

Jenkins, B., 2015b. Brian M. Jenkins on Countering Terrorism for Four Decades. Los Angeles World Affairs Council. Video: 00.09.30 'They have certainly ...' – 00.09.54 '... terrorism has worked'. Available from: <https://www.youtube.com/watch?v=Nfttm4LR5uo> [Accessed 6 December 2017].

Jenkins, B., 2011. 'Is Al Qaeda's Strategy Working?' Paper delivered to the Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence, United States House of Representatives, 6 December. Santa Monica, CA: RAND. Available from: https://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT371.pdf [Accessed 14 December 2017].

Jenkins, B., 2006. 'The New Age of Terrorism'. *McGraw-Hill Homeland Security Handbook*, pp. 117-130. Available from: https://www.rand.org/content/dam/rand/pubs/reprints/2006/RAND_RP1215.pdf [Accessed 9 April 2018].

Jenkins, B., 2002. *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*. Santa Monica, CA: RAND. Available from: https://www.rand.org/pubs/monograph_reports/MR1620.html [Accessed 26 April 2018].

Jenkins, B., 2001. 'The Organization Men'. In: J. Hoge and G. Rose, eds, *How Did This Happen? Terrorism and the New War*. Oxford: Public Affairs.

Jenkins, B., 1999. 'Foreword'. In: Lesser, I., Hoffman, B., Arquilla, A., Ronfeldt, D. and Zanini, M., *Countering the New Terrorism*. Santa Monica, CA: RAND/Project Air Force.

Jenkins, B., 1974. 'International Terrorism: A New Kind of Warfare'. Santa Monica, CA: RAND. Available from: <https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf> [Accessed 24 February 2018].

Jenkins, B. and Butterworth, B., 2020. 'How Sophisticated are Terrorist Attacks n Passenger Rail Transportation'. Mineta Transportation Institution, Project SP 0502, June. Available from: <https://transweb.sjsu.edu/sites/default/files/SP0520-Jenkins-Terrorist-Attacks-Passenger-Rail-Transportation.pdf> [Accessed 7 June 2022].

Jenkins, B. and Godges, J. P., 2011. 'Introduction: The Shadow of 9/11 Across America'. In: B. Jenkins and J. P. Godges, eds, *The Long Shadow of 9/11: America's Response to Terrorism*. Santa Monica, CA: RAND, pp. 1-8.

Jetter, M., 2017. 'Terrorism and the Media: The Effect of US Television Coverage on Al-Qaeda Attacks.' IZA, Institute of Labour Economics, Bonn, Germany, discussion paper, April (IZA DP No. 10708). Available from: <http://ftp.iza.org/dp10708.pdf> [Accessed 23 September 2020].

Johnson, A., 2014. 'Foucault: Critical Theory of the Police in a Neoliberal Age'. *Theoria*, 61 (141), pp. 5-29.

Jones, C., 2006. 'Al-Qaeda's Innovative Improvisers: Learning in a Diffuse Transnational Network'. *Cambridge Review of International Affairs*, 19 (4), pp. 555-569. Available from: https://gvpt.umd.edu/sites/gvpt.umd.edu/files/pubs/Jones_AQInnovativeImprovisers.pdf [Accessed 11 April 2022].

Jorisch, A., 2004a. 'Terrorist Television: Hezbollah Has a Worldwide reach'. *National Review*, 22 December.

Jorisch, A., 2004b. 'Al-Manar: Hizbullah TV, 24/7'. *Middle East Quarterly*, 11 (1), pp. 17-31. Available from: <https://www.meforum.org/583/al-manar-hizbullah-tv-24-7> [Accessed 23 February 2021].

Jorisch, A., 2004c. *Beacon of Hatred: Inside Hizballah's Al-Manar Television*. Washington DC: Washington Institute for Near East Policy. Available from: <https://www.washingtoninstitute.org/policy-analysis/beacon-hatred-inside-hizballahs-al-manar-television> [Accessed 23 February 2021].

Kaczynski, T., 1995. Industrial Society and its Future. This is the text of the 35,000-word manifesto submitted to *The Washington Post* by Kaczynski, popularly known as The Unabomber, and published on September 22, 1995. Available from: <https://www.washingtonpost.com/wp-srv/national/longterm/unabomber/manifesto.text.htm> [Accessed 6 December 2022].

Kalathil, S. and Boas, T., 2003. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington, DC: Carnegie Endowment for International Peace.

Kant, I., 1951 [1790]. *The Critique of Judgment*. Translated by J. H. Bernard. New York: Hafner Publishing Company.

Kaplan, A. and Haenlein, M., 2010. 'Users of the World Unite! The Challenges and Opportunities of Social Media'. *Business Horizons*, 53 (1), pp. 59-68. Available from: <http://michaelhaenlein.com/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf> [Accessed 19 July 2018].

Kaplan, E., 2010. Profile: Hassan Nasrallah. Council on Foreign Relations, 11 August. Available from: <https://web.archive.org/web/20160413075604/http://www.cfr.org/lebanon/profile-hassan-nasrallah/p11132> [Accessed 12 February 2021].

Karam, Z. and El Deeb, S., 2021. Gunbattles Erupt During Protest of Beirut Blast Probe; 6 Die. AP (Associated Press), 15 October. Available from: <https://apnews.com/article/hezbollah-middle-east-lebanon-beirut-explosions-56b61328f420caf4e259aeb3f428fb9a> [Accessed 24 October 2021].

Kauffman, S., 1993. *The Origins of Order: Self-organization and Selection in Evolution*. New York: Oxford University Press.

Kauffman, S., 1992. 'Coevolution in Complex Adaptive Systems'. Grant application to the National Science Foundation for exploratory research. Abstract only. Available from: <http://grantome.com/grant/NSF/DBI-9201536> [Accessed 14 January 2018].

Kauffman, S., 1991a. 'The Sciences of Complexity and "Origins of Order"'. Santa Fe Institute Working Paper: 1991-04-021. Santa Fe, NM: Santa Fe Institute. Available from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.4690&rep=rep1&type=pdf> [Accessed 14 January 2018]. Page numbers refer to online version.

Kauffman, S., 1991b. Coevolution in Complex Adaptive Systems. Outline of exploratory research grant offered by the US National Science Foundation. Available from: <https://grantome.com/grant/NSF/DBI-9201536> <https://grantome.com/grant/NSF/DBI-9201536> [Accessed 21 August 2020].

Kayaoglu, T., 2010. 'Westphalian Eurocentrism in International Relations Theory'. *International Studies Review*, 12 (1), pp. 193-217. Available from: https://d1wqtxts1xzle7.cloudfront.net/50237825/Westphalian_Eurocentrism_in_Internationa20161110-32397-t7etom.pdf?1478813113=&response-content-disposition=inline%3B+filename%3DWestphalian_Eurocentrism_in_Internationa.pdf&Expires=1598036149&Signature=flb~a9kmeV0sxalaBaK~uGgVyViK40jm5MWUlln-f7QgCj0qx08Ke9FYGICcMorsAm8DybhXmMtsBZhmLXCpZ~iyjHbX7C8uN8rVHjNMZFRk-

[~McckSRqyLpTve6qUTukMlhPhFbgjXuQ112~-9rgHUrSHOdx-G5pBFRyxCBARXMUZ6GpeU6MbSdNOMpS~ikaGfJXAmtRXeBXOoe7OOMSZTH3Bx~oi4HjqHkm9MtZRxD8hFjsYgRabumcqPI6MLu4r6N30539BM8FVa8EW-TrWuds5fwxcU8VSR31i6JM3gJt5zKAUD2kdnOJE9XkC4HNnutwvNyQkmeCAxPNfA0jA &Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA](https://pubmed.ncbi.nlm.nih.gov/2181112/) [Accessed 21 August 2020].

Kegley, C., 2003. 'The Characteristics, Causes, and Controls of the New Global Terrorism: An Introduction'. In: C. Kegley, ed., *The New Global Terrorism: Characteristics, Causes, Controls*. Upper Saddle River, NJ: Prentice Hall, pp. 1-13.

Kelly, K., 1994. *Out of Control: The Rise of Neo-Biological Civilization*. Reading, MA: Addison-Wesley.

Kelly, M., 1978. 'Louis Althusser and the Problems of a Marxist Theory of Structure'. *Proceedings of the Royal Irish Academy: Archaeology, Culture, History, Literature*, 78, pp. 199-212.

Kelly, M.G.E, 2018. 'Problematizing the Problematic: Foucault and Althusser'. *Angelaki: Journal of the Theoretical Humanities*, 23 (2), pp. 155-169.

Kenett, D.Y., Stanley, H.E. and Ben-Jacob, E., 2013. 'How High-Frequency Trading Affects a Market Index'. *Scientific Reports*, 3 (2110). Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3743071/> [Accessed 6 December 2022].

Kennedy, J. and Weimann, G., 2011. 'The Strength of Weak Terrorist Ties'. *Terrorism and Political Violence* 23 (2), pp. 201-212.

Kepel, G., 2015. *Jihad: The Trail of Political Islam*. Seventh printing. Translated by A. F. Roberts. Cambridge, MA: The Belknap Press.

Kepel, G., 2004. *The War for Muslim Minds: Islam and the West*. Cambridge, MA: Harvard University Press. Khalaf, S., 1987. *Lebanon's Predicament*. New York: Columbia University Press.

Khatib, L., 2013. *Image Politics in the Middle East: The Role of the Visual in Political Struggle*. London: I. B. Tauris.

Khatib, L., 2012. *Hizbullah's Image Management Strategy*. Los Angeles, CA: Figueroa Press. Available from: https://uscpublicdiplomacy.org/sites/uscpublicdiplomacy.org/files/legacy/publications/perspectives/CPD_Perspectives_Paper1_2012_Final.pdf [Accessed 13 November 2021].

Kifner, J., 1984. 23 Die, Including 2 Americans, in Terrorist Car Bomb Attack on the US Embassy at Beirut; Black Kills Driver. *The New York Times*, 21 September. Available from: <https://www.nytimes.com/1984/09/21/world/23-die-including-2-americans-terrorist-car-bomb-attack-us-embassy-beirut-blast.html> [Accessed 1 March 2021].

Kim, R. and Kaplan, S., 2006. 'Interpreting Socio-technical Co-evolution: Applying Complex Adaptive Systems to IS Engagement'. *Information Technology & People*, 19 (1), pp. 35-54.

Kimmagine, D., 2010. 'Al Qaeda Central and the Internet'. Counterterrorism Strategy Initiative Policy Paper, March. Washington, DC: New America Foundation. Available from: https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HSPI_Report_15.pdf [Accessed 5 December 2017].

- King, A., 2010. 'The Odd Couple: Margaret Archer, Anthony Giddens and British social theory.' *The British Journal of Sociology*, 61 (s1), pp. 253-260. Special Issue: The BJS – Shaping Sociology over 60 Years. Available from: <https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-4446.2009.01288.x> [Accessed 23 August 2021].
- King, G., Keohane, R. and Verba, S., 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press.
- Kisselburgh, L., Vorvoreanu, M. and Spafford, E., 2010. Web 2.0: A Complex Balancing Act (The First Global Study of Web 2.0 Usage, Risks and Best Practice). Available from: https://www.researchgate.net/publication/273729988_Web_2_0_A_Complex_Balancing_Act_The_First_Global_Study_on_Web_2_0_Usage_Risks_and_Best_Practices [Accessed 20 July 2018].
- Knack, 2016. Vorige regeringen noemden Sharia4Belgium clowns met lange baarden. Knack.be, 14 April. Available from: <https://www.knack.be/nieuws/vorige-regeringen-noemden-sharia4belgium-clowns-met-lange-baarden/> (Accessed 13 February 2023).
- Knorr Cetina, K., 2005. 'Complex Global Microstructures: The New Terrorist Societies'. *Theory, Culture and Society*, 22 (5), pp. 213-234. Available from: http://kops.uni-konstanz.de/bitstream/handle/123456789/11460/complex_global_microstructures.pdf?sequence=1 [Accessed 19 July 2019].
- Koerner, B., Why ISIS is Winning the Social Media War. *Wired*. Available from: <https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/> [Accessed 13 June 2022].
- Kosal, M., E., 2020. 'Emerging Life Sciences and Possible Threats to International Security'. *Orbis*, 64 (4), pp. 599-614. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7515815/> [Accessed 28 November 2022].
- Kováč, L., 2004. 'Beyond Utopias: Evolutionary Rationalism and Noocracy'. Paper prepared for the Modern Biology and Visions of Humanity conference, Genoa, 22-23 March. Available from: http://www.biocenter.sk/lkpublics_files/C-16.pdf [Accessed 7 May 2018].
- Kramer, M., 1990. 'The Moral Logic of Hizballah'. In: W. Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*. Cambridge: Cambridge University Press, pp. 131-157. Available from: <https://martinkramer.org/reader/archives/the-moral-logic-of-hizballah/> [Accessed 19 November 2020].
- Krayem, H., 2012. 'The Lebanese Civil War and the Taif Agreement'. American University of Beirut. Available from: https://trello-attachments.s3.amazonaws.com/5a5374b1fd4ad568e5cdeb19/5a5376724ae6e36841ce6c5d/e7b76fec3c67ad2e08164741cddd1d6/AUB_The_Lebanese_Civil_War_and_the-Taif_Agreement.html [Accessed 31.1.2021].
- Krebs, V., 2002. 'Uncloning Terrorist Networks'. *First Monday*, 7 (4), April. Available from: <https://firstmonday.org/ojs/index.php/fm/article/download/941/863> [Accessed 14 July 2020].
- Kriner, M., 2022. 'An Introduction to Militant Accelerationism'. Acceleration Research Consortium. Available from: <https://www.accresearch.org/shortanalysis/an-introduction-to-militant-accelerationism> [Accessed 7 November 2022].

- Kross, P., 2014. *Tales from Langley: The CIA from Truman to Obama*. Kempton, IL: Adventures Unlimited Press.
- Kukoc, M., 2009. 'Liberal Philosophy and Globalization'. *Synthesis Philosophica*, 47 (1), pp. 65-78.
- Kurth Cronin, A., 2009. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton, NJ: Princeton University Press.
- Kurtz, H., 1998. *Spin Cycle: Inside the Clinton Propaganda Machine*. London: Pan Books.
- LaBar, T., Hintze, A. and Adami, C., 2016. 'Evolvability Trade-offs in Emergent Digital Replicators'. *Artificial Life*, 22 (4), pp. 483-498.
- Lala, P. K. and Kumar, B. Kiran, 2003. 'An Architecture for Self-Healing Digital Systems'. *Journal of Electronic Testing*, 19 (1), pp. 523-535.
- Lama, A., 1996. PERU: Tale of a Kidnapping – From Stockholm to Lima Syndrome. IPS (Inter Press Service) News Agency, 10 July. Available from: <http://www.ipsnews.net/1996/07/peru-tale-of-a-kidnapping-from-stockholm-to-lima-syndrome/> [Accessed 2 January 2021].
- Landau, M., 1972. *Political Theory and Political Science: Studies in the Methodology of Political Inquiry*. New York: Macmillan.
- Landes, R., 2011. *Heaven on Earth: The Varieties of Millennial Experience*. New York: Oxford University Press.
- Langer, J. and Nicolich, M., 1981. 'Prior Knowledge and Its Relationship to Comprehension'. *Journal of Reading Behaviour*, XIII (4), pp. 373-379. Available from: <https://journals.sagepub.com/doi/pdf/10.1080/10862968109547426> [Accessed 3 November 2022].
- Langton, C., 1990. 'Computation at the Edge of Chaos: Phase Transitions and Emergent Computation'. *Physica D*, 42 (1-3), pp. 12-37. Available from: <https://pdfs.semanticscholar.org/cb4c/df7812fc8ad56d13317eaabc99b76659e95f.pdf> [Accessed 16 August 2018].
- Langton, C., 1992. 'Life at the Edge of Chaos'. In: C. Langton, C. Taylor, J. Doyne Farmer and S. Rasmussen, *Artificial life II*. Proceedings of the workshop on artificial life held at the Santa Fe Institute, New Mexico, in February, 1990. Boulder, CO: Westview Press.
- Laqueur, W., 2006a. *A History of Terrorism*. Fourth printing. Piscataway, NJ: Transaction Publishers.
- Laqueur, W., 2006b. 'Terror's New Face'. *Harvard International*, 6 May. Available from: <http://hir.harvard.edu/article/?a=307> [Accessed 16 April 2018].
- Lash, S., 2003. 'Reflexivity as Non-Linearity'. *Theory, Culture and Society*, 20 (2), pp. 49-57.
- Lasswell, H., 1968. 'The Future of the Comparative Method'. *Comparative Politics*, 1 (1), pp. 3-18.
- Laub, Z., 2021. 'Syria's Civil War: The Descent into Horror'. Council on Foreign Relations, 17 March. Available from: <https://www.cfr.org/article/syrias-civil-war> [Accessed 22 August 2022].
- Laudon, K. and Laudon, J., 2000. *Management Information Systems: Organization and Technology in the Networked Enterprise*. Sixth edition. Upper Saddle River, NJ: Prentice Hall. Available from:

https://www.amsterdamuas.com/binaries/content/assets/programmes/fbe/start-studiejaar-2021/mandatory-reading-is-and-it_laudon-and-laudon_2018.pdf?1626773999319 [Accessed 10 November 2022].

Lawson, F., 1984. 'Syria's Intervention in the Lebanese Civil War, 1976'. *International Organization*, 38 (3), pp. 451-480. Available from: <https://www.jstor.org/stable/pdf/2706467.pdf?refreqid=excelsior%3A3943f1693348794dc31fbc9b325d6629> [Accessed 20 February 2021].

Lécuyer, C. and Brock, D., 2006. 'The Materiality of Microelectronics'. *History and Technology: An International Journal*, 22 (3), pp. 301-325. Published online, 20 August. Available from: <https://www.tandfonline.com/doi/abs/10.1080/07341510600803440?src=recsys&journalCode=ghat20> [Accessed 14 May 2018].

Lee, M., 2011. Mobile Technology and the Rise of Consumerism. CBSNews.com, 27 June. Available from: <https://www.cbsnews.com/news/mobile-technology-and-the-rise-of-consumerism/> [Accessed 10 May 2022].

Lee, R. and Steele, S., 2014. 'Military Use of Satellite Communications, Remote Sensing, and Global Positioning Systems in the War on Terror'. *Journal of Air Law and Commerce*, 79 (1), pp. 70-112. Available from: <https://scholar.smu.edu/cgi/viewcontent.cgi?article=1334&context=jalc> [Accessed 16 March 2021].

Leggio, J., 2008. Mumbai Attack Coverage Demonstrates (Good and Bad) Maturation Point of Social Media. ZDNet.com, 28 November. Available from: <https://www.zdnet.com/article/mumbai-attack-coverage-demonstrates-good-and-bad-maturation-point-of-social-media/> [Accessed 15 February 2020].

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L. and Wolff, S., 1997. Brief History of the Internet. Internet Society. Available from: <https://www.internetsociety.org/internet/history-internet/brief-history-internet/> [Accessed 21 June 2020].

Lemm, V. and Vatter, M., 2014. 'Introduction'. In: V. Lemm and M. Vatter, eds, *The Government of Life: Foucault, Biopolitics and Neoliberalism*. New York: Fordham University Press, pp. 1-13.

Lenartowitz, M., Weinbaum and Braathen, 2016. 'The Individuation of Social Systems: A Cognitive Framework'. *Procedia Computer Science*, 88, pp. 15-20. Available from: <https://reader.elsevier.com/reader/sd/pii/S1877050916316568?token=E52FC8D6839D28AFA922DD8CC93231914A0360AFE4D2287825F07DB75EDB753E149677EA86A810FF69F700A872498C27> [Accessed 2 April 2019].

Leonnig, C., 2006. Iran Held Liable in Khobar Attack. *The Washington Post*, 23 December. Available from: <https://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200455.html> [Accessed 3 March 2021].

Lesser, I., Hoffman, B., Arquilla, J., Ronfeldt, D. and Zanini, M., 1999. *Countering the New Terrorism*. Santa Monica, CA: RAND.

Leuprecht, C., Walther, O., Skillicorn, D. and Ryde-Collins, H., 2015. Hezbollah's Global Tentacles: A Relational Approach to Convergence with Transnational Organised Crime'. *Terrorism and Political Violence*, 29 (5), pp. 902-921. Available from:

https://www.researchgate.net/publication/284518561_Hezbollah's_global_tentacles_A_relational_approach_to_convergence_with_transnational_organised_crime [Accessed 9 November 2021].

Levitt, M., 2021. *Hezbollah's Regional Activities in Support of Iran's Proxy Networks*. Washington, DC: The Middle East Institute, July. Available from:

<https://www.google.com/search?q=the+middle+east+institute&og=The+Middle+East+Institute&ags=chrome.0.0i51212j0i22i30l3.5031j0j15&sourceid=chrome&ie=UTF-8> [Accessed 17 October 2021].

Levitt, M., 2013. *Hezbollah: The Global Footprint of Lebanon's Party of God*. London: Hurst & Company.

Levitt, M., 2005. Hezbollah Finances: Financing the Party of God. The Washington Institute, Policy Analysis, 13 February. Available from: <https://www.washingtoninstitute.org/policy-analysis/hezbollah-finances-funding-party-god> [Accessed 2 November 2021].

Lewis, B., 1994. 'Why Turkey is the only Muslim Democracy'. *The Middle East Quarterly*, 1 (1), pp. 41-49. Also available from: <http://www.meforum.org/216/why-turkey-is-the-only-muslim-democracy> [Accessed 17 January 2021].

Lia, B., 2015. 'Understanding Jihadi Proto-States'. *Perspectives in Terrorism*, 9 (4), pp. 31-41. Available from:

<https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2015/volume-4/4-understanding-jihadi-proto-states-by-brynjar-lia.pdf> [Accessed 17 January 2021].

Lia, B., 2006. 'The Al-Qaida Strategist Abu Mus'ab al-Suri: A Profile'. Unpublished working paper presented at an OMS Seminar in Oslo, Norway, 15 March.

Liang, C. Schori, 2015. 'Cyber Jihad: Understanding and Countering Islamic State Propaganda'. GCSP (Geneva Centre for Security Policy) Policy Paper, 2015/2. Available from: <https://www.gcsp.ch/News-Knowledge/Publications/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda> [Accessed 26 April 2018].

Lichtblau, D., Haugh, B., Larsden, G. and Mayfield, T., 2006. 'Analysing Adversaries as Complex Adaptive Systems'. Institute for Defence Analyses, IDA Paper P-3868, October. Available from: https://www.researchgate.net/publication/265113147_Analyzing_Adversaries_as_Complex_Adaptive_Systems [Accessed 17 July 2018].

Lijphart, A., 1975. 'The Comparable-Cases Strategy in Comparative Research'. *Comparative Political Studies*, 8 (2), pp. 158-177.

Lijphart, A., 1971. 'Comparative Politics and the Comparative Method'. *American Political Science Review*, 65 (3), pp. 682-693.

Lippmann, W., 1997 [1922]. *Public Opinion*. New York: Free Press Paperbacks.

Livesey, B., 2005. The Salafist Movement' *Frontline*, Public Broadcasting Service, 25 January. Available from: <http://www.pbs.org/wgbh/pages/frontline/shows/front/special/sala.html> [Accessed 6 April 2016].

Lowles, N. and Mulhall, J., 2013. *Gateway to Terror, Anjem Choudary and the Al-Muhajiroun Network*. London: Hope Not Hate Educational Limited. Available from:

<https://hopenothate.org.uk/wp-content/uploads/2018/10/gateway-to-terror-2013-11.pdf> [Accessed 23 June 2022].

Loyd, A., 2022. What Happened to John Cantlie? My Hunt for the Forgotten Isis Hostage. *The Sunday Times*, 24 June. Available from: <https://www.thetimes.co.uk/article/what-happened-to-john-cantlie-my-hunt-for-the-forgotten-isis-hostage-v8wt08sfg> [Accessed 26 June 2022].

Lucia, U., 2009. 'Irreversibility, Entropy and Incomplete Information'. *Physica A: Statistical Mechanics and its Applications*, 388 (19), pp. 4025-4033.

Luhmann, N., 2002. *Das Erziehungssystem der Gesellschaft*. Frankfurt am Main, Germany: Suhrkamp Tachenbuch Verlag.

Luhmann, N., 1995. *Social Systems*. Stanford, CA: Stanford University Press.

Luhmann, N., 1990. *Essays on Self-Reference*. New York: Columbia University Press.

Luhmann, N., 1987. *Social Systems: Outline of a General Theory*. Frankfurt am Main, Germany: Suhrkamp Tachenbuch Verlag. Available from: http://ebooks.bharathuniv.ac.in/gdlc1/gdlc4/Arts_and_Science_Books/arts/sociology/Niklas%20Luhmann/Books/Soziale%20Systeme.pdf [Accessed 13 August 2018].

Luhmann, N., 1986. 'The Autopoiesis of Social Systems'. In: F. Geyer and J. van der Zouwen, eds, *Sociocybernetic Paradoxes*. London: Sage, pp. 172-192

Luhmann, N., 1982a. *The Differentiation of Society*. Trans., S. Holmes and C. Larmore. New York: Columbia University Press.

Luhmann, N., 1982b. 'The World Society as a Social System'. *International Journal of General Systems*, 8 (3), pp. 131-138.

Lynch, M., 2006a. 'Al-Qaeda's Media Strategies.' *The National Interest*, 83 (1), pp. 50-56. Available from: <http://www.marclynch.com/wp-content/uploads/2012/03/out.pdf> [Accessed 10 November 2020].

Lynch, M., 2006b. 'Al-Qaeda's Constructivist Turn'. *Praeger Security International*, 5 May. Available from: <http://www.marclynch.com/wp-content/uploads/2011/03/Al-Qaedas-Constructivism.pdf> [Accessed 14 March 2022].

Macdonald, F., 2015. Science says that technology is Speeding up our Brains' Perception of Time. *ScienceAlert.com*, 19 November. Available from: <https://www.sciencealert.com/research-suggests-that-technology-is-speeding-up-our-perception-of-time> [Accessed 26 June 2022].

Macey, D., 1993. *The Lives of Michel Foucault*. New York: Pantheon Books.

Machamer, P., 2004. 'Activities and Causation: The Metaphysics and Epistemology of Mechanisms.' *International Studies in the Philosophy of Science*, 18 (1), pp. 27-39. Available from <https://blogs.kent.ac.uk/jonw/files/2015/03/Machamer-04-Activities-and-Causation.pdf> [Accessed 3 November 2020].

Machamer, P., Darden, L. and Craver, 2000. 'Thinking About Mechanisms', *Philosophy of Science*, 67 (1), pp. 1-25. Available from:

https://www.researchgate.net/publication/240548010_Thinking_About_Mechanisms [Accessed 3 November 2020].

Madhani, A., 2010. Cleric Al-Awlaki dubbed 'bin Laden of the Internet'. *USA Today* online, 24 August. Available from: https://usatoday30.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm [Accessed 16 February 2020].

Maher, S., 2016. *Salafi-Jihadism: The History of an Idea*. London: Hurst & Company.

Maher, S., 2015. Jordanian pilot murder: Islamic State deploys asymmetry of fear. BBC News, 4 February. Available from: <http://www.bbc.com/news/world-middle-east-31129416> [Accessed 21 July 2018].

Maher, S., 2014. Video. Inside Story. Islamic State 'beheading': A Challenge to US? Al Jazeera English, 20 August. Available from: https://www.google.com/search?q=shiraz+maher+2014+video+youtube&oq=shiraz+maher+2014+video+youtube&aqs=chrome..69i57j0i546l2j0i30i546.9676j0j15&sourceid=chrome&ie=UTF-8#fpstate=ive&vld=cid:03cc8876,vid:BKKeAV_Rczs [Accessed 28 January 2023].

Mahoney, J., 2015. 'Process Tracing and Historical Explanation'. *Security Studies*, 24 (2), pp. 200-218.

Maini, A. and Agrawal, V., 2011. *Satellite Technology: Principles and Applications*. Chichester, West Sussex, UK: John Wiley & Sons Limited.

Mair, D., 2016. '#Westgate, A Case Study: How Al-Shabaab used Twitter During an Ongoing Attack.' *Studies in Conflict & Terrorism*, 40 (1), pp. 24-43.

Malthaner, S., 'Space, Ties, and Agency: The Formation of Radical Networks'. *Perspectives on Terrorism*, 12 (2), pp. 32-43. Available from: <https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2018/2018-02/03-spaces-ties-and-agency-the-formation-of-radical-networks-by-stefan-malthaner.pdf> [Accessed 10 January 2022].

Manchester Arena Inquiry, 2022. An Independent Public Inquiry to Investigate the deaths of the victims of the 2017 Manchester Arena Terror Attack. Available from: <https://manchesterarenainquiry.org.uk> [Accessed 28 January 2023].

Mandel, D. and Irwin, D., 2021. 'Uncertainty, Intelligence and National Security Decisionmaking.' *International Journal of Intelligence and Counterintelligence*, 34 (3), pp. 558-582.

Mank, R., 2017. *Quantum Diplomacy for a New Technological Age*. Calgary, Canada: Canadian Global Affairs Institute. Available from: https://d3n8a8pro7vnm.cloudfront.net/cdfai/pages/3098/attachments/original/1512614857/Quantum_Diplomacy_for_a_New_Technological_Age.pdf?1512614857 [Accessed 2 June 2018].

Marighella, C., 1969. *Mini-manual of the Urban Guerilla*. Montreal: Abraham Guillen Press. Also available from: http://dimitris.apeiro.gr/files/papers/politics/Marighella_Minimanual_of_the_urban_guerrilla.pdf (Accessed 3 July 2018). Page numbers relate to this online version.

Marinescu, D. and Marinescu, G., 2012. *Classical and Quantum Information*. Amsterdam: Elsevier.

- Marion, R. and Uhl-Bien, M., 2003. 'Complexity Theory and Al Qaeda: Examining Complex Leadership'. Lincoln, NE: University of Nebraska, Management department Faculty Publications. Available from: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1008&context=managementfacpub> [Accessed 20 April 2019].
- Markovich, S., 2014. 'Space Exploration and US Competitiveness'. Council on Foreign Relations, 5 December. Available from: <https://www.cfr.org/backgrounder/space-exploration-and-us-competitiveness> [Accessed 24 November 2017].
- Marsden, S. and Schmid, A., 2011. 'Typologies of Terrorism and Political Violence'. In: A. Schmid, ed., *The Routledge Handbook of Terrorism Research*. London and New York: Routledge.
- Martinez-Torres, M. E., 2001. 'Civil Society, the Internet, and the Zapatistas'. *Peace Review*, 13 (3), pp. 347-355.
- Masoud, M. W., 2013. 'An Analysis of Abu Mus'ab al-Suri's 'Call to Global Islamic Resistance''. *Journal of Strategic Security*, 6 (1), pp. 1-18. Available from: <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1230&context=jss> [Accessed 1 June 2022].
- Masters, S., 2015. John Cantlie: British journalist appears in new ISIS propaganda video [online]. *The Independent*, 7 April. Available from: <http://www.independent.co.uk/news/world/middle-east/john-cantlie-british-journalist-appears-in-isis-propaganda-video-calling-on-muslims-to-carry-out-10035116.html> [Accessed 21 July 2018].
- Matar, D., 2008. 'The Power of Conviction: Nasrallah's Rhetoric and Mediated Charisma in the Context of the 2006 July War'. *Middle East Journal of Culture and Communication*, 1 (2), pp. 122-137.
- Maturana, H. and Varela, F., 1972. *Autopoiesis and Cognition: The Realization of the Living*. Dordrecht, The Netherlands: D. Reidel Publishing.
- Matusitz, J., 2018. 'Brand Management in Terrorism: The Case of Hezbollah.' *Journal of Policing, Intelligence and Counter Terrorism*, 13 (1), pp. 1-16. Available from: <https://www.tandfonline.com/doi/abs/10.1080/18335330.2017.1412489> [Accessed 2 November 2021].
- Maurer, S., 2009. 'Technologies of Evil: Chemical, Biological, Radiological, and Nuclear Weapons'. In: S. Maurer, ed., *WMD Terrorism: Science and Policy Choices*. Cambridge, MA: The MIT Press, pp. 1-10.
- Mazzucato, M., 2015. *The Entrepreneurial State: Debunking Public Vs Private Sector Myths*. London: Anthem Press.
- McCormick, T., 2014. 'Al Qaeda Core: A Short History'. *Foreign Policy*, 17 March. Available from: <http://foreignpolicy.com/2014/03/17/al-qaeda-core-a-short-history/#> [Accessed 9 December 2017].
- McDuffie, J., 2017. 'Why the Military Released GPS to the Public'. *Popular Mechanics*, 19 June. Available from: <https://www.popularmechanics.com/technology/gadgets/a26980/why-the-military-released-gps-to-the-public/> [Accessed 7 October 2021].
- McElroy, M., 2000. 'Integrating Complexity Theory'. *Journal of Knowledge Management*, 4 (3), pp. 195-203. Available from:

https://www.researchgate.net/publication/237279219_Integrating_Complexity_Theory_Knowledge_Management_and_Organizational_Learning [Accessed 8 August 2018].

McKelvey, B., 2002. 'Managing Coevolutionary Dynamics'. Paper presented at the 18th EGOS Conference, Barcelona, Spain, 4 – 6 July. Available from: https://www.researchgate.net/publication/228559005_Managing_Coevolutionary_Dynamics [Accessed 13 May 2020].

McKelvey, B., n/d. Changing Business Environment calls for Complexity Leadership. UCLA Anderson School of Management. Available from: <https://www.anderson.ucla.edu/knowledge-assets/bill-mckelvey> [Accessed 20 September 2020].

McKelvey, B., 1999. 'Avoiding Complexity Catastrophe in Coevolutionary Pockets: Strategies for Rugged Landscapes'. *Organization Science*, 10, 1999, pp. 294-321. Available from: https://pdfs.semanticscholar.org/30f6/a527096038fc128f2dc5520019a215a60ffd.pdf?_ga=2.257677323.1413011044.1524476827-1908841928.1524476827 [Accessed 23 April 2018].

McLuhan, M., 1979. Marshall McLuhan Full Lecture: The Medium is the Message. Video. Recorded sat ABC Radio, Australia, 27 June. Available from: <https://www.youtube.com/watch?v=ImaH51F4HBw> [Accessed 27 June 2020].

McLuhan, M., 1967. *Understanding Media: The Extensions of Man*. London: Sphere Books.

McLuhan, M. and Fiore, Q., 1968. *War and Peace in the Global Village*. New York: Bantam Books.

McLuhan, M. and Fiore, Q., 1967. *The Medium is the Message*. New York: Bantam Books.

McLuhan, M. and Powers, B., 1992. *The Global Village: Transformations in World Life and Media in the 21st Century*. Oxford: Oxford University Press.

McShea, D. W., 1996. 'Metazoan Complexity and Evolution: Is there a Trend?' *Evolution: International Journal of Organic Evolution*, 50 (2), pp. 477-492. Available from: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1558-5646.1996.tb03861.x> [Accessed 8 March 2019]

Meleagrou-Hitchens, A., 2011. 'As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad'. The International Centre for the study of Radicalisation and Political Violence. Available from: <http://icsr.info/wp-content/uploads/2012/10/1315827595ICSRPaperAsAmericanAsApplePieHowAnwaralAwlakiBecametheFaceofWesternJihad.pdf> [Accessed 21 July 2016].

Melman, Y., 2002. Virtual Soldiers in a Holy War. *Haaretz*, 13 September. Available from: <https://www.haaretz.com/print-edition/features/virtual-soldiers-in-a-holy-war-1.34332> [Accessed 16 December 2017].

Meltzer, J. P., 2014. 'The Internet, Cross-Border Data Flows and International Trade'. *Asia & The Pacific Policy Studies*, 2 (1), pp. 90-102. Available from: <https://onlinelibrary.wiley.com/doi/full/10.1002/app5.60> [Accessed 20 September 2022].

Meneely, P., Dawes Hoang, R., Okeke, I. and Heston, K., 2017. *Genetics: Genes, Genomes and Evolution*. Oxford: Oxford University Press.

- Mercier, A., 2015. How Social Media Shaped Our Understanding of the Paris Attacks. *The Conversation*, 16 November. Available from: <https://theconversation.com/how-social-media-shaped-our-understanding-of-the-paris-attacks-50814> [Accessed 4 July 2022].
- Mesic, R., Hura, M., Libicki, M., Packard, A. and Scott, L., 2010. *Air Force Cyber Command (Provisional) Support*. Santa Monica, CA: RAND. Available from: https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG935.1.pdf [Accessed 6 June 2020].
- Mesjasz, C., 2015. 'Complex Systems Studies and Terrorism'. In: P. Fellman, Y. Bar-Yam and A. Minai, eds, *Conflict and Complexity: Countering Terrorism, Insurgency, Ethnic and Regional Violence*. New York: Springer/NECSI, pp. 35-72.
- Mesjasz, C., 2008. 'How Complex Systems Studies Could Help in Identification of Threats of Terrorism'. In: A. Minai and Y. Bar-Yam, eds, *Unifying Themes in Complex Systems IV*. New York: Springer, pp. 379-389.
- Metz, C., 2012. Paul Baran, the link between nuclear war and the internet. *Wired*, 4 September. Available from: <https://www.wired.co.uk/article/h-bomb-and-the-internet> [Accessed 12 September 2022].
- Meyer, A. D., Tsui, A. S. and Hinings, C. R., 1993. 'Configurational Approaches to Organisational Analysis', *Academy of Management Journal*, 36 (6), pp. 1175-1195. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2720502 [Accessed 26 October 2020].
- Meyer, C., 1991. *Underground Voices: Insurgent Propaganda in El Salvador, Nicaragua and Peru*. Santa Monica, CA: RAND. Available from: <https://www.rand.org/pubs/notes/N3299.html> [Accessed 12 January 2020].
- Midgley, S. and Rice, V., 1984. *Terrorism and the Media in the 1980s*. Washington, DC: Media Institute.
- Migaux, P., 2007. 'Al Qaeda'. In: G. Chaliand and A. Blin, eds, *The History of Terrorism: From Antiquity to Al Qaeda*. Berkeley, CA: University of California Press, pp. 314-348.
- Miles, M. and Huberman, M., 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. Second edition. Thousand Oaks, CA: Sage.
- Milman, O., 2022. Buffalo Suspect May be Latest Mass Shooter Motivated by 'eco-fascism'. *The Guardian*, 17 May, 2022. Available from: <https://www.theguardian.com/us-news/2022/may/17/buffalo-shooting-suspect-eco-fascism> [Accessed 6 December 2022].
- Milligan, T., 2005. *Modern Antenna Design*. Second edition. Hoboken, NJ: John Wiley & Sons.
- Misangyi, V., Greckhamer, T., Furnari, S., Fiss, P., Crilly, D. and Aguilera, R., 2017. 'Embracing Causal Complexity: The Emergence of a Neo-Configurational Perspective'. *Journal of Management*, 43 (1), pp. 255-282. Available from: https://lbsresearch.london.edu/id/eprint/708/1/Crilly_D_MisangyiY_et_al_JOM_Embracing_Causal_Complexity_2016.pdf [Accessed 26 October 2020].
- Mishal, S. and Rosenthal, M., 2005. 'Al Qaeda as a Dune Organisation: Towards a Typology of Islamic Terrorist Organisations'. *Studies in Conflict & Terrorism*, 28 (4), pp. 275-293. Available from: <https://www.files.ethz.ch/isn/46602/mc20.pdf> [Accessed 2 June 2022].

- Mitchell, M., 2009. *Complexity: A Guided Tour*. Oxford: Oxford University Press. Available from: https://www.academia.edu/40227220/Complexity_A_Guided_Tour_Melanie_Mitchell_2009 [Accessed 9 June 2020].
- Mitchell, M., 2006. 'Complex Systems: Network Thinking'. Santa Fe Institute. SFI Working Paper 2006-10-036. Available from: <https://pdfs.semanticscholar.org/7e3f/dd64740a2a51df32ea0adf5fee42196be1ea.pdf> [Accessed 22 April 2018].
- Mitchell, M., 1995. 'Genetic Algorithms: An Overview'. *Complexity*, 1 (1), pp. 31-39. Available from: <http://liacs.leidenuniv.nl/~csnaco/EA/ps/ga-tutorial.pdf> [Accessed 26 April 2020].
- Mitleton-Kelly, E., 2013. Co-evolution of Intelligent Socio-technical Systems: Modelling and Applications in Large-scale Emergency and Transport Domains. E. Mitleton-Kelly, ed. Heidelberg: Springer.
- Mitleton-Kelly, E., 2011. 'A Complexity Theory Approach to Sustainability: A Longitudinal Study in Two London NHS Hospitals'. *The Learning Organization*, 18 (1), pp. 45-53.
- Mitleton-Kelly, E., 2000. 'Complexity: Partial Support for BPR'. In: P. Henderson, ed., *Systems Engineering for Business Process Change*. London: Springer-Verlag, pp. 24-37. Available from: <https://pdfs.semanticscholar.org/06e1/7b0dcf925578b36784087c9c9acbc8d65d13.pdf> [Accessed 8 August 2018].
- Mitleton-Kelly, E. and Davy, L., 2013. 'The concept of "co-evolution" and its application in the social sciences: A review of the literature'. In: E. Mitleton-Kelly, ed., *Co-Evolution of Intelligent Socio-Technical Systems: Modelling and Applications in Large-scale Emergency and Transport Domains*. Berlin: Springer, pp. 43-57.
- Mobley, B. P., 2001. 'The Ingenuity of Common Workmen: And the Invention of the Computer'. Iowa State University Digital Repository. Available from: <https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1659&context=rtd> [Accessed 14 May 2018].
- Moffat, J., 2003. *Complexity Theory and Network Centric Warfare*. Washington DC: CCRP (Command and Control Research Programme) Publication Series. Available from: https://books.google.nl/books?hl=en&lr=&id=axosGWa29x0C&oi=fnd&pg=PR1&dq=Moffat+J+complexity&ots=uaYoAhZl9a&sig=8PyunB8LLe4hU8_Bh0wcuDpSFic#v=onepage&q=Moffat%20J%20complexity&f=false [Accessed 30 September 2020].
- Moghadam, A., 2013. 'Top-Down and Bottom-Up Innovation in Terrorism: The Case of the 9/11 Attacks'. International Institute for Counter-Terrorism, Inter-disciplinary Centre (IDC), Herzliya, Israel. Working Paper 18, July. Available from: <https://www.ict.org.il/UserFiles/ICTWPS%20-%20Assaf%20Moghadam%20-%202018.pdf> [Accessed 1 February 2023].
- Mokyr, J., 1992. *The Level of Riches: Technological Creativity and Economic Progress*. Oxford: Oxford University Press.
- Momen, M., 1985. *An Introduction to Shi'i Islam: The History and Doctrines of Twelver Shi'ism*. New Haven, CT: Yale University Press.
- Morgan, J., 2015. The 5 Types of Organizational Structures: Part 4, Flatarchies. Forbes.com, 15 July. Available from: <https://www.forbes.com/sites/jacobmorgan/2015/07/15/the-5-types-of-organizational-structures-part-4-flatarchies/#63a3c4646707> [Accessed 30 November 2017].

Morgan, M., 2009. *The Impact of 9/11 on Politics and War: The Day That Changed Everything*. London: Palgrave Macmillan.

Morgan, M., 2004. 'The Origins of the New Terrorism'. *Parameters*, 34 (1), pp. 29-43. Available from: <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2190&context=parameters> [Accessed 8 September 2020].

Morgan, N., Jones, G. and Hodges, A., 2012. 'Social Media: The Complete Guide to Social Media from the Social Media Guys'. Available from: <https://rucreativebloggingfa13.files.wordpress.com/2013/09/completeguidetosocialmedia.pdf> [Accessed 29 June 2021].

Mosendz, P., 2014. 'Beheadings as Terror Marketing'. *The Atlantic*, 2 October. Available from: <https://www.theatlantic.com/international/archive/2014/10/beheadings-as-terror-marketing/381049/> [Accessed 16 June 2022].

Mount, M., 2007. Khalid Sheikh Mohammed: I Beheaded American Reporter. CNN.com, 15 March. Available from: <http://edition.cnn.com/2007/US/03/15/guantanamo.mohammed/index.html> [Accessed 21 August 2021].

Mousavizadeh, N., 2015. The Weaponization of Everything: Globalization's dark side. Reuters blog, 25 September. Available from: <http://blogs.reuters.com/great-debate/2015/09/24/the-weaponization-of-everything-globalizations-dark-side/> [Accessed 28 January 2018].

Moye, W., 1996. ENIAC: The Army-sponsored Revolution. US Army Research Laboratory. Available from: <https://web.archive.org/web/20170521072638/http://ftp.arl.mil/~mike/comphist/96summary/index.html> [Accessed 4 February 2020].

Mueller, J. and Stewart, M., 2016. 'Misoverestimating ISIS: Comparisons with Al-Qaeda'. *Perspectives on Terrorism*, 10 (4), pp. 30-39. Available from: <https://www.jstor.org/stable/pdf/26297616.pdf> [Accessed 16 June 2022].

Murphy, H., 2020. Facebook: The Inside Story – The Many Faces of Mark Zuckerberg. *FT Weekend*, 26 February, Life + Arts p. 9. Available from: <https://www.thuisbezorgd.nl/en/foodtracker?trackingid=4288968876819> [Accessed 29 March 2020].

Mylroie, L., 1995-'96. 'The World Trade Center Bomb. Who is Ramzi Yousef? And Why it Matters?' *The National Interest*, 42 (1), Winter '95-'96, pp. 3-15.

Nacos, B., 2007. *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism*. Second edition. Lanham, MD: Rowman & Littlefield Publishers, Inc.

Nacos, B., 2006. 'Terrorism/Counterterrorism and Media in the Age of Global Communication'. United Nations University Global Seminar, Second Shimame-Yamaguchi Session, 'Terrorism – a Global Challenge', 5-8 August. Available from: http://archive.unu.edu/gs/files/2006/shimane/Nacos_text_en.pdf [Accessed 24 February 2018].

Nacos, B., 1994. *Terrorism and the Media: From the Iran Hostage Crisis to the World Trade Centre Bombing*. Second edition. New York: Columbia University Press.

Nacos, B., Bloch-Elkon, Y. and Shapiro, R., 2011. *Selling Fear: Counterterrorism, the Media, and Public Opinion*. Chicago, IL: The University of Chicago Press.

Nagy, B., Doyne Farmer, J., Trancik, J. and Gonzales, J. P., 2011. 'Superexponential Long-term Trends in Information Technology'. *Technological Forecasting and Social Change*, 78 (8), pp. 1356-1364.

Available from:

<https://dspace.mit.edu/bitstream/handle/1721.1/105411/p.pdf?sequence=1&isAllowed=y>

[Accessed 10 May 2021].

Nan, N., 2011. 'Capturing Bottom-Up Information Technology Use Processes: A Complex Adaptive Systems Model'. *MIS Quarterly*, 35 (2), pp. 505-532.

NASA, 2020. The International Space Station: 20 years of Communications Excellence. nasa.gov, 6 November. Available from: <https://www.nasa.gov/feature/goddard/2020/the-international-space-station-20-years-of-communications-excellence> [Accessed 10 May 2022].

NPR, 2019. The end of the 'Caliphate' doesn't mean the end of ISIS. National Public Radio, 22 March. Available from: <https://www.npr.org/2019/03/22/701266887/analysis-the-end-of-the-caliphate-doesn-t-mean-the-end-of-isis?t=1659298552819> [Accessed 31 July 2022].

Naughton, J., 2016. 'The Evolution of the Internet: From Military Experiment to General Purpose Technology'. *Journal of Cyber Policy*, 1 (1), pp. 5-28. Available from:

<https://www.tandfonline.com/doi/pdf/10.1080/23738871.2016.1157619?needAccess=true>

[Accessed 24 December 2019].

Negroponte, N., 1996. *Being Digital*. London: Coronet Books.

Nesser, P., 2019. 'Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs: How the Islamic State Terror Wave Rose so High in Europe'. *CTC Sentinel*, 12 (3), pp. 15-21. Available from:

<https://ctc.westpoint.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf> [Accessed 21 June 2022].

Nesser, P., 2004. *Jihad in Europe: A Survey of the Motivations for Sunni Islamist Terrorism in post-millennium Europe*. Kjeller, Norway: Norwegian Defence Research Establishment. Available from:

<http://18.195.19.6/bitstream/handle/20.500.12242/1718/04-01146.pdf?sequence=1&isAllowed=y>

[Accessed 28 June 2021].

Neumann, P., 2015. 'Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s'. The International Centre for the Study of Radicalisation and Political Violence, King's College London, 26 January. Available from: <http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/> [Accessed 21 July 2018].

Newhouse, E., 2021. 'The Threat is the Network: The Multi-Node Structure of Neo-Fascist Accelerationism'. *CTC Sentinel*, 14 (5), pp. 17-25. Available from: <https://ctc.usma.edu/wp-content/uploads/2021/05/CTC-SENTINEL-052021.pdf> [Accessed 17 January 2023].

Newton, R., 2019. 'A Practitioner's View of the Evolution of Change Management.' *NUST Business Review*, 1 (1), pp. 50-61. Available from: <https://nbr.nust.edu.pk/wp-content/uploads/2019/12/NBR-19-0109-Final-Proof-RN-MNA.pdf> [Accessed 20 October 2022].

Nilsson, J. and Wallenstein, S.O., 2013. *Foucault, Biopolitics and Governmentality*. Södertörn Philosophical Studies 14. Flemingsberg, Sweden: Södertörn University. Available from:

<https://www.diva-portal.org/smash/get/diva2:615362/FULLTEXT03.pdf> [Accessed 28 January 2018].

Noguchi, Y., 2006. Tracking Terrorists Online. Live Q&A interview with former FBI counterterrorism expert, Evan Kohlmann. Washingtonpost.com, 19 April. Available from: <https://www.washingtonpost.com/wp-dyn/content/discussion/2006/04/11/DI2006041100626.html> [Accessed 9 September 2020].

Norris, P., Kern, M. and Just, M., 2003. *Framing Terrorism: The News Media, the Government and the Public*. New York: Routledge.

Norton, A. R., 1987. *Amal and the Shi'a: The Struggle for the Soul of Lebanon*. Austin, TX: University of Texas Press.

Norton, A. R., 2018. *Hezbollah: A Short History*. Updated and expanded third edition. Princeton, NJ: Princeton University Press.

Nuismer, S., 2017. *Introduction to Co-evolutionary Theory*. First edition. New York: Macmillan.

Nye, J., 2003. 'US Power and Strategy After Iraq'. *Foreign Affairs*, July/August, online. Available from: <https://www.foreignaffairs.com/articles/united-states/2003-07-01/us-power-and-strategy-after-iraq> [Accessed 25 November 2017]. Also available from:

<http://www.nyu.edu/steinhardt/e/pdf/humsocsci/mias/readings07/94.pdf> [Accessed 9 April 2018]. Page numbers relate to the latter.

Nyre, G. and Rose, C., 1997. 'CSE, MO and AA: Three Evaluation Strategies'. *POD Quarterly*, 1 (4), pp. 245-249.

Obolensky, N., 2014. *Complex Adaptive Leadership: Embracing Paradox and Uncertainty*. Farnham, Surrey, UK: Gower Publishing Limited.

O'Donnell, L., 2015. Afghanistan says Taliban Leader Mullah Omar Died Two years Ago. AP (Associated Press), 30 July. Available from: <https://apnews.com/article/8aea0d55437f4bac9f0356cf0510a69b> [Accessed 24 May 2022].

Oestreicher, C., 2007. 'A History of Chaos Theory'. *Dialogues in Clinical Neuroscience*, 9 (3), pp. 279-289. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3202497/> [Accessed 19 October 2022].

O'Hara, V., 2005. Troop Protections from Homemade Bombs Sought. National Public Radio, 4 March. Available from: <https://www.npr.org/2005/03/04/4522369/troop-protections-from-homemade-bombs-sought> [Accessed 1 June 2022].

Opall-Rome, B., 2006. 'Inability to Jam Hezbollah Satellite TV Signal Spurs Israeli Research'. *Space News*, 29 August. Available from: <https://spacenews.com/inability-jam-hezbollah-satellite-tv-signal-spurs-israeli-research/> [Accessed 5 March 2021].

Oppenheimer, A. R., 2009. *IRA, The Bombs and The Bullets: A History of Deadly Ingenuity*. Newbridge, County Kildare, Ireland: Irish Academic Press.

Orbital Today, 2020. Satellites: Evolution of Technology. 4 February. Available from: <https://orbitaltoday.com/2020/02/04/satellites-evolution-of-technology/> [Accessed 1 February 2023].

O'Rourke, S., 2010. 'The Emergent Challenges for Policing Terrorism: Lessons from Mumbai'. Paper presented at the First Australian Counterterrorism Conference, Perth, Western Australia, 30

November. Available from:

https://pdfs.semanticscholar.org/a190/d2b1c3989e9c1b162a787df2993acdaea010.pdf?_ga=2.105422342.469964423.1599676106-697649069.1598700249 [Accessed 9 September 2020].

Pagels, H., 1989. *The Dreams of Reason: The Computer and the Rise of the Sciences of Complexity*. New York: Bantam.

Paletz, D. and Boiney, J., 1992. 'Researchers' Perspectives'. In: D. Paletz and A. Schmid, eds, *Terrorism and the Media: How Researchers, Terrorists, Government, Press, Public, Victims, View and Use the Media*, pp. 6-28. Newbury Park, CA: Sage.

Pape, R., Rowley, M. and Morell, S., 2014. Why ISIL Beheads its Victims: The Islamic State's Brutality has a Strategic Logic. *Politico.com*, 7 October. Available from: <https://www.politico.com/magazine/story/2014/10/why-isil-beheads-its-victims-111684/> [Accessed 12 June 2022].

Paperin, G., Green, D. and Sadedin, S., 2011. 'Dual-phase evolution in complex adaptive systems'. *Journal of the Royal Society, Interface*, 8 (58), pp. 609-629. Available from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3061102/pdf/rsif20100719.pdf> [Accessed 7 August 2018].

Parekh, D., Amarasingam, A., Dawson, L. and Ruths, D., 2018. 'Studying Jihadists on Social Media: A Critique of Data Collection Methodologies'. *Perspectives of Terrorism*, 12 (3), pp. 3-21. Available from: <https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2018/issue-3/01---studying-jihadists-on-social-media-a-critique-of-data-collection-methodologies.pdf> [Accessed 27 June 2021].

Passig, D. and Hasgal, A., 2006. 'Terror Cells as Complex Adaptive Systems'. Begin-Sadat Centre for Strategic Studies, Bar-Ilan University, Israel. Available from: <http://www.vanola.co.il/alons-areas-of-knowledge/mrkw-mstglwt-wrgwny-trwr/terror-cells-as-complex-adaptive-systems> [Accessed 6 July 2018].

Pattee, H. H., 1979. 'The Complementarity Principle and the Origin of Macromolecular Information'. *BioSystems*, 11 (2-3), pp. 217-226.

Pattee, H. H., 1977. 'Dynamic and Linguistic Modes of Complex Systems'. *International Journal of General Systems*, 3 (4), pp. 259-266.

Patton, M. Q., 1999. 'Enhancing the Quality and Credibility of Qualitative Analysis'. *Health Services Research*, 34 (5), pp. 1189-1208. Available from: <http://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC1089059&blobtype=pdf> [Accessed 29.6.2021].

Pearl, J., 2010. 'An Introduction to Causal Inference'. *The International Journal of Biostatistics*, 6 (2), Article 7, pp. 1-59. Available from: https://ftp.cs.ucla.edu/pub/stat_ser/r354-corrected-reprint.pdf [Accessed 11 November 2020].

Pearl, J., 1988. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Revised second printing. San Francisco, CA: Morgan Kaufmann Publishers, Inc.

Perez, C., 1983. 'Structural Change and Assimilation of New Technologies in the Economic and Social Systems'. *Futures*, 15 (5), pp. 357-375. Available from:

http://dev1.carlotaperez.org/downloads/pubs/scass_v04.pdf [Accessed 15 January 2018]. Page numbers refer to online version.

Pfister, D. S., 2011. 'Networked Expertise in the Era of Many-to-Many Communication: On Wikipedia and Invention'. *Social Epistemology*, 25 (3), pp. 217-231. Available from: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1009&context=commstudiespapers> [Accessed 9 February 2020].

Pfister, D. S., 2011. 'Networked Expertise in the Era of Many-to-Many Communication: On Wikipedia and Invention'. *Social Epistemology*, 25 (3), pp. 217-231. Available from: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1009&context=commstudiespapers> [Accessed 9 February 2020].

Phillips, C., 2018. *The Battle for Syria: International Rivalry in the New Middle East*. Revised and updated edition. New Haven, CT: Yale University Press.

Phister, P., 2011. 'Cyberspace: The Ultimate Complex Adaptive System'. *The International C2 Journal*, 4 (2), pp. 1-30. Available from: http://dodccrp.org/files/IC2J_v4n2_03_Phister.pdf [Accessed 16 May 2019].

Picard, R., 1986. 'News Coverage as the Contagion of Terrorism: Dangerous Charges Backed by Dubious Science'. Presented at the 69th annual meeting of the Association for Education in Journalism and Mass Communication, University of Oklahoma, August 3-6. Available from: <https://files.eric.ed.gov/fulltext/ED271786.pdf> [Accessed 25 February 2018].

Pierson, P., 2000. 'Increasing Returns, Path Dependence and the Study of Politics'. *American Political Science Review*, 94 (2), pp. 251-267. Available from: <http://www.louischauvel.org/piersonpathdep2586011.pdf> [Accessed 29 August 2020].

Plsek, P., 1997. 'Some Emerging Principles for Leaders in Complex Adaptive Systems'. Atlanta, GA: Paul E. Plsek & Associates. Available from: <http://www.directedcreativity.com/pages/ComplexityWP.html> [Accessed 9 April 2019].

Price, B. and Al-'Ubaydi, M., 2017. *The Islamic State's Internal Rifts and Social Media Ban*. Combatting Terrorism Centre, US Military Academy, West Point, 21 June. Available from: <https://ctc.usma.edu/ctc-perspectives-the-islamic-states-internal-rifts-and-social-media-ban/> [Accessed 20 July 2018].

Prigogine, I. and Stengers, I., 1984. *Order out of Chaos: Man's New Dialogue with Nature*. New York: Bantam Books.

Purkiss, J. and Serle, J., 2017. 'Obama's Covert Drone War in Numbers: Ten Times More Strikes than Bush.' *The Bureau of Investigative Journalism*, 17 January. Available from: <https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush> [Accessed 7 October 2021].

Qassem, N., 2005. *Hizbullah: The Story from Within*. London: Saqi.

Rabah, M., 2020. *Conflict on Mount Lebanon: The Druze, the Maronites and Collective Memory*. Edinburgh, UK: Edinburgh University Press.

Rabasa, A., Blackwill, R., Chalk, P., Cragin, K., Fair, C., Jackson, B., Jenkins, B., Jones, S., Shestak, N. and Tellis, A., 2009. *The Lessons of Mumbai*. Santa Monica, CA: RAND. Available from:

https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf
[Accessed 15 February 2020].

Ranstorp, M., 2007. 'The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation'. In: J. Eriksson and G. Giacomello, eds, *International Relations and Security in the Digital Age*. London: Routledge, pp. 38-71.

Ranstorp, M., 2004. 'Al-Qaida in Cyberspace: Future Challenges of Terrorism in an Information Age'. In: L. Nicander and M. Ranstorp, eds, *Terrorism in the Information Age: New Frontiers?* Stockholm: Swedish National Defence College, pp. 83-96.

Ranstorp, M., 1998. 'Interpreting the Broader Context and Meaning of Bin-Laden's "Fatwa"'. *Studies in Conflict and Terrorism*, 21 (4), pp. 321-330. Available from: <https://www.tandfonline.com/doi/pdf/10.1080/10576109808436072?needAccess=true> [Accessed cscs30 January 2022].

Ranstorp, M., 1997. *Hizb'allah in Lebanon: The Politics of the Western Hostage Crisis*. Basingstoke, UK: Palgrave Macmillan.

Ranstorp, M. and Normark, M., 2015. 'Introduction: Understanding Terrorism Innovation and Learning – Al-Qaeda and Beyond'. In: M. Ranstorp and M. Normark, eds, *Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond*. London: Routledge, pp. 1-15.

Rawlinson, K., 2014. Jewish Museum Shooting Suspect 'is Islamic State torturer'. *The Guardian*, 6 September. Available from: <https://www.theguardian.com/world/2014/sep/06/jewish-museum-shooting-suspect-islamic-state-torturer-brussels-syria> [Accessed 3 July 2022].

Reeve, S., 2000. *One Day in September: The Story of the 1972 Munich Olympics Massacre*. London: Faber and Faber.

Regalado, A., 2016. Top US Intelligence Official Calls Gene Editing a WMD Threat. *MIT Technology Review*, 9 February. Available from: <https://www.technologyreview.com/2016/02/09/71575/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/> [Accessed 25 November 2022].

Reid, F. and Hurley, N., 2011. 'Diffusion in Networks with Overlapping Community Structure'. Proceedings of IEEE 11th International Conference on Data Mining Workshops, pp. 969-978. Available from: <https://arxiv.org/pdf/1105.5849.pdf> [Accessed 18 March 2019]. Page numbers relate to online version.

Reinares, F., 2012. Discussion Point: Terrorist Studies is not a Sub-Discipline. START (Studies of Terrorism and Responses to Terrorism), October 31. Available from: <https://www.start.umd.edu/news/discussion-point-terrorism-studies-not-sub-discipline> [Accessed 17 January 2023].

Reuters, 2017. Uzbekistan Says Told West That Stockholm Attack Suspect was IS Recruit. 14 April. Available from: <https://www.reuters.com/article/us-sweden-attack-uzbekistan-idUSKBN17G0J1> [Accessed 23 June 2022].

Reuters, 2007. FACTBOX: The Madrid Train Bombings and What Happened Next. Reuters.com, 15 February. Available from: <https://www.reuters.com/article/uk-spain-trial-march11-factbox-idUKL1428993920070214> [Accessed 2 June 2022].

Reynolds, D., 2001. *One World Divisible: A Global History Since 1945*. London: Penguin.

Rida, N., 2021. US Reopens File of Hezbollah's American Hostage Taking in Beirut. *Asharq Al-Awsat*, 5 December. Available from: <https://english.aawsat.com/home/article/3342081/us-reopens-file-hezbollahs-american-hostage-taking-beirut> [Accessed 9 January 2022].

Riedel, B., 2011. Al-Qaeda's Tentacles. *Los Angeles Times* op-ed, 14 January. Available from: <http://articles.latimes.com/2011/jan/14/opinion/la-oe-0114-riedel-al-qaeda-20110114> [Accessed 28 November 2017].

Robbins, T. and Palmer, S., 1997. *Millennium, Messiahs, and Mayhem: Contemporary Apocalyptic Movements*. London: Psychology Press.

Robinson, K., 2020. 'What is Hezbollah?' Council on Foreign Relations, backgrounder, 1 September. Available from: <https://www.cfr.org/backgrounder/what-hezbollah> [Accessed 20 February 2021].

Roca, D., Nemirovsky, D., Nemirovsky M., Milito, R. and Valero, M., 2016. 'Emergent Behaviors in Internet of Things: The Ultimate Ultra-Large-Scale System'. *IEEE Micro*, IOT Special Issue. Available from: <https://core.ac.uk/download/pdf/81580604.pdf> [Accessed 26 September 2020].

Rogers, P., 2009. 'Global Security After the War on Terror'. Oxford Research Group briefing paper, November. Available from: https://www.files.ethz.ch/isn/110112/09-11_Global_Security.pdf [Accessed 23 May 2022].

Rohlfing, I., 2014. 'Comparative Hypothesis Testing Via Process Tracing'. *Sociological Methods & Research*, 43 (4), pp. 606-642.

Ronfeldt, D., 2003. 'Foreword: Netwar Observations'. In: R. J. Bunker, ed., *Non-State Threats and Future Wars*. London: Frank Cass.

Ronfeldt, D., Arquilla, J., Fuller, G. and Fuller, M., 1998. *The Zapatista Social Netwar in Mexico*. Santa Monica, CA: RAND. Available from: https://www.rand.org/content/dam/rand/pubs/monograph_reports/1998/MR994.pdf [Accessed 27 August 2017].

Rosińska-Bukowska, M., 2013. 'Adjustment of Corporate Organizational Structure to the Demands of Competition in a Fast-Changing Global Economy'. *International Business and Global Economy 2013*, 32, pp. 175-186. Available from: <http://www.instytutgm.uni.lodz.pl/about-the-institute/the-department-of-international-business-and-trade-staff/dr-hab-magdalena-rosinska-bukowska-associate-professor/> [Accessed 8 August 2018].

Ross, J. I., 2007. 'Deconstructing the Terrorism-News Media Relationship'. *Crime, Media, Culture: An International Journal*, 3 (2), pp. 215-225. Available from: https://s3.amazonaws.com/academia.edu.documents/2023874/Ross-terrorism_and_media.pdf?response-content-disposition=inline%3B%20filename%3DDeconstructing_the_News_Media-Terrorism.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191201%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191201T152712Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=aaa9684d86cdcb07c70b48438889000e4e9532f8c964653bb2d950de55d5165f [Accessed 1 December 2019].

Ross, J. I., 2004. 'Taking Stock of Research Methods and Analysis on Oppositional Political Terrorism'. *The American Sociologist*, 35 (2), pp. 26-37.

Roth, S., 2011. 'Les deux angleterres et le continent: Anglophone sociology as the guardian of old European semantics'. *Journal of Sociocybernetics*, 9 (1), pp. 19-34. Available from: https://www.researchgate.net/publication/256063615_Les_Deux_Angleterres_Et_Le_Continent_Anglophone_Sociology_as_the_Guardian_of_Old_European_Semantics [Accessed 24 February 2019].

Rothrock, J., 1997. 'Information Warfare: Time for Some Constructive Skepticism'. In: J. Arquilla and D. Ronfeldt, eds, *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, pp. 217-229. Available from: https://www.rand.org/pubs/monograph_reports/MR880.html [Accessed 11 October 2021].

Rousseau, D., 1979. 'Assessment of Technology in Organisations: Closed Versus Open Systems Approaches'. *Academy of Management Review*, 4 (4), pp. 531-542. Available from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.978.9066&rep=rep1&type=pdf> [Accessed 24 November 2019].

Roy, O., 2004. *Globalized Islam: The Search for a New Ummah*. New York: Columbia University Press.

Royal Commission Report, 2020. Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019. Executive Summary. Available from: <https://christchurchattack.royalcommission.nz/the-report/executive-summary-2/executive-summary/> [Accessed 6 December 2022].

Rupert, M., Rattrout, A. and Hassas, S., 2008. 'The Web from a Complex Adaptive Systems Perspective'. *Journal of Computer and System Sciences*, 74 (2), pp. 133-145. Available from: https://ac.els-cdn.com/S0022000007000451/1-s2.0-S0022000007000451-main.pdf?_tid=70343a36-f7b9-11e7-93bb-0000aacb361&acdnat=1515776336_de7d53f83524bb0e9c452840b178e5c4 [Accessed 12 January 2018].

Russell, P., 1995. *The Global Brain Awakens: Our Next Evolutionary Leap*. Palo Alto, CA: Global Brain Inc.

Russo, F. and Williamson, J., 2007. 'Interpreting Causality in the Health Sciences'. *International Studies in the Philosophy of Science*, 21 (2), pp. 157-170. Available from: https://blogs.kent.ac.uk/ionw/files/2015/03/interpreting_causality2007.pdf [Accessed 22 October 2020].

Ruthven, M., 2015. 'Inside the Islamic State'. *The New York Review of Books*, 9 July. Available from: <http://www.nybooks.com/articles/2015/07/09/inside-islamic-state/> [Accessed 17 January 2021].

Saad-Ghorayeb, A., 2006. 'Hizbollah's Outlook in the Current Conflict. Part 1: Motives, Strategy, and Objectives'. Carnegie Endowment for International Peace, August. Middle east Programme. Police Outlook. Available from: https://carnegieendowment.org/files/saad_ghorayeb_final.pdf [Accessed 31 October, 2021].

Sageman, M., 2005. 'Understanding Jihadi Networks'. *Strategic Insights*, 4 (4), (April 2005). Available from: https://www.iwp.edu/wp-content/uploads/2019/05/20140819_SagemanUnderstandingJihadiNetworks.pdf [Accessed 31 March 2022].

Sageman, M., 2004. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press.

- Sahay, C. D. and Garge, R., 2017. Mosul Recaptured: Is this the end of Daesh? Vivekananda International Foundation, 9 August. Available from: <https://www.vifindia.org/article/2017/august/09/mosul-recaptured-is-this-the-end-of-daesh> [Accessed 4 July 2022].
- Sanders, T. I., 2002. To Fight Terror, We Can't Think Straight. *The Washington Post*, 5 May, p. B2. Available from: https://www.washingtonpost.com/archive/opinions/2002/05/05/to-fight-terror-we-cant-think-straight/c25c95a8-cdac-46c7-9ff4-c7f817d55579/?noredirect=on&utm_term=.483c585290d7 [Accessed 4 April 2019].
- Santa Fe Institute, 2018. The Meaning of Information. Santa Fe Institute, Santa Fe, New Mexico. Available from: [https://www.santafe.edu+++++events/meaning-information](https://www.santafe.edu+++++/events/meaning-information) [Accessed 15 May 2019].
- Saunders, R. and Souva, M., 2020. 'Air Superiority and Battlefield Victory'. *R&P (Research and Politics)*, October-December 2020, pp. 1-8. Available from: <https://journals.sagepub.com/doi/pdf/10.1177/2053168020972816> [Accessed 17 August 2022].
- Scheller, B., 2017. *The Wisdom of Syria's Waiting Game: Foreign Policy Under the Assads*. London: Hurst.
- Schelling, T., 1966. *Arms and Influence*. The Henry L. Stimson Lectures, Yale University. New Haven, CT: Yale University Press.
- Schiff, Z., 2002. Don't Underestimate Assad Jr. *Haaretz*, 2 August. Available from: <https://www.haaretz.com/1.5050535> [Accessed 2 November 2021].
- Schmid, A., 2017. 'Moderate Muslims and Islamist Terror: Between Denial and Resistance'. ICCT Research Paper, August. International Centre for Counter-Terrorism, The Hague. Available from: <https://icct.nl/wp-content/uploads/2017/08/ICCT-Schmid-Moderate-Muslims-and-Islamist-Terrorism-Aug-2017-1.pdf> [Accessed 29 February 2020].
- Schmid, A. and De Graaf, J., 1982. *Violence as Communication: Insurgent Terrorism and the Western News Media*. Beverly Hills, CA: Sage.
- Schoenenberger, L., Schenker-Wiki, A. and Beck, M., 2014. 'Analysing Terrorism from a Systems Thinking Perspective'. *Perspectives on Terrorism*, 8 (1), pp. 16-36. Available from: https://www.researchgate.net/publication/262826171_Analysing_Terrorism_from_a_Systems_Thinking_Perspective (Accessed 14 April 2019).
- Schumpeter, J., 1939. *Business Cycles*. New York: McGraw-Hill.
- Scriven, M., 1991. *Evaluation Thesaurus*. Fourth edition. Newbury Park, CA: Sage.
- Scriven, M., 1974. 'Evaluation Perspectives and Procedures'. In: J. Popham, ed., *Evaluation in Education: Current Application*. Berkeley, CA: McCutcheon, pp. 3-93.
- Segaller, S., 1987. *Invisible Armies: Terrorism into the 1990s*. London: Sphere Books.
- Servan-Schreiber, D., Cleeremans, A. and McClelland, J., 1989. 'Learning Sequential structure in Simple Recurrent Networks.' In: D. S. Touretsky, ed., *Advances in Neural Information Processing Systems 1*. San Mateo, CA: Morgan Kaufmann Publishers, pp. 643-652. Available from:

<https://papers.nips.cc/paper/1988/file/9dcb88e0137649590b755372b040afad-Paper.pdf> [Accessed 23 May 2021].

Seth, A., 2021a. Interviewed by Tom Sutcliffe on Start the Week, BBC Radio 4, 13 September. Available from: <https://www.bbc.co.uk/programmes/m000zkn1> [Accessed 26 September 2021].

Seth A., 2021b. *Being You: A New Science of Consciousness*. London: Penguin Random House.

Shadnia, D., Newhouse, A., Kriner, M. and Bradley, A., 2022. 'Militant Accelerationism Coalitions: A Case Study in Neo-Fascist Accelerationist Coalition Building Online'. Tech Against Terrorism, Middlebury Institute of International Studies at Monterey. Available from: <https://ctc.usma.edu/wp-content/uploads/2021/05/CTC-SENTINEL-052021.pdf> [Accessed 17 January 2023].

Shaikh, S. and Williams, I., 2018. 'Hezbollah's Missiles and Rockets'. Centre for Strategic & International Studies. CSIS Briefs, 5 July. Available from: <https://www.csis.org/analysis/hezbollahs-missiles-and-rockets> [Accessed 6 March 2021].

Shane, S. and Hubbard, B., 2014. ISIS Displaying a Deft Command of Varied Media. *The New York Times*, 30 August. Available from: <http://www.nytimes.com/2014/08/31/world/middleeast/isis-displaying-a-deft-command-of-varied-media.html> [Accessed 21 July 2018].

Shannon, C., 1948. 'A Mathematical Theory of Communications'. *The Bell System Technical Journal*, 27 (July and October), pp. 379-423 and pp. 623-656. Available from:

<http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf> [Accessed 16 June 2018] Shapir, Y., 2017. 'Hezbollah as an Army'. Institute for National Security Studies Strategic Assessment, 19 (4), pp. 67-77. Available from: <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/INSSstrategic%20assessment%2019-4%20full%20text.pdf> [Accessed 9 November 2021].

Shapira, S., 1988. 'The Origins of Hizballah'. *Jerusalem Quarterly*, 46 (1), pp. 115-130.

Sharma, P., 2008. Characteristics of Web 2.0 Technology. TechPluto.com, 28 November. Available from: <https://www.techpluto.com/web-20-services/> [Accessed 20 July 2018].

Sharrock, D., 2001. Real IRA scores propaganda coup with BBC bomb. *The Telegraph*, 5 March. Available from: <http://www.telegraph.co.uk/news/uknews/1325075/Real-IRA-scores-propaganda-coup-with-BBC-bomb.html> [Accessed 7 April 2016].

Shephard, M., 2009. The Powerful Online Voice of Jihad. *The Star*, 18 October. Available from: https://www.thestar.com/news/world/2009/10/18/the_powerful_online_voice_of_jihad.html [Accessed 16 February 2020].

Shpiro, S., 2002. 'Conflict Media Strategies and the Politics of Counter-terrorism'. *Politics*, 22 (2), pp. 76-85.

Shukla, M., 2019. The Democratization of Technology. Forbes.com, 7 November. Available from: <https://www.forbes.com/sites/forbestechcouncil/2019/11/07/the-democratization-of-technology/#966437d37967> [Accessed 22 May 2021].

Siggelkow, N., 2002. 'Evolution Toward Fit'. *Administrative Science Quarterly*, 47 (1), pp. 125-159. Available from: <https://journals.sagepub.com/doi/pdf/10.2307/3094893> [Accessed 5 January 2021].

- Simon, H. A., 1962. 'The Architecture of Complexity'. *Proceedings of the American Philosophical Society*, 106 (6), pp. 467-482. Available from: <http://www2.econ.iastate.edu/tesfatsi/ArchitectureOfComplexity.HSimon1962.pdf> [Accessed 15 August 2018].
- Simon, S. and Benjamin, D., 2001. 'The Terror'. *Survival*, 43 (4), pp. 5-18.
- Singer, P. and Brooking, E., 2018. *Like War: The Weaponization of Social Media*. New York: Houghton, Mifflin, Harcourt Publishing Company.
- Sinofsky, S., 2014. The Four States of Disruption. Recode.net, 6 January. Available from: <https://www.recode.net/2014/1/6/11622000/the-four-stages-of-disruption-2> [Accessed 7 December 2017].
- Smelser, N., 2007. *The Faces of Terrorism: Social and Psychological Dimensions*. Princeton, NJ and Oxford, UK: Princeton University Press.
- Smelser, N., 1976. *Comparative Methods in the Social Sciences*. Englewood Cliffe, NJ: Prentice Hall.
- Smith, H., 2009. Al-Awlaki May be Al Qaeda Recruiter. CBS News online, 30 December. Available from: <https://www.cbsnews.com/news/al-awlaki-may-be-al-qaeda-recruiter/> [Accessed 16 February 2020].
- Soifer, H. D., 2010. 'The Causal Logic of Critical Junctures'. *Comparative Political Studies*, 45 (12), pp. 1572-1597. Available from: http://www.critical-juncture.net/uploads/2/1/9/9/21997192/soifer_the_causal_logic_of_critical_junctures.pdf [Accessed 27 October 2020].
- Solé, R., 2011. *Phase Transitions*. Princeton, NJ: Princeton University Press.
- Solomon, E., Chazan, G. and Jones, S., 2015. Isis Inc: How Oil Fuels and Jihadi Terrorists. FT Investigations. The Financial Times, 14 October. Available from: <https://www.ft.com/content/b8234932-719b-11e5-ad6d-f4ed76f0900a#axzz3rhwAkkfP> [Accessed 14 June 2022].
- Solvit, S., 2012. *Dimensions of War: Understanding War as a Complex Adaptive System*. Paris: L'Harmattan.
- Soni, J. and Goodman, R., 2018. *A Mind at Play: How Claude Shannon Invented the Information Age*. New York: Simon & Schuster.
- Sorel, J-M., 2003. 'Some Questions about the Definition of Terrorism and the Fight Against its Financing.' *European Journal of International Law (EJIL)*, 14 (2), pp. 365-378. Available from: <http://www.ejil.org/pdfs/14/2/420.pdf> [Accessed 19 August 2021].
- Spencer, A., 2006. 'Questioning the Concept of New Terrorism'. *Peace, Conflict and Development*, 8, January, pp. 1-33. Available from: <https://core.ac.uk/download/pdf/12174153.pdf?repositoryId=454> [Accessed 8 September 2017].
- Stern, J. and Berger, J. M., 2015. *ISIS: The State of Terror*. London: William Collins.
- Stichweh, R., 2000. 'Systems Theory as an Alternative to Action Theory? The Rise of "Communication" as a Theoretical Option'. *Acta Sociologica*, 43 (1), pp. 5-13. Available from:

https://www.fiw.uni-bonn.de/demokratieforschung/personen/stichweh/pdfs/11_stw_systems-theory-as-an-alternative-to-action-theory-2000.pdf [Accessed 3 February 2019].

Strogatz, S., 1994. *Nonlinear Dynamics and Chaos*. Reading, MA: Perseus Books. Available from: <http://www.fulviofrisone.com/attachments/article/464/Strogatz,%20S.H.%20-%20Nonlinear%20dynamics%20and%20chaos.pdf> [Accessed 12 October 2020].

Sudkamp, T. and Cotterman, A., 1988. *Languages and Machines: An Introduction to the theory of Computer Science*. Volume 2. Reading, MA: Addison-Wesley

Swindells, M., Rae, M., Pearce, M., Moodie, S., Miller, R. and Leach, P., 2002. 'Application of High-throughput Computing in Bioinformatics.' *Philosophical Transactions of the Royal Society: Mathematical, Physical and Engineering Sciences*, 360 (1795), pp. 1179-1189. Available from: <https://www.jstor.org/stable/3066432?seq=1> [Accessed 28 December 2019].

Tamturk, V., 2017. How Each Generation Responds to Marketing Communications. CMSConnected, 7 July. Available from: <http://www.cms-connected.com/News-Archive/July-2017/How-Each-Generation-Responds-To-Marketing-Channels-and-Messaging> [Accessed 13 July 2018].

Tannenwald, N., 2015. 'Process Tracing and Security Studies'. *Security Studies*, 24 (2), pp. 219-227. Available from: https://www.researchgate.net/publication/279312041_Process_Tracing_and_Security_Studies [Accessed 17 October 2020].

Tarsiero, R., 2006. 'Community-based Information Technology Interventions for Persons with Mental Illness'. In: H. Rahman, ed., *Empowering Marginal Communities with Information Networking*. Hershey, PA: Idea Group Publishing.

Taylor, F., 1911. *The Principles of Scientific Management*. New York: W. W. Norton.

Teilhard de Chardin, P., 1959. *The Phenomenon of Man*. London: Collins.

Tenet, G., 2002. Unclassified version of CIA Director, George Tenet's testimony before the Joint Inquiry into Terrorist Attacks Against the United States. Washington DC, 18 July. Available from: https://irp.fas.org/congress/2002_hr/061802tenet.pdf [Accessed 17 April 2022].

Terranova, T., 2007. 'Futurepublic: On Information Warfare, Bio-racism and Hegemony as Noopolitics.' *Theory, Culture and Society*, 24 (3), pp. 125-145. Available from: <https://ur.booksc.eu/book/36852739/e2e027> [Accessed 9 October 2021].

Thatcher, M., 1985. Speech to the American Bar Association in London, 15 July. The Margaret Thatcher Foundation. Available from: <https://www.margaretthatcher.org/document/106096> [Accessed 9 April 2018]. See sub-heading, 'Terrorism'.

The Centre for Public Integrity, 2011. New Details on Kidnapping and Murder of reporter Daniel Pearl'. 19 January. Available from: <https://publicintegrity.org/inside-publici/new-details-on-kidnapping-and-murder-of-reporter-daniel-pearl/> [Accessed 4 April 2022].

The New Humanitarian, 2006. The Many Hands and Faces of Hezbollah. 29 March. Available from: <https://www.thenewhumanitarian.org/report/26242/lebanon-many-hands-and-faces-hezbollah> [accessed 2 November 2021].

The 9/11 Commission Report, 2004. *Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W. W. Norton & Company. Available from: <https://www.9-11commission.gov/report/911Report.pdf> [Accessed 24 May 2021].

The 9/11 Commission Report Executive Summary, 2004. Available from: https://govinfo.library.unt.edu/911/report/911Report_Exec.pdf [Accessed 7 April 2022].

Theraulaz, G. and Bonabeau, E., 1999. 'A Brief History of Stigmergy'. *Artificial Life*, 5 (2), pp. 97-116.

Thomas, C., 2021. 'Al Qaeda: Background, Current Status, and U.S. Policy'. Congressional Research Service, 14 June. Available from: <https://crsreports.congress.gov/product/pdf/IF/IF11854> [Accessed 16 January 2022].

Thomas, G., 2006. William Buckley: The Spy Who Never Came in from the Cold. Canada Free Press, 9 November. Available from: <https://web.archive.org/web/20061109092551/https://www.canadafreepress.com/2006/thomas102506.htm> [Accessed 9 January 2022].

Thomas, T., 2003. 'Al Qaeda and the Internet: The Danger of 'Cyberplanning''. *Parameters*, Spring 2003, pp. 112-123. Available from: <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2139&context=parameters> [Accessed 4 April 2022].

Toffler, A. and Toffler, H., 1997. 'Foreword: The New Intangibles'. In: J. Arquilla and D. Ronfeldt, eds, *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, pp. xiii-xxiv. Available from: https://www.rand.org/pubs/monograph_reports/MR880.html [Accessed 11 October 2021].

Torok, R., 2010. 'Make a Bomb in Your Mum's Kitchen': Cyber Recruiting and Socialisation of 'White Moors' and Home-grown Jihadists. Proceedings of the 1st Australian Counter-terrorism Conference, Edith Cowan University, Perth, Western Australia, 30 November. Available from: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1005&context=act> [Accessed 15 February].

Tran, M. and Weaver, M. A., 2014. Isis announces Islamic caliphate in area straddling Iraq and Syria [online]. *The Guardian*, 30 June. Available from: <http://www.theguardian.com/world/2014/jun/30/isis-announces-islamic-caliphate-iraq-syria> [Accessed 1 February 2023].

Tremlett, G., Jones, S. and Burgen, S., 2017. Spain Terror Cell Planned Barcelona Bombing Rampage. *The Guardian*, 19 August. Available from: <https://www.theguardian.com/world/2017/aug/18/accidental-blast-thwarts-huge-bomb-attack-by-spain-terror-cell> [Accessed 5 July 2022].

Trochim, W., 1985. 'Pattern Matching, Validity, and Conceptualization in Program Evaluation'. *Evaluation Review*, 9 (5), pp. 575-604. Available from: <http://www.billtrochim.net/research/Pattern%20Matching,Validity,%20and%20Conceptualization.PDF> [Accessed 6 November 2020].

Tschirgi, R. and Irani, G., 1982. 'The United States, Syria, and the Lebanese Crisis'. UCLA Centre for International and Strategic Affairs. Research note 8. Cited in Lawson 1984.

Tsvetovat, M. and Carley, K., 2005. 'Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence'. *Journal of Social Structure*, 6 (2). Available from: <http://www.cmu.edu/joss/content/articles/volume6/TsvetovatCarley/> [Accessed 19 December 2017].

Tucker, D., 2001. 'What's New About the New Terrorism and How Dangerous Is It?' *Terrorism and Political Violence*, 13 (Autumn), pp. 1-14. Available from: https://calhoun.nps.edu/bitstream/handle/10945/44722/Tucker_The_New_Terrorism_2001.pdf?sequence=1 [Accessed 11 June 2018].

Tucker, P., 2016. How Will Terrorists Use the Internet of Things? The Justice Department is Trying to Figure that Out. *Defense One*, 8 September. Available from: <https://www.defenseone.com/technology/2016/09/how-will-terrorists-use-internet-things-justice-department-trying-figure-out/131381/> [Accessed 15 July 2018].

Tucker, S., 2015. *US Conflicts in the Twenty-first Century: Afghanistan War, Iraq War, and the War on Terror*. Three volumes. Santa Barbara, CA: ABC-CLIO.

Turing, A., 1948. 'Intelligent Machinery'. National Physical Laboratory, Mathematics Division. Available from: http://www.alanturing.net/Turing_archive/archive/I/I32/L32-001.html [Accessed 15 October 2020].

Tushman, M. and Anderson, P., 1986. 'Technological Discontinuities and Organizational Environments'. *Administrative Science Quarterly*, 31 (3), pp. 439-465.

UNODC (United Nations Office on Drugs and Crime), 2012. *The Use of the Internet for Terrorism Purposes*. UNODC in collaboration with UN Counter-Terrorism Implementation Task Force. Vienna: UN Publishing. Available from: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [Accessed 1 February 2023].

US Department of the Treasury, 2006. 'U.S. Designates Al-Manar as a Specially Designated Global Terrorist Entity'. Press Centre, 23 March. Available from: <https://www.treasury.gov/press-center/press-releases/Pages/js4134.aspx> [Accessed 24 October 2021].

US Quadrennial Defense Review, 2010. United States Department of Defense, Washington DC, February 1. Available from: <http://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf> [Accessed 23 February 2019].

Vallée, R., 1993. 'Systems Theory: A Historical Presentation'. In: R. Rodriguez Delgado and R. Banathy, eds, *International Systems Science Handbook*. Madrid: Systemic Publications.

Van Evera, S., 1997. *Guide to Methods for Students of Political Science*. Ithaca, NY: Cornell University Press.

Vernadsky, V. I., 1926. *The Biosphere*. New York: Copernicus.

Waldrop, M., 2001. 'Claude Shannon: Reluctant Father of the Digital Age'. *MIT Technology Review*, 104 (6), pp. 64-71.

Wallace, P., 2017. 'Why we are still Living in the Sputnik Era'. *Prospect*, Science & Technology, 30 September. Available from: <https://www.prospectmagazine.co.uk/science-and-technology/why-we-are-still-living-in-the-sputnik-era> [Accessed 5 October 2021].

Waltz, K., 1979. *A Theory of International Politics*. Reading, MA: Addison-Wesley. Available from: https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf [Accessed 24 October 2020].

Wang, R-S, Saadatpour, A. and Albert, R., 2012. 'Boolean Modelling in Systems Biology: An Overview of Methodology and Applications'. *Physical Biology*, 9 (5), online article ID, 055001.

Ward, A., 2018. 'ISIS's USE of Social Media Still Poses a Threat to Stability in the Middle East and Africa'. *Georgetown Security Studies Review*, 10 December. Available from: <https://georgetownsecuritystudiesreview.org/2018/12/10/isiss-use-of-social-media-still-poses-a-threat-to-stability-in-the-middle-east-and-africa/> [Accessed 19 October 2019].#

Waterman, S., 2006. 'Thai Militants Learn from Iraq Insurgency'. United Press International, 15 February. Available from: <https://www.upi.com/Defense-News/2006/02/15/Thai-militants-learn-from-iraq-insurgency/85611140036186/> [Accessed 1 June 2022].

Watts, C., 2016. Expert on the effect of 'cascading terrorism'. Video. MSNBC, 29 June. Available from: <https://www.msnbc.com/morning-joe/watch/expert-on-the-effect-of-cascading-terrorism-715100739718> [Accessed 16 October 2019].

WDD, 2009. The History and Evolution of Social Media. Webdesignerdepot.com, Interactive Design, 7 October. Available from: <https://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/> [Accessed 19 July 2018].

Weaver, M. A., 2006. 'The Short, Violent Life of Abu Musab al-Zarqawi.' *The Atlantic*, July/August. Available from: <https://www.theatlantic.com/author/mary-anne-weaver/> [Accessed 12 June 2022].

Weber, M., 2009. 'The Permanent Character of the Bureaucratic Machine'. In: H. H. Gerth and C. W. Mills, eds, *From Max Weber: Essays in Sociology*. New York: Oxford University Press, pp. 228-229.

WEF 2013a. *Digital Wildfires in a Hyperconnected World*. Global Risks Report 2013. 8th edition. World Economic Forum. Available from: <http://reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-a-hyperconnected-world/> [Accessed 19 April 2018].

WEF 2013b. *Perspectives on a Hyperconnected World: Insights from the Science of Complexity*. World Economic Forum, January. Available from: http://www3.weforum.org/docs/WEF_GAC_PerspectivesHyperconnectedWorld_ExecutiveSummary_2013.pdf [Accessed 19 April 2018].

Wege, C.A., 2010. 'Hizballah's Bekka Organization'. *Perspectives on Terrorism*, 4 (3). Available from: <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/105/html> [Accessed 31 January 2021].

Wege, C.A., 2008. 'The Hizballah Security Apparatus'. *Perspectives on Terrorism*, 2 (7). Available from: <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/42/html> [Accessed 12 February 2021].

Weik, M., 1961. The ENIAC Story. US Army Research Laboratory. Available from: <https://web.archive.org/web/20110814181522/http://ftp.arl.mil/~mike/comphist/eniac-story.html> [Accessed 4 February 2020].

Weimann, G., 2014. 'New Terrorism and New Media'. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars. Available from: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/STIP_140501_new_terrorism_F.pdf [Accessed 14 July 2020].

Weimann, G., 2010. 'Terror on Facebook, Twitter, and YouTube'. *Brown Journal of World Affairs*, 16 (11), pp. 45-54. Available from: <http://bjwa.brown.edu/16-2/terror-on-facebook-twitter-and-youtube/> [Accessed 15 February 2020].

Weimann, G., 2008. 'Al-Qa'ida's Extensive Use of the Internet'. *CTC Sentinel*, 1 (2), January. Available from: <https://ctc.westpoint.edu/wp-content/uploads/2010/06/Vol1Iss2-Art3.pdf> [Accessed 30 March 2022].

Weinberger, E., 1991. 'Local properties of Kauffman's NK Model: A Tunably Rugged Energy Landscape'. *Physical Review A*, 44, pp. 6399-64.

Weiser, M., 1991. 'The Computer for the 21st Century'. *Scientific American*, 265 (3), pp. 94-104. Available from: <https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf> [Accessed 17 July 2018].

Weiss, M. and Hassan, H., 2015. *ISIS: Inside the Army of Terror*. New York: Regan Arts

Western, B., 1998. 'Causal Heterogeneity in Comparative Research: A Bayesian Hierarchical Modelling Approach'. *American Journal of Political Science*, 42 (4), pp. 1233-1259.

White, J. R., 2012. *Terrorism and Homeland Security*. Seventh edition. Belmont, CA: Wadsworth.

Whitlock, C., 2006. Al-Zarqawi's Biography. *The Washington Post*, Thursday, 8 June. Available from: https://www.washingtonpost.com/wp-dyn/content/article/2006/06/08/AR2006060800299.html?nav=rss_world/africa [Accessed 2 May 2022].

Widholm, A., 2018. 'Transnational News Consumption and Digital Content Mobility'. *Journalism Studies*, 20 (10), pp. 1472-1490. Available from: <https://www.tandfonline.com/doi/pdf/10.1080/1461670X.2018.1526642?needAccess=true> [Accessed 5 October 2021].

Wiener, N., 1948. *Cybernetics: Or Control and Communication in the Animal and the Machine*. Cambridge, MA: The MIT Press. Available from: <http://www.allen-riley.com/utopia/cybernetics.pdf> [Accessed 1 August 2018].

Wigginton, C., 2017. *Global Mobile Consumer Trends: Second Edition*. Deloitte & Touche LLP. Available from: <https://www2.deloitte.com/bd/en/pages/technology-media-and-telecommunications/articles/gx-global-mobile-consumer-trends.html> [Accessed 10 May 2022].

Wilkinson, P., 2006. *Terrorism versus Democracy: The Liberal State Response*. Second edition. London and New York: Routledge.

Williams, M. and Dyer, W., 2017. 'Complex Realism in Social Research'. *Methodological Innovations*, 10 (2), pp. 1-8. Available from: <https://journals.sagepub.com/doi/pdf/10.1177/2059799116683564> [Accessed 23 September 2021].

Williams, P., 2021. 'Preserving the Selfless Heroism of the Passengers of United Flight 93'. *The New Yorker*, 10 September. Available from: <https://www.newyorker.com/news/dispatch/the-selfless-heroism-of-the-passengers-of-united-flight-93> [Accessed 19 September 2022].

Wilson Centre, 2019. Timeline: The Rise, Spread, and Fall of the Islamic State. Wilson Centre, Insight & Analysis, October 28. Available from: <https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state> [Accessed 12 May 2022].

Wooley, J., Limperos, A. and Oliver, M. B., 2010. 'The 2008 Presidential Election, 2.0: A Content Analysis of User-Generated Political Facebook Groups'. *Mass Communication and Society*, 13 (5), pp. 631-652.

Wright, G., 2021. ARPANET. TechTarget, November. Available from: <https://www.techtarget.com/searchnetworking/definition/ARPANET> [Accessed 12 September 2022].

Wudka, J., 2006. *Relativity, Space-Time and Cosmology*. Cambridge: Cambridge University Press. Available from: <https://www.scribd.com/document/13727174/Relativity-Space-Time-and-Cosmology-J-Wudka> [Accessed 2 June 2018].

Yip, K., Patel, P., Kim, P., Engelman, D., McDermott, D. and Gerstein, M., 2008. 'An Integrated System for Studying Residue Coevolution in Proteins'. *Bioinformatics*, 24 (2), pp. 290-292. Available from: <https://academic.oup.com/bioinformatics/article/24/2/290/228702> [Accessed 13 October 2020].

Yocabet, C. and Reijnen, J., 2021. The Key to Connectivity: Interoperability and Open Networks. Blog, 29 September. Available from: <https://tiekinetix.com/en/blog/key-connectivity-interoperability-open-networks> [Accessed 25 April 2022].

Young, T. R., 1991. 'Chaos and Social Change: Metaphysics of the Postmodern', *The Social Science Journal*, 28 (3), pp. 289-305.

Yürük, B., 2022. Millions of Ukrainians at Risk Amid Russian attacks on Critical Infrastructure: UN. Anadolu Agency, 6 December. Available from: <https://www.aa.com.tr/en/russia-ukraine-war/millions-of-ukrainians-at-risk-amid-russian-attacks-on-critical-infrastructure-un/2756310#> [Accessed 6 December 2022].

Zaks, S., 2021. 'Updating Bayesian(s): A Critical Evaluation of Bayesian Process Tracing.' *Political Analysis*, 29 (1), pp. 58-74.

Zanini, M. and Edwards, S., 2001. 'The Networking of Terror in the Information Age'. In: J. Arquilla and D. Ronfeldt, eds, *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, pp. 29-60. Available from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.180.1418&rep=rep1&type=pdf> [Accessed 7 June 2022].

al-Zawahiri, A., 2008. 'Knights Under the Banner of the Prophet'. In: M. Perry and H. Negrin, eds., *The Theory and Practice of Islamic Terrorism: An Anthology*. New York: Palgrave Macmillan, pp. 49-57.

Zelin, A., 2014. 'The War Between ISIS and Al-Qaeda for Supremacy of the Global Jihadist Movement'. Research Notes, Number 20 (June). The Washington Institute of Near East Policy. Available from: <https://www.washingtoninstitute.org/media/2714> [Accessed 12 June 2022].

Zelin, A., 2013. The State of Global Jihad Online: A Qualitative, Quantitative and Cross-Lingual Analysis. New America Foundation, January.

Zeuner, L., 1999. 'Margaret Archer on Structural and Cultural Morphogenesis.' *Acta Sociologica*, 42 (1), pp. 79-86. Available from: https://www.jstor.org/stable/4201123?seq=1#metadata_info_tab_contents [Accessed 23 August 2021].

Zisser, E., 2011. 'Iranian Involvement in Lebanon'. *Military and Strategic Affairs*, 3 (1), pp. 3-16. Available from: [https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/\(FILE\)1308129458.pdf](https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1308129458.pdf) [Accessed 9 November 2021].

Zlotnik, G. and Vansintjan, A., 2020. 'Storage of Information and its Implications for Human Development: A Dialectic Approach'. *Frontiers in Psychology*, 16 July. Available from: <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01715/full> [Accessed 7 December 2022].