Beyond Twitter Revolutions: The Impact of Digital Media Logistics on Terror Networks of Communication in Iraq and Syria from 2014 to 2016

Ahmad Mahmoud Shehabat

Follow this and additional works at: https://ro.uow.edu.au/theses1

University of Wollongong

Copyright Warning
You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au
Beyond Twitter Revolutions: The Impact of Digital Media Logistics on Terror Networks of Communication in Iraq and Syria from 2014 to 2016

This thesis is presented in fulfilment of the award of the degree

DOCTOR OF PHILOSOPHY

From

THE UNIVERSITY OF WOLLONGONG

By

AHMAD MAHMOUD SHEHABAT, BA, MA, MA (HONS)

SCHOOL OF THE ARTS, ENGLISH AND MEDIA

2018
Declaration of Originality

I, Ahmad Mahmoud Shehabat, declare that this thesis, submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of The Arts, English and Media, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

15/08/2018
Table of Contents

Declaration of Originality ............................................................................................................. i
Table of Contents ........................................................................................................................ ii
List of Figures ................................................................................................................................ vii
List of Tables ............................................................................................................................... xii
List of Abbreviations .................................................................................................................... xiii
Abstract ........................................................................................................................................ xiv
Acknowledgements .................................................................................................................... xvi
Timeline of ISIS’ operations 2014-2016 ....................................................................................... xvii
Introduction ................................................................................................................................... 1
Research Questions ...................................................................................................................... 12
Theoretical Base .......................................................................................................................... 13
Study Approaches ...................................................................................................................... 23
Aims and Scope of the Study ........................................................................................................ 25
Methodology .................................................................................................................................. 29
Platform Analysis ........................................................................................................................ 31
Screenshots .................................................................................................................................... 32

1 Chapter 1: Terror Organisations and Web Technology in the Arab World in the 21st Century ................................................................................................................................. 34

1.1 Introduction ............................................................................................................................ 34
1.2 The Emergence of Jihadi Movements—A Historical Perspective ........................................... 35
1.3 The Rise of Hamas .................................................................................................................. 36
1.4 The Rise of Al-Qaeda ............................................................................................................. 37
1.5 Al-Qaeda in Iraq (AQI) ........................................................................................................... 39
1.6 Terror Communication Before the Emergence of ISIS ............................................................ 40
1.7 Al-Qaeda’s Cyber Operations ................................................................................................. 40
1.8 Al-Qaeda Prior to September 11, 2001 ................................................................................. 42
1.9 The Occupation of Iraq in 2003 and the Emergence of ISIS .................................................. 44
1.10 The Logistics of Psychological Warfare ................................................................................. 45
1.11 Hezbollah’s Media Strategy ................................................................................................... 49
1.12 Information Dissemination During the 1996 and 2006 Lebanon Wars with Israel ............... 51
1.13 Social Media Networks During the 2006 Lebanon War ....................................................... 54
1.14 Information Warfare—Hezbollah Versus Israel .................................................................... 57
## Chapter 2: Post-Arab Spring Networking Dynamics—Information-Centric Warfare and Social Media Networks

### 2.1 Introduction

### 2.2 Web 2.0 and the Arab Spring Uprisings

### 2.3 Networking Tendencies and Political Polarisation During the Arab Spring Uprisings

### 2.4 Political Polarisation and Mobilisation Logistics

### 2.5 Networks of Outrage and Hope

### 2.6 Networks of Antagonism and Hate

### 2.7 Networks of Terror

### 2.8 Syrian Case Study

#### 2.8.1 Social Media Warfare—Syrian Free Army versus Syrian Electronic Army

#### 2.8.2 Digital Logistics of the Syrian Uprising

### 2.9 The Fake YouTube

### 2.10 The Facebook Interface

### 2.11 Skype Encryption Tools

### 2.12 Social Media Networks: Information-Centric Warfare

### 2.13 Iraq Case Study—Anbar Uprisings

### 2.14 Conclusion

## Chapter 3: ISIS’ Information Operations—A Strategic Narrative Perspective

### 3.1 Introduction

### 3.2 ISIS’ Organisational Structure, Politics and Religious Aims

### 3.3 The Strategic Deployment of High Definition Productions

### 3.4 Understanding ISIS’ Information Operations

### 3.5 The Strategic Logic of ISIS’ Information Operations—A Strategic Narrative Perspective

### 3.6 The Strategic Narrative of ISIS Networks

### 3.7 Re-Establish the Caliphate

#### 3.7.1 Utopia

#### 3.7.2 Supremacy

#### 3.7.3 Sharing Grievances and Representations of Victimhood

### 3.8 United Sunnis
Chapter 4: Promoting a Terror Narrative—ISIS’ Information Logistics

1. Introduction .................................................................................................................. 157
2. Understanding ISIS’ Information Logistics ................................................................. 159
3. Understanding the Paradigm Shift in ISIS’ Logistics of Information ......................... 164
4. Physical Paradigm ....................................................................................................... 165
5. Cognitive Paradigm ..................................................................................................... 167
6. Social Informatics ....................................................................................................... 169
7. Social Media Platforms as Logistics .......................................................................... 170
8. ISIS’ Information Operations on Twitter ..................................................................... 171
9. Intuitive and Technical ............................................................................................... 172
   9.1 Dissemination Mechanisms—Retweet, Reply, Like and Hashtag .......................... 172
   9.2 Interconnectivity and Networking ......................................................................... 174
   9.3 Convenience—Anonymity, Mobile Phone Applications and Ease-of-Use ......... 176
10. Objectives of Usage .................................................................................................... 177
    10.1 Partaking in Media War ....................................................................................... 178
    10.2 Radicalisation and Recruitment ......................................................................... 180
    10.3 Spread of Propaganda ....................................................................................... 182
11. How ISIS Games Twitter ........................................................................................... 183
    11.1 Use of Active Hashtags .................................................................................... 183
    11.2 Command and Control Operations .................................................................... 186
    11.3 Manoeuvre Warfare ........................................................................................... 188
12. Actor–Network Theory ............................................................................................... 189
13. ISIS’ Media Outlets .................................................................................................... 196
14. Propaganda Videos—Content Analysis ..................................................................... 200
    14.1 Message to America ............................................................................................. 201
    14.2 Flames of War .................................................................................................... 203
    14.3 Healing of the Believers’ Chests ........................................................................ 204
15. Going Viral—Disseminating the Message of Terror ..................................................... 205
16. Conclusion .................................................................................................................... 208

Chapter 5: Degrading Operation—Attacking the Digital Logistics of ISIS’ Networks

1. Introduction .................................................................................................................... 212
5.2 Attack ISIS’ Digital Logistics .................................................................................. 214
5.3 Phase One—Degrading and Destroying ................................................................. 217
  5.3.1 The Whack-a-Mole Operation .......................................................................... 219
  5.3.2 Interaction and Isolation ................................................................................... 221
5.4 Collective Collaboration—Social Media Platforms Approach to ISIS’ Content...222
5.5 Terms of Service Violations .................................................................................. 225
5.6 Phase Two—Countering ISIS’ Narrative ............................................................... 227
5.7 Counternarrative Actors ....................................................................................... 230
  5.7.1 Sawab Centre .................................................................................................. 230
  5.7.2 United States Department of State’s Team ...................................................... 233
  5.7.3 #TruthAboutISIS Hashtag ............................................................................. 235
  5.7.4 UK Against Daesh ......................................................................................... 237
5.8 Phase Three—Hacking and Information Warfare .................................................. 238
5.9 Operation Ice ISIS ............................................................................................... 240
5.10 CtrlSec ................................................................................................................ 242
5.11 Data Analysis of Reported Accounts .................................................................. 245
5.12 Conclusion .......................................................................................................... 247
6 Chapter 6: ISIS’ Information Feedback Loop .......................................................... 249
  6.1 Introduction .......................................................................................................... 249
  6.2 Case Study One: Black-Boxing the Black Flag—Anonymous Sharing Platforms and
      ISIS’ Content Distribution Tactics ...................................................................... 251
  6.3 The Rise of ISIS on Information Environments .................................................. 252
  6.4 Degrading ISIS’ Online Activities ...................................................................... 255
  6.5 Anonymous Platforms as Black Boxes ............................................................... 259
  6.6 ISIS’ Black Boxes ................................................................................................ 261
    6.6.1 JustPaste.it ..................................................................................................... 261
    6.6.2 Sendvid.com ................................................................................................. 266
    6.6.3 Dump.to ........................................................................................................ 269
  6.7 Discussion ............................................................................................................ 272
  6.8 Conclusion .......................................................................................................... 275
  6.9 Case Study Two: Encrypted Jihad—Investigating the Role of Telegram Application
      in Lone Wolf Attacks in the West ........................................................................ 276
  6.10 Introduction ....................................................................................................... 276
  6.11 Methodology ..................................................................................................... 278
  6.12 Terror Socio-Sphere .......................................................................................... 280
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.3</td>
<td>Quantitative</td>
<td>335</td>
</tr>
<tr>
<td>7.7.4</td>
<td>Qualitative</td>
<td>336</td>
</tr>
<tr>
<td>7.8</td>
<td>Observe, Orient, Decide and Act Loop Effect on ISIS’ Networks</td>
<td>337</td>
</tr>
<tr>
<td>7.8.1</td>
<td>Generators</td>
<td>341</td>
</tr>
<tr>
<td>7.8.2</td>
<td>Aggregators</td>
<td>342</td>
</tr>
<tr>
<td>7.8.3</td>
<td>Disseminators</td>
<td>343</td>
</tr>
<tr>
<td>7.9</td>
<td>Conclusion</td>
<td>344</td>
</tr>
</tbody>
</table>
List of Figures

Figure 1. ‘We Are All Khaled Said’ Facebook page. 73
Figure 2. Fake YouTube site used by Syrian Electronic Army to trap activists. 88
Figure 3. Fake Facebook interface page. 90
Figure 4. Skype encryption tool run by the Syrian Electronic Army. 91
Figure 5. Links to Skype encryption, generated by Syrian Electronic Army. 91
Figure 6. Screenshot of the hacking of Harvard University website by Syrian Electronic Army. 93
Figure 7. Screenshot of the hacked Facebook page of Barack Obama. 94
Figure 8. Screenshot of hacked The Independent by Syrian Electronic Army. 95
Figure 9. The political structure of ISIS. 101
Figure 10. The stages to establish the Caliphate. 113
Figure 11. Findings of scholarly research on ISIS’ strategic narrative. 113
Figure 12. Results of Milton’s study. 119
Figure 13. ISIS’ media releases, January 2015 – August 2016. 119
Figure 14. Word cloud findings of the analysis of six of Dabiq and Rumiyyah ISIS magazines. 150
Figure 15. Capturing information operation objectives of ISIS networks. 121
Figure 16. Screenshot of Mujatweet, episode 8. 125
Figure 17. Eid celebrations in Raqqa, Syria. 125
Figure 18. Post by ‘Speak the Truth’ Twitter account by @6Haqq. Posted on 21 March 2015. 126
Figure 19. Six media narratives of ISIS networks between 2014 and 2015. 128
Figure 20. Utopia narrative subcategories of ISIS networks between 2014 and 2015. 128
Figure 21. ISIS flag. 130
Figure 22. Caliph Abu Bakr Al-Baghdadi. 130
Figure 23. ISIS passports and golden dinar. 130
Figure 24. The application of sharia law in Raqqa, Syria. 131
Figure 25. Screenshot of first release of The End of Sykes-Picot video. 132
Figure 26. Screenshots from The End of Sykes-Picot propaganda video by Al-Hayat Media Center. 133
Figure 27. The main narratives aimed to unite Sunnis. 134
Figure 28. Screenshot from One Nation video produced by Al-Furat Media. 136
Figure 29. Screenshot of Revenge of the Desert propaganda video. 136
Figure 30. Screenshot of The Fertile Nation propaganda video. 137
Figure 31. Diagram representing the relationship between fear, recruitment and radicalisation. 137
Figure 32. Screenshots of messages disseminated via Nashir Telegram channel. 139
Figure 33. Screenshot of propaganda messages to support stay and expand narrative.

Figure 34. Screenshot obtained from Stay for the End Times video production.

Figure 35. The land ISIS planned to control, as shown on their press releases.

Figure 36. Country of origin for the foreign fighters who joined ISIS in 2015.

Figure 37. Screenshot of Inside video production.

Figure 38. A message to encourage Muslims to migrate to ISIS’ lands.

Figure 39. Screenshot of a message sent via Telegram to encourage migration to ISIS’ land.

Figure 40. Screenshot shows signs for Al-Naba, ISIS’ Arabic Magazine.

Figure 41. Screenshot shows ISIS videos on scribd.com.

Figure 42. The Caliphate Twitter.

Figure 43. ISIS encourage its followers to use Twitter to disseminate, tweet and upload.

Figure 45. Message forwarded by Gazwa Telegram channel.

Figure 46. A message to join the ‘Baqiya Family’ group and a message from Usudul Islam to ‘Baqiya Family’.

Figure 47. Mobile phone usage among ISIS supporters.

Figure 48. Message forwarded by @Kawasir_AlNashr on Telegram channel.

Figure 49. Message forwarded from Nashir Political Service, Telegram channel.

Figure 50. A tweet from @DseVcjd, stating that infidels must be fought with money, hands and tongues (including Twitter).

Figure 51. Message of recruitment disseminated to ISIS’ Twitter feed.

Figure 52. Propaganda material posted to Twitter for recruitment purposes.

Figure 53. An example of active Twitter hashtags after the terror attack in Nice, France.

Figure 54. An example of active Twitter hashtags after a terror attack in Germany.

Figure 55. ISIS shows how to connect multiple accounts in one platform.

Figure 56. Diagram of ISIS’ logistics.

Figure 57. ISIS’ media wing and media productions.

Figure 58. Screenshot from Message to America propaganda video.

Figure 59. Screenshot of Flames of War propaganda production.

Figure 60. Screenshot from Healing the Believer’s Chests propaganda production.

Figure 61. A tweet by Hend Amry, showcasing the first use of #ISISMediaBlackout hashtag.

Figure 62. Cartoon depicting the Whack-a-Mole operation.

Figure 63. Abul Muthanna’s reply to the United States’s Whack-a-Mole operation.

Figure 64. Screenshot of Sawab Center.

Figure 65. Screenshot of the narrative disseminated by Sawab Center.

Figure 66. Screenshot of Sawab Center’s anti-ISIS narrative.

Figure 67. Screenshot of the Arabic USDOS Team Twitter account.
Figure 72. Screenshot of #TruthAboutISIS hashtag Twitter account.

Figure 73. Screenshot of ‘UK Against Daesh’ Twitter account.

Figure 74. The type of messages used by ‘UK Against Daesh’, posted to Twitter.

Figure 75. Screenshot of ‘Operation Ice ISIS’ Twitter account, operated by Anonymous.

Figure 76. Screenshot shows false flags of suspected ISIS accounts.

Figure 77. Screenshot of CtrlSec’s Twitter account.

Figure 78. Screenshot of CtrlSec website.

Figure 79. Screenshot of ISIS-affiliated Twitter accounts, as reported by CtrlSec in 2015.

Figure 80. Screenshot of ISIS-affiliated Twitter accounts, as reported by CtrlSec in 2016.

Figure 81. Screenshot of number of ISIS-affiliated content on JustPaste.it, reported by CtrlSec in 2017.

Figure 82. Monthly removal rate of ISIS’ products on JustPaste.it.

Figure 83. A tweet posted by Jim Berger on 20 September 2014.

Figure 84. Cover of Dabiq magazine, issue hosted by JustPaste.it.

Figure 85. Tweet with extreme content posted by ISIS members on JustPaste.it.

Figure 86. Tweet with material advertising migration to ISIS-held territory posted on JustPaste.it.

Figure 87. JustPaste.it traffic in November 2015.

Figure 88. A copy of the letter sent by Abu Talout Al-Khurasani to Zurawek.

Figure 89. Screenshot of video titled The Happiness of Almojahideen, posted to Sendvid.

Figure 90. Sendvid links to ISIS content, titled Message to the Tyrants of Jordan.

Figure 91. Screenshot of iBRABO Twitter account, highlighting the use of dump.to by ISIS.

Figure 92. Jihadi training materials, books and propaganda available on dump.to.

Figure 93. Links to Dabiq propaganda magazine on dump.to.

Figure 95. Some significant dumps by Al-Hayat Media Center (e.g., news reports, breaking news).

Figure 97. Detrimental use of social media by ISIS: an information warfare perspective.

Figure 98. OpIceISIS screenshot.

Figure 99. Message forwarded from the Nashir Telegram channel.

Figure 100. Infographic demonstrating ISIS’ links to lone wolf attacks.

Figure 101. Screenshot from ISIS Telegram channel, Nashir Political Services.

Figure 102. Screenshot obtained from UCC Telegram Channel.

Figure 103. Screenshot obtained from UCC Telegram Channel, titled ‘Lone Wolves #getready’.

Figure 104. Screenshot obtained from SITE intelligence group discussing the #RioLW hashtag.
Figure 105. Screenshot from the Sham State Media Organisation Telegram Channel, encouraging more attacks.  
Figure 106. Screenshots from a propaganda video encouraging attacks, posted on the Barood Telegram Channel.  
Figure 107. Screenshot from ISIS Telegram channels celebrating lone wolf attacks.  
Figure 108. Amaq News Agency claiming responsibility for lone wolf attacks.  
Figure 109. Video of Wurzburg attacker, Muhammad Riyad, pledging allegiance to ISIS.  
Figure 110. Screenshot shows Islamic fundamentalism is not a major catalyst for lone wolf attacks in the West.  
Figure 111. Coordination among ISIS networks.  
Figure 112. ISIS claiming successful attacks in Europe.  
Figure 113. A diagram of the observe, orient, decide, act (OODA) loop, showing the OODA loop functions during combat.  
Figure 114. ISIS used #shahz Al-hemam—that is, ‘glad tidings’—to assert their continued use of popular social media networks for electronic jihad.  
Figure 115. An illustration of ISIS’ implementation of the observe, orient, decide and act loop.  
Figure 116. Inside the observe, orient, decide and act loop of ISIS’ adversaries.  
Figure 117. Screenshot of Twitter feed of ISIS propagandist, Shami Witness.  
Figure 118. Hybrid web log links to ISIS content disseminated via Telegram.  
Figure 119. Diagram explaining the observe, orient, decide and act loop effects on ISIS networks.  
Figure 120. Illustration of the swarming operation of ISIS networks.  
Figure 121. Example of information generator #Al-Hayat.  
Figure 122. Example of information aggregator on Telegram channel.  
Figure 123. Example of information disseminator on Telegram channel.
List of Tables

Table 1. Findings of scholarly research on ISIS’ strategic narrative.......................118
Table 2. Number of Lone Wolf Attacks Against Western Countries, Weapons Used and Number of Causalities..............................................................293
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>artificial intelligence</td>
</tr>
<tr>
<td>ANT</td>
<td>actor–network theory</td>
</tr>
<tr>
<td>AQI</td>
<td>Al-Qaeda in Iraq</td>
</tr>
<tr>
<td>BBC</td>
<td>British Broadcasting Corporation</td>
</tr>
<tr>
<td>C2</td>
<td>command and control</td>
</tr>
<tr>
<td>CGI</td>
<td>computer-generated images</td>
</tr>
<tr>
<td>CSCC</td>
<td>Center for Strategic Counterterrorism Communications</td>
</tr>
<tr>
<td>CVE</td>
<td>Countering Violent Extremism</td>
</tr>
<tr>
<td>DDoS</td>
<td>distributed denial-of-service</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defence</td>
</tr>
<tr>
<td>DoS</td>
<td>denial-of-service</td>
</tr>
<tr>
<td>EFF</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>GTI</td>
<td>Global Terrorism Index</td>
</tr>
<tr>
<td>HD</td>
<td>high definition</td>
</tr>
<tr>
<td>IDF</td>
<td>Israeli Defence Forces</td>
</tr>
<tr>
<td>IO</td>
<td>information operation</td>
</tr>
<tr>
<td>IP</td>
<td>internet protocol</td>
</tr>
<tr>
<td>ISI</td>
<td>Islamic State of Iraq</td>
</tr>
<tr>
<td>ISIS</td>
<td>Islamic State of Iraq and Syria</td>
</tr>
<tr>
<td>LCC</td>
<td>Local Coordination Committee</td>
</tr>
<tr>
<td>MENA</td>
<td>Middle East and North Africa</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organisation</td>
</tr>
<tr>
<td>NCW</td>
<td>network-centric warfare</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>OODA</td>
<td>Observe, Orient, Decide and Act</td>
</tr>
<tr>
<td>PLO</td>
<td>Palestinian Liberation Organisation</td>
</tr>
<tr>
<td>PSYOP</td>
<td>psychological warfare operation</td>
</tr>
<tr>
<td>SEA</td>
<td>Syrian Electronic Army</td>
</tr>
<tr>
<td>SFA</td>
<td>Syrian Free Army</td>
</tr>
<tr>
<td>SITE</td>
<td>Search for International Terrorist Entities</td>
</tr>
<tr>
<td>SMN</td>
<td>social media networks</td>
</tr>
<tr>
<td>StratCom</td>
<td>Strategic Communication Centre of Excellence</td>
</tr>
<tr>
<td>TOS</td>
<td>Terms of Service</td>
</tr>
<tr>
<td>TOR</td>
<td>the onion routers</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>UCC</td>
<td>United Cyber Caliphate</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USDOS</td>
<td>United States Department of State</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>WTN</td>
<td>Worldwide Television News</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>
Abstract

This study examines the information operations strategy of the Islamic State of Iraq and Sham (ISIS), focusing on the 2014-2016 period. Using extensive case studies of ISIS-related information warfare operations, the study examines the online manoeuvre tactics deployed by ISIS to survive counter-operations aimed against its propaganda networks. The thesis uses a conceptual framework informed by John Boyd’s OODA loop model, actor network theory, and stigmergic swarm operations in digital media environments. The study argues that anonymous sharing platforms such as justpaste.it and Telegram, and to a lesser extent, Twitter, have been instrumental in allowing individual jihadists to generate content, disseminate propaganda, and communicate freely while routing around filtering practiced by popular social media networks (SMNs). The study suggests that the failure of ISIS’ adversaries in operating inside the OODA loop of ISIS led to the organisation’s survival, the evolution of its network, and the proliferation of its information operations.
Acknowledgements

I begin by dedicating this thesis to my parents who had patiently waited for me to embark on my PhD journey but didn’t live to see how it ends. To my beloved Mum and Dad, I say peace and mercy upon your souls, I wish you were here with me to celebrate my happiness and joyous moments. I would like to thank my wonderful supervisors who patiently accompanied me on this challenging learning journey. I extend my deepest gratitude to my Principal Supervisor, Dr. Teodor Mitew, who pushed the boundaries of my research beyond my original plans. I have been extremely lucky to have a supervisor who cared so much about my work and myself, and who responded to my questions and queries so promptly. Our discussions in his office and online brainstorming sessions opened my eyes to fundamentally new areas of research.

I would also like to extend my appreciation to my co-supervisor, Dr. Christopher Moore. I thank Dr Moore for his support and the insights gained from his valuable comments and suggestions. I am truly grateful to them both for their friendship, wisdom and support. To them, I owe a debt of gratitude for their time, sincerity and courage. I also thank Dr. Susan Ballard, the head of postgraduate studies, for her support and encouragement during my PhD journey. I must express my gratitude to Fadia, my wife, for her continuous support and encouragement. I wish to honour my children, brothers and sisters who stood by me and supported me throughout my period of study. Special thanks to my dearest brother Dr. Issa Shehabat for his courage and continuous support. Finally, I conclude by thanking all my friends and colleagues who believed in me and supported me. Special thanks go to Dr. Yahia Alzoubi, Dr. Foad Al-Shyyab, and Mr. Raid Al-Omary for friendship and moral support during my candidature.
Timeline of ISIS’ operations 2014-2016

2014

January: ISIS takes over Raqqa and declares it the capital of the ISIS emirate.

February 3: Al Qaeda officially cuts ties with ISIS.

June 10: ISIS takes over Mosul, launching its largest offensive to date.

June: 96,000 ISIS Twitter accounts were identified (Morgan, 2014).

June 11: ISIS militants take over Tikrit (the birth city of Saddam Hussein).

June 18: Iraq asks the United States to conduct airstrikes against ISIS.

June 29: ISIS announces the establishment of a caliphate under the leadership of Abo Baker Al-Baghdadi.

July 18: Operation degrading ISIS’ digital capabilities launched.

2015

February: Telegram application used as prime hub for ISIS.

May 17: ISIS takes over Ramadi, Iraq.

May 20: ISIS seizes the ancient Syrian city of Palmyra.

May 21: ISIS militants takes full control of Sirte, Libya – Muammar Qaddafi’s hometown.

June: Marks the highs of microblogging platforms (Justpaste, Sendvid) used by ISIS.

Dec 27: Iraqi military forces seize Ramadi from ISIS.

2016

March 27: The Syrian army supported by Russian airstrikes recaptured the city of Palmyra from ISIS.

May 19: Iraqi forces retake the western town of Rutbah.

May 23: Iraqi forces, aided by U.S. and coalition airstrikes, advanced on Fallujah, which ISIS had held since 2014.
May 24: Kurdish forces backed by U.S. airstrikes launched an offensive on territory north of Raqqa, Syria.

June 26: The Iraqi army retakes Fallujah from ISIS.

October 16: Iraq launches a U.S. backed campaign to liberate Mosul from the Islamic State.

December 11: ISIS fighters recapture Palmyra from the Syrian government.

December 29: Iraqi security forces launch ‘we are coming Nenawa’ campaign against the Islamic State.
Introduction

Your military force is attacking us daily in Iraq, your strikes caused casualties among Muslims, you are no longer fighting an insurgency we are and Islamic army and a state. Any aggression against our state will result in bloodshed against your own people¹.

These were the words of Mohammed Emwazi,² who left the music industry to become a well-known Islamic terrorist who appears in ISIS’ first HD video propaganda. He was dressed in black, with his victim in red, in front of a film set-up scene. A coded message was uploaded to the internet, with many more to come. On 19 August 2014, Mohammed Emwazi appeared in ISIS’,³ first beheading video,⁴ titled Message to America.⁵ In this video, ISIS utilised, arguably, professional tools of media production, including GoPro cameras, multiple angle screenshots, professional montage, and use of sound devices. Overall, this marked the first time a terror organisation had produced a high-quality video through its own media outlet (Rose, 2014). A decade ago, Al-Zarqawi himself beheaded Nick Berg,⁶ during a live

¹ Jihad John’s message to the US government depicted in ISIS’ first media production “Message to America.
² Also known as Jihadi John, a British rapper who joined ISIS in 2013 and appeared in ISIS’ first propaganda video production.
³ Also known as IS (Islamic State), ISIL (Islamic State of Iraq and Levant) and Daesh (Arabic acronym for Dawlah Islamyah fe Eraq wa Sham). In this thesis I use ISIS as the most popular acronym for this organisation, as used by world governments and scholars.
⁴ The video was produced by Al-Hayat media productions and first appeared on the Al-Hayat Twitter account.
Historically, the first beheading video posted to the World Wide Web by Al-Qaeda was of Daniel Pearl in 2002.
⁵ This is the first message produced by ISIS.
⁶ US communications facilities contractor beheaded in Iraq in 2004.
propaganda event on the internet, but the footage was of amateurish quality compared to ISIS propaganda productions.

However, compared to Al-Qaeda’s propaganda productions, ISIS has strengthened its propaganda machine by producing well-crafted videos uploaded to a plethora of digital media environments. These images have a memetic value – that is why they spread so fast and have such propaganda value. According to Gladwell (2010), “ideas and products and messages and behaviours spread just like viruses do” (p. 7).

To understand the need for ISIS to establish communication networks in the digital information environments, it is necessary to examine the geographical space they operate in, the political structure of its organisation, its need for jihadi and military logistics, and the number of active combats in which they are involved. It must be noted that ISIS has created a new tendency and paradigm shift in terror communication in comparison to other terror organisations such as Al-Qaeda, El-Shabab, and Boko Haram. This shift appears through three strategic developments harnessing of digital media environments that include, social media sites and services, anonymous sharing portals, and encrypted communication applications. It is the strategic combination of the use of these platforms that has distinguished ISIS from all other terror networks.

---

7 According to the US’s DOD “The information environment is the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information” (cited in Prisco, 2012, p. iv).

8 Thomas Kuhn (1996) defined paradigms as “universally recognized scientific achievements that, for a time provide model problems and solutions for a community of researchers” (P. x).
First, ISIS’ weaponisation of digital media platforms aims to achieve information operation\(^9\) (IO) objectives. The United States Department of Defence (DoD) defined IO as “The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO” (DoD, 2006). That is, ISIS used digital media platforms as narrowcasting command and control (C2) operation centres and domains for information manoeuvre warfare. According to Owen (2008), “Manoeuvre warfare is a warfighting philosophy that seeks to shatter the enemy’s cohesion through a variety of rapid, focused, and unexpected actions, which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope” (p. 1). That is, ISIS strategically used social media platforms, encrypted media platforms, blogs and other anonymous portals to confuse, subjugate and influence the efforts of its adversaries in establishing an effective countering strategy. As Nissen (2015) noted, “Command and Control is a question of using social network media for communication and coordination and synchronisation of activities” (p. 60).

Second, stigmergic\(^{10}\) swarming of multiple information environments was a successful strategy that maintained ISIS’ networking structure and flow of information. In this shift, ISIS members are affiliated to swarm digital media environments with propaganda materials and creation of accounts to maintain flows of information, while stigmergy is used as a mechanism to explain the swarming activity (see sections 7.6 and 7.7). The third strategic

\(^9\) Will be discussed in detail in Chapter 3.

\(^{10}\)Stigmergy is the indirect coordination between the network actors. I will discuss the notion of stigmergy in detail in Chapter 7.
activity involves an ISIS paradigm shift from using popular SMNs such as Facebook and YouTube, to carry out manoeuvring operations via digital information environments giving them superiority over their adversaries. That is, the agility and speed of ISIS’ IO in production tactics and dissemination made it operate around the information loop of its adversaries.\textsuperscript{11} In other words, the emergence of the digital information environments, such as anonymous sharing portals (e.g., JustPaste.it, dump.to and sendvid.com), encryption telephone applications (e.g., Telegram, Signal and WhatsApp), and other digital media tools (e.g., bots and applications) have enabled ISIS to maintain its networking structure and flow of information in the face of the US and its allies waging operations designed to degrade ISIS capabilities. This is what war strategist and historian Von Clausewitz (1832) called “an increasing continuation of war by other means”. Therefore, the emergence of digital information environments, “presents new challenges and requires dramatic shifts in strategic thinking regarding national security and countering terrorism” (Aly, Macdonald, Jarvis & Chen, 2016, p. 61).

Arguably, in the face of ISIS, the world faces one of the most sophisticated terror networks ever. However, it is dependent on an IO strategy that is based on strategic narrative and attentive propaganda, which will be examined in Chapter three. Through this strategy, ISIS has managed to create powerful messages, targeting international audiences for potential recruits. ISIS adversaries (e.g. the US, Iraqi and Syrian governments, Shia militias, collective and individual hackers) must design and implement policies to tackle this growing phenomenon, particularly after the number of recruits increased from less than 1000 in 2011, to more than 3,500 Jihadists in Iraq in 2012, to an estimated 30,000 Jihadists by the end of

\textsuperscript{11} John Boyd’s theory on manoeuvre warfare will be discussed in Chapter 7.
2015 (Schmid, 2015, p. 1). The United States (US) strategy of degrading terror organisations resulted in unprecedented information-centric warfare between ISIS and its adversaries. A part of this strategy involves degrading ISIS’ digital media capabilities through suspending its accounts on social media platforms and other information environments. These approaches are known as a ‘Whack-a-Mole’ and ‘Interaction and Isolation’ which are examined in detail in Chapter 5.

The origin of ISIS can be traced back to Al-Zarqawi and his affiliation with Al-Qaeda in 2004. Al-Zarqawi led an insurgency, operating under Al-Qaeda in Iraq (AQI), after the fall of Saddam Hussein (Atwan, 2015; Stern & Berger, 2015). Al-Zarqawi targeted both US troops and Shia, sparking a bloody sectarian rift between Sunni and Shia Muslims. Fighting US troops in the Sunni stronghold of Anbar Province, Al-Zarqawi’s successor, Abu Omar Al-Baghdadi, named his organisation Islamic State of Iraq (ISI) in 2006 (Ignatius, 2015). In 2010, Abu Bakr Al-Baghdadi succeeded Abu Omar after he was killed by a US air strike. ISI was a powerful player during the Anbar uprisings in March 2013. The Iraqi government’s rejection of protesters demands, and the use of military forces to crush the Anbar protests, created an alliance between the tribal Sunni militias and ISI fighters (Ignatius, 2015). This alliance led to an attack in Mosul, Iraq, in 2013 and Abu Bakr Al-Baghdadi was asked by his supporters in Anbar to declare Islamic caliphate. As Stern and Berger observed in March 2014, “ISIS launched a Twitter hashtag campaign, with its supporters seemingly rising as populist mass to tweet, ‘We demand Sheikh Al-Baghdadi declare the caliphate’” (Stern & Berger, 2015, p. 17). Ultimately, the events of the Syrian and Anbar uprisings led to the rise of ISIS. The pattern of ISIS is a top-down structure were Abo Baker Al-Baghdadi was the

12 His real name is Ibraheem Awwad Al-Badri born in Samarra in Iraq in 1971.
command in chief aided by ‘shura council’. The way ISIS are managing their operations was based on ‘Auftragstaktik’\textsuperscript{13}, which means that their decision is centralised while execution is based on decentralization of command and control (C2) operations\textsuperscript{14}. The notion of ‘Auftragstaktik’ helps to understand ISIS’ C2 operation and how ISIS has weaponised information domains, such as social media platforms and mobile phone applications, to achieve its mission. To ISIS, the Al-Baghdadi was the highest command who designed operations to the individual actors that work independently in the network to achieve a successful mission, while social media platforms, and other encrypted communication channels, acted as control operation centres that mediate ISIS messages and all other information operation missions. In other words, ISIS’ organisational and technical attributes depend on information resources that are employed as C2 operations to achieve its ambitions.

Interestingly, before the emergence of ISIS, social media platforms have been credited as instrumental in galvanising the Arab spring uprisings. SMNs had a profound role in shaping these events (Howard, 2011; Dabashi 2012); however, their use changed dramatically throughout the uprisings. SMNs have been praised for having a significant role in tipping the balance of power in the interest of the grassroots movements (Meyer, 2011, Shehabat 2015). In the context of Iraq, these were ad-hoc alliances between disaffected Sunni, radicalised Jihadi elements, and tribal coalitions. Through these movements, SMNs helped grassroots

\textsuperscript{13} Auftragstaktik was developed as a military doctrine by the Prussians following their losses to Napoleon, when they realised they needed a systematic reorganisation of their centralised command structure. The term denotes mission-based orders, providing commanders with tactical freedom and a C2 culture of decentralised improvisation (Kallmes, 2017). This term will be discussed in Chapter 7.

\textsuperscript{14} Innovation of terrorist groups is discussed extensively by (Moghadam, 2013, Horowitz, 2010).
movements and rebel forces to outmanoeuvre, and sometimes topple, governments in the region. These platforms allowed communication and coordination to flow around government-imposed control.

The advancement of communication technologies - in particular, the proliferation of web 2.0 platforms,\(^{15}\) the ubiquitousness of internet connectivity and affordability of mobile phone technologies - have had an even greater impact on empowering anti-government movements and protests. Moreover, web 2.0 played a critical role in organising anti-World Trade Organisation (WTO) protests, worldwide Occupy movements, the London riots and democratic movements in the Arab world during the evolution of the Arab Spring uprisings.

The widespread use of information and communication technologies (ICTs) and social media applications in the Middle East and North Africa (MENA) region, created new avenues of political activism. This new wave of technologically generated political activism had a critical role in the pervasive social uprisings and political mobilisations that led to the downfall of the Mubarak, Ben Ali, Al-Qaddafi and Saleh governments in 2011 (Aday, Farrell, Lynch, Sides & Freelon, 2012; Anderson, 2011; Dabashi, 2012; Khamis, Gold & Vaughn, 2012).

The significant role played by social media platforms such as Twitter, Facebook and YouTube have even caused academics and journalists to refer to these events as the

\(^{15}\) Web 2.0 platforms, a term which proliferated in 2004, led to a new paradigm of social interaction which was beyond the imagination of the original web creators. The term, ‘Web 2.0’, was coined in 1999 by Darcy DiNucci; it was then popularised by Tim O’Reilly at the O’Reilly Media Web 2.0 conference in late 2004. Web 2.0 is a trend in the use of World Wide Web technology and web design that aims to enhance creativity, information sharing, and collaboration among users.
‘Facebook and Twitter revolutions’ and the ‘YouTube uprisings’ (Khamis et al., 2012). Castells (2012) called digital media platforms ‘networks of outrage and hope’. However, it is worth clarifying at this point that social media platforms offered tools for people to communicate and for other commercial purposes. People revolt, not tools. These tools had a key role in accelerating movements, raising awareness of abuses and atrocities, and facilitating political mobilisation. However, it is also worth noting, that governments harnessed these platforms to disseminate misinformation, monitor groups through surveillance techniques, and gather intelligence. Social media platforms also notified governments of upcoming events, which allowed them to trace charismatic leaders and the voices of anti-government movements. As a result, individuals could be identified and arrested, as was done in Egypt and Syria.

Pro-government organisations and individuals utilised social media platforms to counter anti-government movements. As such, the social media revolution began to display a darker side (Morozov, 2012); social media platforms became the weapons of information-centric warfare between pro and anti-government groups. Social media networks established political and ideological polarisation, which penetrated society, furthered political mobilisation, and catalysed information-centric warfare between anti and pro-government actors. Also, the rise of political Islam in the aftermath of the ousting of Hosni Mubarak, Muammar Al-Qaddafi, and Zine El Abidine Ben Ali, during the years 2011 - 2012 bifurcated society, resulting in the emergence of two, strong subgroups. These subgroups replaced what was once a large network of participants, who marched together in public squares. For example, in Syria, Egypt and Iraq, information-centric warfare emerged between pro-Islamists and anti-Islamists; this led to the emergence of new networking tendencies, which destabilised and challenged social structures. This bifurcation appeared first in social media platforms -
mainly Facebook.\textsuperscript{16} Thus, these new possibilities for networking also invited the emergence of ‘networks of antagonism and hate’ (Shehabat, 2015, p. 17).

The events of the Arab Spring uprisings have, arguably, led to the rise of new types of terror organisations, such as those that hijacked the uprisings in Iraq and Syria. A new organisational form emerged from and ended up shaping the future of Arab uprisings - that is, the emergence of ‘networks of terror’. One could argue that dissenter groups’ (e.g. We Are All Hamzah Al-Khateeb, the Syrian revolution 2011) established on social media (particularly on Facebook) has shifted from facilitating ‘networks of outrage and hope’ (Castells, 2013) to creating ‘networks of antagonism and hate’ (Shehabat, 2015) and ultimately, ‘networks of terror’.

In the Arab Spring uprisings in Syria, Iraq, Libya and Yemen, Al-Qaeda and ISIS emerged as power players and game changers in the destruction of these countries. These organisations were distinguished by their sophisticated use of digital media logistics to establish their political status. In this thesis, logistics does not refer to military logistics (e.g., ammunition, petrol and food supplies), but rather media logistics (e.g., hardware and software). These tools of content creation and dissemination became the logistics of \textit{performativity}. That is, through their use of social media platforms, anonymous sharing portals and encrypted communication channels, terror organisations have created international associations and enrolment processes that support the activation of potential recruits.

\textsuperscript{16}Facebook was the preferred social media platform by Arab youth during the 2011 uprisings (Dubai School of Government, 2011).
For non-state actors who were engaged in asymmetrical (i.e., uneven in terms of military capability) war, digital logistics became the hub for C2 operations and a domain for information warfare. Nissen (2015, p. 72) proposed six ways that social media could be used to support military C2 operations: intelligence collection, targeting, cyber operations, defence, C2, and influencing information through psychological warfare operations (PSYOP)\(^\text{17}\). Thus, terror organisations have weaponised social media platforms and other digital information environments to achieve their political ends. ISIS aims to generate a global effect by spreading messages of fear to increase sympathy, recruitments and, media coverage. The network form of ISIS emerged as it exploited multiple digital media logistics, including media production tools and software logistics. Therefore, digital media logistics have played a pivotal role that shaped the generation and dissemination of terror around the globe. As Nissen (2015) argued:

> The weaponisation of social media translates into “military” activities such as targeting, intelligence, psychological warfare, cyber-operations (offensive and defensive), and command and control in support of the achievement of political or military effects created in and through social network media. (p. 81)

In his 1838 text, *The Art of War*, the French military strategist Antoine-Henri de Jomini (as cited in Neilson, 2012) argued that, “logistics is not merely a ‘science of details’ but a ‘general science’ that plays a leading role in the organisation of war and the execution of strategy and tactics” (p. 5). Neilson (2012) agreed with this assumption, considering the

\(^{17}\) This thesis only examined PSYOPS carried out by ISIS in online media platforms, not on the physical ground and its effects of gain of territories. The discussion of the impact of PSYOPS on the physical environments is beyond the scope of this thesis.
developments of warfare and the civilian logistics revolution. He argued that, “strategic decisions are limited by the resources at hand and tactical manoeuvres unfold within a situation defined by lines of information and supply” (Neilson, 2012, p. 5). The aim of adapting information logistics is to gain advantage over adversary. For example, ISIS adapted encrypted communication channels to secure information and anonymity of users. The utilisation of anonymous sharing portals has helped ISIS to launch a tactical, manoeuvring warfare to evade degrading operations and sustain information flows.

When discussing the information logistics of terror networks, it is important to note that information has been a strategic weapon of non-state actors, who fight physical wars with the most advanced militaries in the world. The use of information logistics during wartime will advance the organisations cyber-warfare capabilities. As Saad, Bazan and Varin (2011) stated, “Cyber-warfare is hence an asymmetric warfare that requires non-conventional means of action. An asymmetric war is a conflict opposing two unbalanced forces, most of the time a State against a non-State actor” (p. 3). When fighting an unbalanced war, information has always been a strategic tool to network, spread, and produce propaganda and disinformation. Internet based tools have expanded these strategies, as Saad et al. (2011) further argued:

In this context, non-conventional methods are used, and Web-related actions are progressively considered as part of that a generation of weaponry. The Web is a virtual territory, a virtual target. But it is also a direct tool of aggression, in terms of strategic content production and disinformation. (p. 3)

To understand the sophistication of message assemblages in the information age, and the objectives of IO, and the planning of ISIS flows of information that have emerged, it is important to explore the logistical processes of ISIS. That said, digital media logistics played
a key role in creating an association between the ISIS capital in Iraq and ISIS sympathisers and affiliates around the world. Further, it changed the dynamics of communication (see sections 4.8, 6.5 and 6.13). This change includes the settings and mechanisms of communication tools (e.g., coded formatting, encryption, machine disseminations) and the use of these communications as C2 operation centres. That is, harnessing and exploiting digital information environments enabled ISIS to communicate directly with sympathisers and affiliates around the world (e.g., sending encrypted one-to-one and one-to-many messages, and sharing manuals and instructions via Dropbox, Google Drive, JustPaste.it and SHAREit). As a result, thousands of foreign-fighter recruits have pledged allegiance to the caliphate, and many more acted on behalf of ISIS to destabilise the West by unprecedented terror attacks (Cohen 2015; Archetti, 2015).

Since ISIS managed to spread their propaganda online and capturing news headlines, the US and its allies determined at an urgent meeting in 2014, in Hanover, Germany, that ISIS’ message must be stopped, and its digital infrastructure rooted out. However, the countering of ISIS’ propaganda on popular social media platforms only encouraged ISIS to seek other anonymous digital platforms, such as JustPaste.it, Sendvid, Kik, Pinterest, dump.to, SHAREit and archive.org. More recently, ISIS established channels on Telegram and Tumblr networks, which were extensively utilised by ISIS affiliates and members.

**Research Questions**

This study examines the role of digital media logistics in ISIS IO, strategic narrative and propaganda from a network warfare perspective. The primary question of inquiry, and the two secondary research questions, are:
1. What was the role of ISIS’ digital media logistics in resisting attempts to degrade its IO objectives between 2014-2016?

2. Were the three phases of the countering operation (disruption of information flows, countering narratives and open hacking) successful in their attempts to degrade ISIS IO objectives between 2014-2016?

3. Did ISIS’ three communication strategies of weaponisation of information environments, stigmergy, and manoeuvring operations enable it to counter attempts to degrade its propaganda and recruitment networks?

Theoretical Base

The main argument in this thesis is that a paradigm shift in terror communication has emerged, involving: weaponisation of digital media environments, stigmergic swarming operations, and a strategy of manoeuvre within information warfare operations. Arguably, this shift has helped ISIS to carry out and achieve its IO objectives in the period between 2014-2016.

To understand how ISIS managed to survive account suspension on popular social media platforms and maintain success in information warfare, tracing of the information logistics of its networks is necessary, as suggested by Actor-Network Theory (ANT). ANT is important to the understanding of information logistics. The framework of ANT clarifies how information is distributed, perceived, and acted upon from interacting agents to achieve their goals. In other words, information can be translated into indirect forms (e.g., information sign) or pheromone trails that can be used by other network actors to act upon. Callon (1986), Latour (1996), and Law (1992) argued that ANT attempts impartiality between all actors—human and non-human—and makes no distinction in approach between the social, natural,
and technological. Using the ANT approach, all the factors (both human and non-human) that influence the adaption of multiple information environments are defined as actors.

The framework of ANT can explain how ISIS established and connected to networks outside its territories, as Law (1986) proposed in his long-distance control essay. It also explains how networks are developed and maintained by interactions of human and non-human actors (e.g., WhatsApp and Telegram channels). Law (1986) argued:

> The envelope of mobility and durability in the face of a range of environments was extended by a combination of technological artefact and human resources. That long-distance social control depended upon creating a structure of elements, both human and natural, capable of generating an envelope of durable mobility for vessels. (Law, 1986, p. 10)

The value of using ANT to understand the network logistics of ISIS is twofold. First, ANT is a first step to understanding how networks emerged and maintained themselves through processes of translation and enrolment (see section 4.12). Second, tracing the logistics of terror networks (as proposed by ANT) provides necessary insights into message assemblages and other digital toolkits used by ISIS, which will be essential in strategic operations to counter and thwart terror networks. Further, tracing network actants (and ISIS’ information logistics) as network actors can highlight the communication patterns of ISIS networks.

Tracing information logistics as network actors, leads to an exploration of processes, information flows, and coordination between human actors in the network. Therefore, to understand the processes of information logistics and trace of information flows; ISIS media productions produced by media outlets such as Al-Hayat media, Al-Forgan and Anjad media outlets were traced in chapter 4. These media outlets were responsible of ISIS’ information operations that include producing of propaganda videos, magazines, pamphlets, and radio broadcast.
Also, using screenshot methodology is another way to trace information flows of ISIS networks. Screenshots were obtained from primary resources of ISIS communication channels such as Telegram application, Justpate, sendvid and dump.to, that lead to understand the pattern of ISIS’ communication across its networks. Furthermore, to understand how ISIS maintained its network structure and established affiliated networks outside its regional territory, in chapters 6 and 7, tracing of microblogging platforms, encrypted applications and anonymous sharing portals were necessary. Another way ANT helps to understand network actors and trace of ISIS communication has been highlighted in chapter 5 through the tracing of specific hashtags ISIS widely celebrated across the Twitter sphere.

Therefore, ANT can be more: technically described as a material-semiotic method, mapping relations that are:

simultaneously material (between things) and semiotic (between concepts). Everything in the social and natural worlds does not exist separately but is being constantly generated by relationships between actors in networks. (Law, 2007 cited in O’Connell, Ciccotosto, & De Lange, 2014)

To understand how these networks are built, it is important that no assumptions are made by the researcher regarding the positions or beliefs of the actors within the network, including how the actor defines and associates with other actors (Callon, 1986; Latour, 1987, 2005).

The logistics approach in this thesis acknowledges that logistics forge the network’s existence.\footnote{That is, anonymous digital networks helped in creating new terror networks and established channels of information dissemination.}
The weaponisation processes of anonymous sharing portals can be understood through the agency of network actants. The concept of actants in a network stresses the interaction between material and human factors in any process (Latour 2009). An actant can be a human, laptop, or computer software. These actants establish the Actor Networks. Using ANT in the context of ISIS media logistics is important as it leads to the understanding of the network structure and know the tools of its information operations and propaganda strategy to establish the best practises for counter-narrative strategies. Tracing of network actants can also uncover media operations and communication strategies, used by ISIS, to maintain its network structure and information flows. The utilisation of ANT increased my knowledge on the methods used by ISIS to encrypt communication platforms and anonymous sharing portals. These portals and platforms played a pivotal role in establishing the global terror network that spread fear into many parts of the world.

To better understand ISIS’ IO objectives, strategic narrative and propaganda, it is important to trace the network actants. Creating and disseminating compelling messages requires a large amount of resources—both human and non-human actants. These resources have helped ISIS to establish their actor networks. The human actants presented in this thesis are ISIS jihadists, affiliates, and sympathisers who played a role in sustaining flows of information. The non-human actants can be the following: digital media logistics (i.e. software, platforms and applications), technical tools (i.e. computers, cameras, mobile phones), and other necessary internet logistics materials such as routers, sockets modems and cables.
ANT (Callon, 1986; Latour, 1996; Law, 1992) attempts to understand the role of all network actors—whether human or non-human—and makes no distinction between the social and the technological. As such, ANT is key to understanding the logistics of ISIS’ networks. Thus, as Krieger and Belliger (2014) note, understanding networking means “understanding those normative principles that guide those particular communicative activities that build, maintain, and transform networks. This is where new media studies come in” (p. 9). I believe that the conceptual toolkit of ANT offers an important perspective in understanding the communication strategies of ISIS’ affiliated networks. It also helps to understand how the networks emerge, are leveraged, and maintain themselves through processes of translation and enrolment. As Krieger and Belliger (2014) argued “actor networks are much more like processes, performances, socio-technical rituals, and enactments […] They are driven by the dynamics of making connections, of binding things together, of extending associations, of “translating” and “enrolling” actors into networks”. That is, ANT focuses on how connections are established between network actors. ANT argues that as long as the network actants keep interacting with each other, the actant network will look stable, and when the interaction ends, the actor network will breakdown. In other words, the relations between human actors and non-human actors establish networks as long as these network actors are connected to each other. Therefore, to maintain a connection between network actants to sustain flows of information, ISIS managed to translate and enrol many network actors. This includes encrypted communication channels, anonymous portals, and all other digital media networks. Stern and Modi (2010) argued, terrorists’ manoeuvre in different environments that shape their mission, therefore information logistics are important to sustain the messages of terror (p. 282).
From an ANT perspective, the associations between hardware and software logistics produce actants (Latour, 2005, p. 54). These actants have agency, “which means that they make a difference: hitting a nail with and without a hammer, boiling water with and without a kettle, fetching provisions with or without a basket” (Latour, 2005, p. 71). The same could be said for digital media tools, mobile phone applications, malware, military clothing, and guns. To apply this to ISIS’ terrorism, an individual jihadist—who has access to digital technologies, weaponry, and video production equipment—may commit an act of terror. “Action is therefore not the property of humans only but of associations of actants” (Latour, as cited in Archetti, 2012, p. 10).

In this thesis, the logistics analysis approach is used to understand how the network is brought into existence, understanding network assemblages and information logistics, which are “the planning of information flows” (Sandkuhl, 2007, p. 47). As Krieger and Belliger (2014) suggested, “flow opens up black boxes and transforms purely functional intermediaries into actors, participants, and mediators. When interactions among large numbers of actors become the rule and knowledge reconfigures itself into a cloud” (p. 144).

Utilising multiple digital communication platforms has allowed ISIS to leverage their networks and enlist new actants, which assisted in the emergence of new networks (see chapter 6). Efforts to degrade ISIS’ digital logistics, control its flows of information, and disrupt its channels of communication on popular SMNs has been challenged by the emergence of anonymous digital platforms, sophistication of message assemble, and speed of

---

19 That is, anonymous digital networks helped in creating new terror networks and established channels of information dissemination which is part of their IO strategy.
20 The ‘black box’ is an ANT term which will be discussed in detail in chapter 6.
dissemination. Anonymous sharing platforms immediately stand out, because they act as accelerators of information flows, while making it harder to trace the logistics of how these flows are performed.

From a swarming perspective, ISIS’ speed of command in harness of microblogging platforms and other encrypted applications, has the preference to maintain its flows of information. Tracing of ISIS’ digital logistics can explain how swarming activity occurred and how the interaction between ISIS Jihadists and the digital media platforms has shaped the organisational form of ISIS networks that enabled it to carry out IO and engage in Network-Centric Warfare (NCW).

The utilisation of new digital information environments in the context of OODA loop can generate an NCW effect. This effect can be examined through observation of ISIS and its opponents’ OODA loops. Tracing of ISIS’ online activity can explain how swarming activity occurred and how the interaction between Jihadists and the online environments has shaped the organisational form of ISIS networks.

From the lenses of ANT, swarming activity of ISIS has changed the agency of the online environment. In other words, Justpaste.it, Telegram and Sendvid were created to share videos and files, the extensive use of these portals by ISIS have changed its agency and became hubs and tools that helped ISIS’ propaganda to flourish.

As a result, attacking ISIS’ digital logistics on social media platforms, with the purpose of degrading its online performance to control the terror narrative, has been ineffective.

**Rationale**
Fighting terrorism in the digital sphere is not a new phenomenon. However, based on the issues briefly listed above, this thesis identifies three main challenges involved in countering the ISIS narrative:

- The sophistication of message assemblages (e.g., high definition [HD] productions, editing, screening and casting).
- The processes of dissemination and redistribution (e.g., automation and speed in redistribution processes).
- The proliferation of anonymous sharing portals and the capacity for information sharing to be powered by the internet.

David Kilcullen (as cited in Kalb & Saivetz, 2007) noted, “if bin Laden didn’t have access to global media, satellite communications and the Internet, he’d just be a cranky guy in a cave” (p. 7). That is, the internet facilitates both terror communication and the pervasiveness of terror narrative; the weaponisation of information environments promotes terror narratives by using marketing strategies, permitting the promotion of its brand to a potential global audience.

The internet and terrorism are both very fast-changing phenomena. Information logistics (e.g., hardware and software) enabled ISIS to produce over 38 items of visual propaganda every day in 2015 (Winter, 2015b), and thousands of other digital artefacts, which were posted to Twitter (see section 4.11) and Telegram (see section 6.18). Files and other photo documents were shared via JustPaste.it and dump.to (see sections 6.6.1 and 6.6.3), Russia Mail and SHAREit. The massive social and technical assemblage that involves technologies, people, networks, geographies, and technical materials enabled ISIS to produce the huge number of visual propaganda and messages every day.
The main challenge facing the US, and ISIS’ other adversaries, is how to counter ISIS’ strategic narrative and disrupt its information loop. To achieve this end, in chapter 5, this study argues that there have been three distinct strategic phases concerning the countering of ISIS’ online messages and attacking its digital logistics.

In phase one (see section 5.3), this thesis discusses the main challenge of disrupting ISIS’ information loop, which was a degrading and destroying mission. Part of degrading the mission that was discussed was the role played by Twitter and Google to delete ISIS’ active accounts on their platforms. This measure resulted in deleting hundreds of thousands of accounts and messages, which also led to ‘influence warfare’ (Forest, 2009) between ISIS’ affiliates and opponents (see section 5.4).

Phase two involved countering ISIS’ propaganda (see section 5.6). To compete with ISIS’ propaganda, in 2014 the US government expanded the Centre for Strategic Counterterrorism Communications (CSCC), which was established in 2011, to counter Al-Qaeda’s communication activities (Higham, 2015). The CSCC released its first video production, *Welcome to ISIS Land* in 2014. According to Scott Higham (2015), “The video became a viral phenomenon—viewed more than 844,000 times on YouTube—and a cause of significant irritation to its target”. The CSCC also launched the ‘Think Again Turn Away’ platform on Twitter to stop foreign fighters joining ISIS and documenting atrocities committed by ISIS jihadi. However, in return, ISIS launched the ‘Run Do Not Walk to U.S. Terrorist State’ platform on Twitter to recruit potential members from the West (Higham, 2015).
Phase three involved hacking activities carried out by hacktivists groups such as (anonymous and CtrlSec). Although disrupting ISIS’ information loops, discussed in phase one and phase two are part of information warfare, in this phase, this thesis focuses on the role of hacktivist groups who declared #Operation-ISIS and #OpIceISIS. According to Griffin (2015), these operations “ha[ve] largely focused on finding and shutting down social media accounts and websites of ISIS”, using denial-of-service (DoS) attacks and reporting ISIS accounts to Twitter. The hacking activity has paralysed hundreds of channels of information dissemination such as ‘The Dawn of Glad Tidings’ (#op_ISIS, 2015). According to Berger and Morgan (2015), the ‘Dawn of Glad Tidings’ application was “an official ISIS product promoted by its top users, [and was] advertised as a way to keep up on the latest news about the jihadi group”.

The sophistication of ISIS’ swarmcast\footnote{The use of multiple information environments from all directions to generate and disseminate messages.} operations, which started in 2014, demanded that the world adopt a holistic approach to counter the new terror threat it represented. Tracing ISIS’ digital activity from one domain to another, is beyond the capacity of states and intelligence services. That’s because of the complexity of ISIS’ IO, the scale of its operations, and anonymity of its users. Meanwhile, ISIS sympathisers and affiliates tried to protect their digital legacy (e.g. circulation of propaganda videos and statements of its charismatic leaders) and channels of dissemination. As a result, information warfare occurred between ISIS and its adversaries. This cyberwar was not limited to social media platforms, but reached to other information environments, including Sendvid, JustPaste.it, Woodvid, Telegram, and archive.org. In addition, web site creators and administrators have recently designed artificial intelligence (AI), to locate information that is uploaded by ISIS affiliates before it reaches a
wider audience. AI and people’s intelligence formed an alliance to counter ISIS’ narrative and paralyse its IO across various information environments. However, to maintain networking structures and the flow of information, ISIS mobilised hackers, disseminators, information aggregators, and propagandists. For example, the United Cyber Caliphate (UCC) are hackers who have waged information warfare against ISIS’ adversaries and have often managed to disrupt their information flows (see section 6.18.2).

To summarise, this thesis argues that between 2014 and 2016, ISIS managed to survive attacks that targeted their digital infrastructure and other attempts to disrupt their IO. The ISIS paradigm shift included the weaponisation of IO objectives, the use of stigmergic swarming strategies, and advanced manoeuvring within digital media environments, which included the rapid production of HD propaganda videos, which have helped ISIS to maintain its networking structure and secure flows of information. That is, ISIS managed to maintain an information feedback loop by translating and enrolling multiple information environments, including social media platforms, anonymous sharing portals, and encrypted communication channels.

**Study Approaches**

To understand the role of information in promoting a terror narrative and the creation of distributed decentralised networks, this thesis sets out to understand issues highlighted in the rational section that were:

1) The capacity and objectives of information uploaded by ISIS.

---

22 In early 2018, Facebook adapted AI technologies to trace ISIS propaganda videos. However, AI hasn’t been discussed as it is beyond the scope of this thesis.
How ISIS managed to manoeuvre across digital media platforms and maintain its networking structure in the period between 2014 and 2016.

These issues are approached from two perspectives. The first approach involves dealing with information as a paradigm; this aims to understand the purpose and process of message assemblages. The second approach aims to understand digital information warfare and how ISIS managed to survive degrading operations against it by adapting their warfare strategies based on the OODA loop model.

To understand the paradigm shift that appeared after the rise of ISIS, and how ISIS managed to leverage its networks by creating networks of affiliates around the world, Raber’s (2003) three-paradigm approach to information is used to explain this phenomenon. These three paradigms are: physical paradigm, cognitive paradigm, and social informatics. This approach provides insight into how information is transmitted and retrieved across information environments, the volume of information disseminated, the dynamics of video productions, the processes of recruitment and radicalisation, the internal and external communication between ISIS members and affiliates, and how the audience perceive and interpret information.

The second approach involves taking on board the concepts developed in information-centric warfare, the OODA loop warfare model. This approach is important as this thesis demonstrates that ISIS adversaries launched information warfare strategy to tackle the rise of ISIS on digital information environments. The OODA loop is a theory of manoeuvre warfare,
developed by Colonel John Boyd in 1974. Safranski (2008) recognised three significant Boydian ideas that apply to network-centric warfare (NCW):

- The idea of manoeuvre warfare.
- Swarming operations, dependent on units acting in synchronicity—which Boyd referred to as *auftragstaktik*—from a decentralised C2.
- Information superiority as a decisive advantage in completing OODA loop cycle accurately and rapidly.

These operations depend on complex information systems. The OODA loop model provides an understanding of how ISIS deepened on the roots of its network structure across digital communication platforms and how information-centric warfare was performed. The OODA loop identifies the dynamics of how information-centric warfare arose in the networked digital media environments. It also allows a way of thinking about warfare, model of conflict, and a theory of manoeuvre warfare strategy. The outcome of this approach is that “the side that can make the quickest decisions is most likely to win” (Osinga, 2005).

**Aims and Scope of the Study**

The emergence of ISIS, within the political struggle in Iraq and Syria, added a new complexity to the socio-technical debate on the use of digital technologies by terror organisations (Nacos, 2016; Stohl, 2006). This study aims to map, analyse, and provide an

---

23 Boyd did not publish his work but preferred to present his theory through many hours, long slide lectures. His work has been interpreted by several military theorists, such as Osinga (2005) and Safranski (2008).
understanding of the logistics of ISIS’ digital media networks, which have been employed strategically to achieve ISIS’ political objectives. This study analysed the role of digital media and communication channels, prior to the emergence of ISIS. Chapter 1 provides an outline of terror organisations, such as Hezbollah, Hamas and Al-Qaeda, and how these organisations operated in the Middle East through mass media channels and web technologies. Chapter 2 reviews the significance of the emergence of web 2.0 on the Arab Spring uprisings until the rise of ISIS. This chapter argues that SMNs aided in the establishment of political and ideological polarisation, which penetrated social fabric and inspired political mobilisation. Chapter 3 aims to understand strategic narrative and propaganda produced by ISIS. This chapter contains an in-depth analysis of the media strategy of ISIS, used to achieve its political objectives in establishing a global caliphate. Chapter 4 aims to understand the construction processes of terror messages, including its assemblages and flows of information across digital networks. This chapter will analyse the dynamics and function of the tools that helped the generation and dissemination of these messages from the ANT perspective. Chapter 5 provides insights into the operation for degrading ISIS’ digital media logistics. This chapter aims to answer this thesis’s secondary question: how has the suspension of Twitter and YouTube accounts impacted on ISIS’ networking performance? In this chapter, I identify the phases of the degradation operation: degrading and destroying, countering ISIS’ propaganda, and hacking and information warfare. Chapter 6 is divided into two case studies that explores the new digital media logistics that ISIS adapted in the aftermath of the degrading operation. Case study 1 (see section 6.2)\textsuperscript{24}, highlighted the role of Anonymous sharing portals in sustaining the

\textsuperscript{24} An early version of this case study was published as journal article on perspectives on Terrorism. Cited As: Shehabat, A., & Mitew, T. (2018). Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. \textit{Terrorism Research Initiative}, 12(1).
information loop of ISIS. Case study 2 (see section 6.3)\textsuperscript{25} demonstrates how the use of the Telegram helped ISIS maintain its network structure. Chapter 7 aims to identify the tactics of digital manoeuvre warfare established by ISIS to survive the degrading operation initiated by its adversaries. In this chapter, I emphasise that the IO of terror organisations is not limited to a certain application of networking and communication channel. Rather, the emergence of anonymous digital environments (e.g., JustPaste.it and Sendvid) and encryption communication applications (e.g., Telegram and WhatsApp) have enabled ISIS’ IO and helped ISIS to maintain its networking structure.\textsuperscript{26}

While many scholars, journalists, and academics have addressed the processes of radicalisation, recruitment, and fundraising as the ultimate purpose for ISIS’ use of SMNs (Bermingham, Conway, McInerney, O’Hare & Smeaton, 2009; Gerdes, 2011; Neumann, 2010), this thesis examines the perspective that SMNs, anonymous sharing portals, and encrypted communication channels, played a pivotal role at the strategic management of ISIS’ media logistics. Tactically, ISIS was able to maintain information flows, distribute a pervasive terror narrative, enlist actors, and secure communication channels. Strategically, ISIS was able to craft a consistent narrative and execute its psychological operations and propaganda at a global scale. The ultimate goal of this was, and still is, to establish a global

\textsuperscript{25}An early version of this case study was published as journal article on the journal of strategic security. Cited as: Shehabat, A., Mitew, T., & Alzoubi, Y. (2017). Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West. \textit{Journal of strategic security, 10}(3), 3.

\textsuperscript{26}An early version of this case study was published as journal article on the media and information warfare. Cited as: Shehabat, A., & Mitew, T. (2017). Distributed Swarming and Stigmergic Effects on ISIS Networks: OODA Loop Model. \textit{Journal of media and information Warfare, 10}(x), 79-109.
caliphate. Recruitment and radicalisation is one part of the process to achieve this objective. Regarding the process of radicalisation and recruitment, ISIS’ IO objectives were designed to achieve short-term and long-term strategies to recruit and radicalise individuals. These strategies can be achieved by disseminating both grievances and utopian messages.

The primary aim of this thesis is to highlight new perspectives on the types of digital media logistics used by ISIS in its IO. To that effect, this thesis examines the weaponisation of digital media platforms and the use of sophisticated media production (see section 4.3). This thesis also examines the effectiveness of the counter-ISIS degrading operation from an information warfare perspective. These perspectives have not yet been used in the literature to examine and understand the first three years of media information warfare against ISIS. Therefore, this thesis makes an important contribution to the literature.

The scope of this research, however, is focused on ISIS’ online IO part of the information warfare it waged to maintain its networking structure in the period between 2014 and 2016. Meanwhile, the relationship between real-world networks and their online manifestation is beyond the scope of this thesis. However, I have added a timeline of ISIS’ on-ground operations that highlighted main ups and downs of ISIS during real-world operations (see pages xvii-xviii).

To this end, the time frame studied is concerned with the rise of ISIS as a caliphate. Before the year 2013, journalists and scholars speculated about the existence of a digital caliphate (Atwan, 2015). Ironically, after the Iraqi and Syrian governments declared victory against ISIS in November 2017, a caliphate digital activity was reinstated in the digital information environments.
Methodology

The research objective of this thesis is to understand, through an information warfare perspective, how the emergence of anonymous digital platforms and other digital logistics contributed to ISIS’ networks. It seeks to interrogate how ISIS networks engaged these media logistics to support its resistance of the attempts to degrade its IO objectives and operations between 2014 and 2016.

The study of terrorism and the internet is a multidisciplinary topic, which incorporates media, terrorism, military, internet, and political science studies. To better understand the relationship between terrorism and the internet, several methodological approaches are required, including big data analysis, social network analysis, digital ethnography approaches, and text and visual analysis. However, to investigate the complexity of the use of digital media logistics that helped in the formation of ISIS’ IO strategy, strategic narrative, and propaganda, I have employed a mixed digital methods approach that involves the ANT directed, small-scale visual and textual analysis coupled with platform analysis.

With regard to the visual analysis, it is important to acknowledge three facts regarding ISIS’ material, which are coherent elements of its digital media logistics and resistance of attempts to degrade its IO objectives. First, ISIS has created a sophisticated, new jihad social media ecology compared to other terror organisations in the region. Second, ISIS has produced a huge amount of HD media—both videos and images. Third, ISIS has rapidly responded to degradation operations by creating information signs and traces for its affiliates to follow. In other words, ISIS managed to maintain its networking structure and flows of information by reprocessing its digital legacy and disseminating it via anonymous sharing portals and
encrypted communication channels, sophistication of message assemblages and processes, and speed of dissemination. The visual analysis in this thesis (see section 4.14) includes the most circulated propaganda videos, which were intended to be most effective in representing ISIS’ ideology.

As this research aims to understand how ISIS’ digital media logistics IO were used to achieve a political end, it is essential to trace the digital activity of ISIS over multiple information environments to comprehensively understand ISIS’ propaganda strategies and IO.

Chapter 4 examines ISIS’ Romeyah English magazine to capture the trends and themes of ISIS’ IO strategy, in which non-Arabic speakers were targeted. To do this, I selected seven editions of Romeyah English magazines, downloaded from two primary sources: archive.org and Nashir Political Services ISIS Telegram channel. I used the NVivo software analytic tool to capture the trends and themes of ISIS’ strategic narrative. My findings are presented as a screenshot.

Tracing the network associations and online activity of ISIS, via the work of Latour and ANT, requires a mixed digital methods approach. As Marres (as cited in Kanngieser, Neilson & Rossiter, 2014) argued, “This approach develops ‘natively digital’ research tools that take advantage of the analytic and empirical capacities that are embedded in online media”.

Within the framework of ANT, this research traced the online activity of ISIS on popular and anonymous digital platforms. By tracing ISIS’ activity, particularly on anonymous digital networks (e.g., dump.to, Sendvid and JustPaste.it), their logistical associations with other digital networks (such as Twitter) can be discerned. Ultimately, this will provide insights into how these networks operate and perform. Moreover, tracing digital activity using a mixed
digital method will also unveil the associations and interactions with these networks through the lenses of number of views, shares, and comments. This is helpful in capturing the trends and trajectory of ISIS’ terror narrative. As this research involves tracing the online activity of ISIS, mixed digital research methods will be used, including platform analysis, data visualisation, and screenshots.

**Platform Analysis**

Joss Hands (2013) defined ‘platforms’ as:

> A software framework running on the World Wide Web or Internet, in the form of social media interfaces, apps, or most commonly ‘Web 2.0’ portals that gather users in interfaces with each other and with the Web and the Internet itself. (p. 3)

The structure of platforms—operated by systems, devices, and objects (human or non-human)—and the operation of platforms is a result of convergence between its elements of structure. As digital platforms are designed to generate and aggregate content, information dissemination and communication, platform analysis will identify associations between content generators and the platform itself. This thesis highlights the importance of the platform analysis approach in charting the qualitative information on anonymous digital platforms (e.g., JustPaste.it, Sendvid and dump.to), encrypted communication channels (e.g., Telegram) and Twitter. Platform analysis provides insight into the socio-political change

---

27 Platforms are part of digital media environments discussed in this thesis. However, platforms are different from portals in a way that platforms offer users tools that enable them to build their groups and networks within the setting of the platform. Therefore, in this thesis, Facebook and Twitter were treated as platforms while Justpaste and Sendvid are treated as portals.
created by the multiple uses of different digital environments to disseminate a pervasive terror narrative. With the concentration of attention on these elements, the aim is to learn how digital media networks contribute to the discourse of terror networks.

**Screenshots**

I am using screenshots to illustrate my key points within the thesis. I have provided screenshots that are evidence to ISIS’ IO on the information domains. In this thesis, the screenshot methodology approach is twofold. First, I have captured screenshots that were widely celebrated and circulated by ISIS members and sympathisers through Telegram, and other microblogging sites used by ISIS, to capture the evidence of propaganda and media narrative of ISIS networks used as part of network communication. Moore (2014) suggested that “As media objects they can be dynamically traced across the networks of their dissemination and require a re-evaluation of the axioms of cultural production that considers texts independently of experience”. Second, screenshots obtained from Twitter and video productions are used to interpret the thematic analysis of media narrative of ISIS networks. Siegler (2015) considered screenshots as a powerful way to manoeuvre around Twitter’s 140-character limit. He suggested that, “people figured out that you could take a screenshot of any text on the web and share that as the image payload of a tweet”. These shared screenshots can be gathered, mapped and interpreted which help to understand the communication pattern of ISIS networks.

According to Moore (2014), screenshots “play important and unacknowledged roles in the method of mapping, graphing and visualising as well as the general communication of research” (p. 142). In my research, this analysis sought to answer some important ontological and epistemological questions: what do these data represent and what claims can be made
from them? Moore (2014) highlighted the importance of screenshots in making sense of data visualisation. Moore (2014) noted:

> Screenshots are an excellent example: as digital tools, they diminish permanence in exchange for malleability and performativity. As media objects they can be dynamically traced across the networks of their dissemination and require a re-evaluation of the axioms of cultural production that considers texts independently of experience. (p. 142)

Screenshots played a critical role in ISIS’ IO and is considered an important element of ISIS’ logistics. For instance, it is used as a recruitment tool of foreign fighters, catalyst of lone-wolfs, and carryout media propaganda operations. Within this context, screenshots are together with videos and other media, considered as important actants in the ISIS actor-network, which ANT allows me to follow, trace, capture, and analyse.

Capturing of circulated screenshots was an important element of media propaganda used by ISIS to leverage its networks. Also, capturing screenshots from ISIS propaganda videos is crucial and tangible evidence of horror genre produced by ISIS.
1 Chapter 1: Terror Organisations and Web Technology in the Arab World in the 21st Century

1.1 Introduction

The objective of this chapter is to understand the influence of digital media logistics such as ICTs and SMNs and how it became an integral part of influence warfare during wartime in some parts of the Arab world. In this chapter, I examine how the evolution of internet technologies and independent satellite channels have shaped a new wave of terrorism that has erupted across the MENA region and extended beyond the borders of the Arab world.

This chapter aims to expand on and explain the paradigm shift in terror communication established before the emergence of ISIS. It also pictured how digital media logistics are used as weapons by guerrillas as instruments of information warfare. Therefore, this chapter explores two main ideas.

First, this chapter outlines how previous terror organisations, such as Al-Qaeda, Hezbollah and Hamas, operated in the Middle East—and were dependent on mass media channels and web technologies for communication purposes—prior to the emergence of ISIS. Second, this study explores how information environments enabled terror organisations to flourish; these environments were useful information sources, which informed warfare and military confrontations. This chapter will examine three case studies on the most notorious terror organisations (i.e., Al-Qaeda, Hezbollah and Hamas) in the Middle East, prior to ISIS. This

---

28 Influence warfare is part of information operation that includes the dissemination of propaganda in pursuit of a competitive advantage over an opponent. The use of this term in this thesis was suggested by James Forest during an early review version of this thesis who suggested that influence warfare may appear better term than information warfare/cyber warfare.
chapter argues that ICTs and SMNs have played a key role in the existence, maintenance of flows of information, and leverage of terror networks. This chapter is divided into three parts. First, I discuss the historical roots of terror networks in the Middle East and Iraq. Second, I examine how the exploitation of ICTs aided Al-Qaeda’s operations and affected world security. Third, I explore how Hezbollah and Hamas weaponised SMNs and websites for C2 operations.

1.2 The Emergence of Jihadi Movements—A Historical Perspective

The Arab world suffered a severe setback after the establishment of the State of Israel in 1948. Egypt, Syria, and Jordan lost a six-day war against Israel in 1967 that resulted in Israel occupying the West Bank of Jordan, the Golan Heights of Syria, and Sinai of Egypt. To retaliate and seize their occupied territories, Syria and Egypt attacked Israel in 1973, but could not achieve military victory as US troops intervened and protected Israel. In 1978, the US offered Egypt a peace agreement with Israel in Camp David (i.e., the Camp David Accords). Part of the agreement stated that Sinai and other occupied Egyptian lands would be returned to Egypt.

However, the Camp David Accords had consequences for the relationship between Arab nations and Palestinians. Palestine felt betrayed by Arab nations who favoured peace with Israel, over achieving a successful military operation to liberate Palestine. Since then, jihadi and secular Palestinian movements emerged to take up arms against Israel. The Palestinian Liberation Organisation (PLO), Islamic Jihad, Al-Aqsa Martyrs’ Brigades and Hamas have attacked Israel with suicide bombings, abductions and shootings. The outcome of the Camp David peace treaty with Israel created an internal conflict in Egyptian society and the broader Arab world. Egyptian Salafi extremists known as Al-Gama’a Al-Islamiya started to attack
government interests, target foreign tourists, and assassinate police and military personnel. Zanini (1999) argued that “the Al-Gama’a Al-Islamiya [wa]s the most active Islamic extremist group in Egypt. In November 1997 Al-Gama’a Al-Islamiya carried out an attack on Hatshepsut’s Temple in Luxor, killing 58 tourists and 4 Egyptians” (p. 249). This jihadi movement caused significant economic and political damages; Egyptian Salafists paralysed Egypt’s tourism industry and then succeeded in the assassination of President Anwar Sadat in 1980.

1.3 The Rise of Hamas

In 1982, Israel attacked Lebanon to secure its northern border from daily skirmishes with PLO guerrillas, under the leadership of Yasser Arafat. A few years later Hezbollah (The Party of God)\textsuperscript{29}, under the leadership of Sheikh Sobhi Toufaily, was stationed in southern Lebanon after the Lebanese government managed to send Yasser Arafat and his PLO leaders to Tunisia. Hezbollah officially formed in 1985 after the Amal Movement became secular. As Schleifer (2006, p. 4) noted, Hezbollah found in Lebanon fertile ground for their activities, particularly after Israel started to attack the PLO. Since its emergence in 1985, Hezbollah has fought the Israeli army over its occupation. Hezbollah’s operations against Israel resulted in withdrawal of the Israeli army from southern Lebanon in 2000. With daily border skirmishes, Israel launched two massive military operations in 1996 and 2006 against Hezbollah; however, Israel failed to end Hezbollah’s hostility. On the Palestinian front, the conflict between PLO (rebranded as Fateh) and Hamas eased the attacks on Israel; the internal armed conflict divided the Palestinians into two groups: Islamists and secular individuals.

\textsuperscript{29}A Lebanese political organisation that emerged from Muslim Shi’a fundamentalism, which became part of a growing worldwide Shi’a alliance under Iran’s ideological, financial, and military authority.
In 2006, Hamas won the national Palestinian elections, but the US and Israel criticised this victory as Hamas explicitly denied the existence of Israel. According to Wilson (2006), “The election results stunned U.S. and Israeli officials, who have repeatedly stated that they would not work with a Palestinian Authority that included Hamas, which both countries and the European Union have designated as a terrorist organisation”. Hamas argue that Israel is a land occupier. As such, Hamas “favours the creation of a Palestinian nation on land that now includes Israel rather than the road map’s two-state solution” (Wilson, 2006). However, the US, European Union, Palestinian National Authority and Israel refuse to acknowledge Hamas as an equal partner in the negotiations with Israel, as Hamas is understood to be “a terrorist organisation that refuses to recognise Israel or renounce violence” (Tran, 2007). The rejection of the 2006 democratic elections led to Hamas’s decision to seize control of the Gaza Strip. Hamas managed to disarm the Fateh movement in Gaza Strip and declare Gaza as independent from Palestinian Authority. As Zeitoff (2011) asserted, “Hamas, and hence Gaza, was isolated internationally as it refused to recognize Israel as a state, renounce violence, and follow previous Palestinian Authority agreements reached with Israel” (p. 941).

While Hamas was in control of Gaza under Islamist rule, Israel imposed a blockade on Gaza from land and sea and continued to assassinate Hamas’s top leaders. Consequently, Hamas continued its rocket attacks against Israeli targets. Three major confrontations in 2008, 2012 and 2014 occurred between Hamas and the Israel Defence Forces (IDF). Significantly, in this war between 2012 and 2014, Hamas and IDF harnessed media tactics to rally international support, and disseminate information, propaganda and disinformation.

1.4 The Rise of Al-Qaeda
The emergence of Al-Qaeda under the leadership of Osama bin Laden, can be traced to the Soviet–Afghan War of 1979. Tarabay (2013) from Al Jazeera News argued, “The expansion of Arab Afghan Mujahedin movements during Russian attempts to occupy Afghanistan in 1979 was a tipping point for the rise of ‘Al-Qaeda’”. Thousands of young Arab nationals, mainly from Saudi Arabia, Iraq, Jordan, and Yemen travelled to Afghanistan in response to the Afghan mujahedin’s call for jihad. The Soviet Union’s involvement in Afghanistan sought to support the communist Afghani government, led by Najeeb Allah, against the rebelling mujahedin, who claimed the government to be anti-Islamic (Hilali, 2005). The US government backed the mujahedin by supplying weapons and other military logistics to defeat the Soviet Union forces, as the US was concerned about the expansion of communism (Wittmeyer, 2013). During the Soviet–Afghan war, which lasted for 10 years, the US installed the National Security Advisor, Zbigniew Brzezinski, in Afghanistan to monitor the performance of the mujahedin and to establish a database (translating to ‘Al-Qaeda’ in Arabic) of the mujahedin for intelligence and military purposes (Chossudovsky, 2008). In 1989, the Soviet Union leader—Mikhail Gorbachev—ended the war, due to its significant military and economic costs. Steven Randolph (n.d.) from the US Office of the Historian described the aftermath of Russian departure from Afghanistan as “the Soviets left a shattered country in which the Taliban, an Islamic fundamentalist group, seized control, later providing Osama bin Laden with a training base from which to launch terrorist operations worldwide”.

The return of the Afghan Arab mujahedin to their countries of origin concerned Arab governments and the US, as the mujahedin’s leader—Osama bin Laden—shifted his jihad strategy to the US after establishing military bases in Saudi Arabia in 1991\textsuperscript{30}. The US

\textsuperscript{30} In this sentence, I am not discussing the origins of Al-Qaeda. I am talking about the danger posed by the mujahedin who fought in Afghanistan after they returned to their homelands, particularly in Saudi Arabia.

1.5 Al-Qaeda in Iraq (AQI)

In the aftermath of the September 11 attacks on US soil, the US declared a Global War on Terrorism to seek revenge for the attacks, for which Al-Qaeda claimed responsibility. In 2002, the US managed to occupy Afghanistan and prepared to attack Iraq. In April 2003, the US troops occupied Iraq, but confronted resistance from Sunni militants in the Anbar Province, after the ousting of Saddam Hussein. Since the occupation of Afghanistan and Iraq, Al-Qaeda and its affiliates started to emerge as subgroups (almost as if the terror organisation was franchising itself), attacking US interests around the world. For example, in Iraq, Al-Qaeda affiliated with a jihadist group, under the leadership of Abu Musab Al-Zarqawi, who established a resistant group—Al-Jihad wa Al-Tawhid—to fight US troops (Atwan, 2015; Stern & Berger, 2015). Al-Zarqawi appointed Abu Bakr Al-Baghdadi as his deputy, who eventually became Caliph after the emergence of ISIS in 2013.

Despite the centralised structure of Al-Qaeda, Hamas, and Hezbollah, the use of ICTs—especially the internet—has changed the form of these organisations to be decentralised, distributed, and leaderless (Sageman, 2011). Thus, this chapter explores the role of ICTs and the internet in changing the shape and ways that terror organisations form IOs and maintain their networking structure. As Zanini (1999) argued,
Terrorist groups are taking advantage of information technology to coordinate the activities of dispersed members. Such technology may be employed by terrorists not only to wage information warfare, but also to support their own networked organisations (p. 247).

1.6 Terror Communication Before the Emergence of ISIS

SMNs and other ICTs have been noted for their role in galvanising social movements and mediating terrorist communications over the last decade (Cox, 2006; Garrett, 2006; Jefferson, 2007). The network design of terror organisations or groups is dependent on connections between individuals, which requires communication tools to create these networks. Thus, communication tools are essential as terror organisations acquire C2 operations. McLuhan (as cited in Soriano, 2008)—one of the most distinguished researchers on the social impact of mass media—indicated that “without communication, terrorism would not exist” (p. 2).

To understand the role of media in shaping the organisational form of Middle Eastern terror organisations, Arquilla, Ronfeldt and Zanini (1999) in their book, Networks and Netwars, claimed:

Middle East Arab terrorists are on the cutting edge of organisational networking and stand to gain significantly from the information revolution. They can harness information technology to enable less hierarchical, more network design—enhancing their flexibility responsiveness and resilience. (p. 29)

This chapter examines three case studies of terror networks, and how these terror organisations deepened their roots in ICTs and SMNs to maintain their networking structure and sustain flows of information. The case studies include Al-Qaeda, Hezbollah and Hamas.

1.7 Al-Qaeda’s Cyber Operations
This case study will discuss how Al-Qaeda harnessed the internet and digital information environments for C2 operations, the spread of ideology, the coordination of attacks, the dissemination of propaganda, and the call for global jihad (Conway, 2012; Conway & McInerney, 2008; Hoffman, 2003; Sageman, 2004; Weimann, 2010). Al-Qaeda jihadists were aware that they were fighting a battle, in which the main setting was the news media itself. This view was expressed by Ayman Al-Zawahiri in a personal letter to Al-Zarqawi (as cited in Soriano, 2008):

However, despite all of this, I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our Umma. And that however far our capabilities reach, they will never be equal to one thousandth of the capabilities of the kingdom of Satan. (p. 9)

Al-Qaeda has strategically adapted internet technologies to recruit potential followers and to win the hearts and minds of Muslims around the globe. Al-Qaeda have also used online media to present itself as a social online movement. As Gerdes (2011, p. 172) suggested, by presenting itself as a social movement, Al-Qaeda allowed potential followers easy access to participate. This impacted on its web activity, as more participants were driven to the organisation. Therefore, Al-Qaeda expanded its reach by adapting and creating more web pages and harnessing multiple information environments.

The literature on Al-Qaeda’s utilisation of digital technologies is overwhelming. Thus, in this case study, I will highlight Al-Qaeda’s digital terrorism in correlation with ISIS terrorism. That is, ISIS inherited the media legacy of Al-Qaeda, as ISIS operated under Al-Qaeda prior to declaring the Islamic caliphate in July 2014. The argument put forward in this case study is based on a prediction by terrorism scholar, Peter Neumann (2010), who suggested that:
By 2020, an entirely new generation of ‘jihadists’ will have gone through Al Qaeda’s training camps, who will have returned to their home countries and re-created the kind of global network that emerged in the 1990s. In addition to being trained in terrorist tactics, this ‘second generation’ of Al Qaeda will harness the full power of the Internet to coordinate attacks as well as communicate and propagate their views. (pp. 10–11)

This case study is twofold. The first aspect is concerned with how Al-Qaeda harnessed internet technologies prior to the September 11, 2001 attacks. The second aspect of this study is concerned with the rise of AQI in 2003 until the Arab Spring uprisings of 2010.

1.8 Al-Qaeda Prior to September 11, 2001

Prior to the September 11 terror attacks on the US in 2001, Al-Qaeda harnessed the internet to communicate via email and World Wide Web (WWW) with sympathisers of the global jihadist movement around the world (Behnke & Hellmich, 2012; Hoffman, 2003; Levin, 2011; Rudner, 2016; Schmid, 2014; Weimann, 2010). The use of ICTs was essential for operational and organisational purposes. At an operational level, Al-Qaeda’s communication during this period relied on the WWW to act as an information environment, to disseminate propaganda, spread the culture of jihad, coordinate attacks, recruit and radicalise new members, and raise funds (Adhami, 2007; Arquilla et al., 1999; Jefferson, 2007; Lesser, Arquilla, Hoffman, Ronfeldt & Zanini, 1999). As a further example of Al-Qaeda’s ability to make intelligent use of the WWW, Al-Zawahiri (in 2007) participated in an online interview, including a chat session with questions from individuals and news organisations (Sieb, as cited in Gerdes, 2011, p. 172).
Al-Qaeda invested in websites, such as Neda’a Al-Islam and Shumukh Al-Islam, to become the main hubs for Al-Qaeda’s ideology and propaganda distribution. Al-Qaeda also established the *Inspire* magazine, as well as As-Sahab media\(^{31}\) and Al-Forqan\(^{32}\) media wings\(^{33}\) to produce propaganda videos. Zanini (1999) observed that in the network structure of Al-Qaeda:

> The most decentralized groups—appear to have embraced information technology to coordinate activities and disseminate propaganda and ideology. This is consistent with the rise in the Middle East of what has been termed techno-terrorism, or the use by terrorists of satellite communications, e-mail, and the World Wide Web. (p. 251)

Other communication technologies, such as Paltalk and Bulletin Boards, were used for organisational and internal communication purposes. Zanini (1999) reported:

> According to reporters who visited bin Laden’s headquarters in a remote mountainous area of Afghanistan, the terrorist financier has computers, communications equipment, and a large number of disks for data storage. Egyptian ‘Afghan’ computer experts are said to have helped devise a communication network that relies on the World Wide Web, e-mail, and electronic bulletin boards so that the extremists can exchange information without running a major risk of being intercepted by counterterrorism officials. (p. 251)

\(^{31}\)The official media wing of Al-Qaeda.

\(^{32}\)This media wing has served ISIS as a propaganda machine.

\(^{33}\)Media wings and media arms are metaphors used to express the important role played by these media platforms in the organisation’s propaganda war.
However, most of Al-Qaeda’s digital activity focused on depleting US resources and spreading fear among the Western world through PSYOP. Some of these operations included threats to attack the US using biological and chemical weapons, direct messages sent by bin Laden on regular bases, threats of imminent attacks, and the claiming of responsibility for small attacks by individuals in the West. Simultaneously, Al-Qaeda directed its call to jihad towards Muslims around the world. As Theohary (2011) noted, “Most Al Qaeda-produced ideological material reflects Al Qaeda supporters’ shared view of jihad as an individual duty to fight on behalf of Islam and Muslims” (p. 1).

As Al-Qaeda claimed responsibility for the September 11 attacks and the US declared its Global War on Terrorism, a new chapter of terror communication emerged. Retrospectively, this era is marked by the establishment of global terror networks affiliated with Al-Qaeda.

1.9 The Occupation of Iraq in 2003 and the Emergence of ISIS

In the wake of the September 11 attacks, the US government decided to destroy Al-Qaeda in Afghanistan. However, while the US managed to occupy Afghanistan by 2002, Al-Qaeda operatives fled to Pakistan, Iraq, North Africa and Yemen. The attack on Iraq and the ousting of the former president, Saddam Hussein, resulted in the creation of a political vacuum and fertile sphere for insurgency networks to emerge. One of these networks was Al-Qaeda. However, this subsection will focus on Al-Zarqawi’s use of internet technologies to carry out PSYOP to establish AQI and resist US forces after the demise of Saddam Hussein. As Conway and McInerney (2008) explained, “By going online, however, Zarqawi was able to both control the interpretation of his violent message and achieve greater impact with smaller operations” (p. 23). Part of this discussion will highlight the Al-Nusra terror organisation’s use of SMNs as part of their propaganda strategy.
After the September 11 attacks until the rise of ISIS, Al-Qaeda harnessed websites as the main hub for information dissemination. Additionally, the emergence of web 2.0 technologies made a significant contribution to Al-Qaeda’s IO purposes. Adhami (2007) observed, “The jihadi websites are a phenomenon that has developed considerably in the post-9/11 era” (p. 864). According to Weimann (2010), in 1998, the US Department of State counted no more than 15 websites maintained by terrorist groups; however, in 2005, there were more than 4,000 websites supporting terrorist activities. In the post–March 2003 era, Iraq had become the main subject of discussion on these websites (Weimann, 2010). The material posted on these websites included, video clips of bin Laden in training camps in Afghanistan, electronic journals that contained analyses of the conflict in Iraq and Al-Qaeda operations, technical information about bomb-making, instructions on how to conduct simple operations, and speeches by clerics who emphasised the importance of jihad (Adhami, 2007; Conway, 2012).

The literature on Al-Qaeda’s use of communication technologies is immense and for the purpose of this thesis, I have highlighted some aspects of information production and dissemination tactics—which have been rarely documented and researched in academia—as a first step in understanding the IO strategy of ISIS networks. However, ISIS invested more in the production of ‘terror HD’ propaganda videos than PSYOP. Therefore, in Section 1.7 I have only highlighted the most important elements of the logistics of PSYOP exercised by Al-Qaeda.

1.10 The Logistics of Psychological Warfare

In this section, the thesis discusses the logistics of PSYOP carried out by Al-Zarqawi’s group, AQI, and their IO strategy. Part of their productions include the Baghdad sniper
propaganda videos. AQI (Al-Zarqawi’s group) realised the potential for video technology to be used during operations, in which US troops could be targeted with the intention of causing psychological and morale effects. In May 2004, Al-Zarqawi himself beheaded an American hostage live on video. This was the first propaganda video produced by Al-Zarqawi that was posted on the internet. Conway (2012) argued that:

The entire purpose of the beheading was to video it, to create images that would grip the imaginations of friends and enemies alike. It worked. Zarqawi risked almost nothing in this operation; but he started a withdrawal of foreign contractors which has paralysed reconstruction in Iraq and done as much if not more to undermine US plans as a bomb that killed 100 people in Najaf. And he made himself a hero to jihadis across the world. (p. 23)

The relationship between the camera and the gun proved a more powerful weapon than the gun and bullet. While a bullet may kill an active combatant, a video camera has the power to cause psychological damage to troop morale. For example, Al-Qaeda’s Sniper 1 (Juba Baghdad Sniper) video production generated great effect on the morale of US troops in Iraq. Every single bullet that was directed at the head of a US marine was documented with a video camera that was attached to the sniper’s gun. As described by Rory (2005), the “sniper saps the morale of US marines in Iraq”. The 30-minute video included over 50 Al-Qaeda operations, which invited other jihadi to join the fight against US troops in Iraq. Rory (2005) recounted some of the harrowing dialogue, “The video starts with a man saying, “I have nine bullets in this gun and I have a present for George Bush. I am going to kill nine soldiers. I am doing this for the viewers to watch”. According to counterterrorism expert, Abdul Hameed Bakier (as cited in Adhami, 2007), “The most effective jihadi propaganda videos are currently the two clips of Baghdad’s sniper, nicknamed Juba” (p. 866).
The psychological success of the documentary, *Sniper 1*—measured by its contribution to demoralising the US marines—encouraged Al-Qaeda to produce *Sniper 2* and *Sniper 3* in 2007, and *Sniper 4* in 2008. In these videos, Al-Qaeda have used more sophisticated video cameras and post-production techniques. The video discusses the alleged fear generated within the coalition forces by insurgency snipers and shows ‘Juba’ returning from a sniping mission, marking a tally of dead US troops on a wall. To generate maximum psychological effect on US marines, the spokesperson in the videos shows sniper footage of dozens of US marines targets, along with jihadi *Nasheeds* (i.e., songs). These videos end with footage of dozens of Iraqi snipers operating on the ground. Significantly, to spread more fear among US marines and its coalition operating in Iraq, Al-Qaeda has *Sniper 4*’s subtitles translated into many languages.

It is important to mention that before the *Sniper 1* and *Sniper 2* productions, Al-Qaeda’s information production in Iraq was less sophisticated. That is, their propaganda went unnoticed as most of their earlier productions were simple, low-quality videos that documented attacks of military vehicles with no images of US casualties. These examples of failed propaganda productions led to ISIS’ adoption of sophisticated media strategies as part of its IO strategy.

Consequently, as Al-Qaeda noticed the change of dynamic and participation with its videos after using sophisticated production strategies, it moved to produce more propaganda videos that were dependent on web 2.0 technologies such as Twitter, YouTube, and Facebook to expand its audience and reach. Marks (2005) observed an advertisement on Al-Qaeda’s website that said, “Wanted: Video editors, writers, and webmasters to help Al Qaeda spread its message. Contact: The Global Islamic Media Front via email.” Marks (2005) claimed that
“prior to 9/11, only a handful of extremist websites existed. Now there are thousands of increasingly sophisticated sites offering everything from chat rooms, to videos of beheadings, as well as in-depth instructions on kidnapping, bomb-making, and recruiting”.

To this end, AQI under the leadership of Al-Zarqawi have built a strong network in Iraq. After his death in 2007, Al-Qaeda became an integral part of the Sunni community in Anbar Province, and consequently, played a significant political role during the Iraqi uprisings in 2012. The internet helped Al-Zarqawi build his brand very quickly. Arguably, his use of production strategies assisted in breeding the most sophisticated terror organisation in the Middle East, ISIS. However, in Syria, Al-Qaeda was operating under the Al-Nusra terror organisation. Al-Nusra had a critical role during the Syrian Civil War, which started in March 2011, and is recognised as part of the Arab Spring uprisings.

The Al-Nusra leader, Abu Mohammad Al-Julani, was Abu Bakr Al-Baghdadi’s aid before Al-Baghdadi proclaimed himself as Caliph. During the years between 2012 and 2013, AQI (now under the leadership of Al-Baghdadi) sent logistical aid (e.g., weapons, ammunition and cars) to Al-Julani to fight the Syrian army. However, the rejection of Al-Julani’s pledge of allegiance to the Caliph, and his insistence to maintain his position in Al-Qaeda, forced Al-Baghdadi to declare war against him. Al-Nusra has been designated as a terrorist organisation by both the US and Russian governments. Unlike ISIS, Al-Nusra does not receive a great deal of coverage in mainstream media. This is partially due to the way that Al-Nusra manages to fly under the radar on Twitter. However, Al-Nusra has been described as the harshest anti-Assad guerrillas, and it has been distinguished for its application of sharia law on its own people.
1.11 Hezbollah’s Media Strategy

Hezbollah is one of the most sophisticated terror organisations that has emerged from the Middle East. That is, it is structured as a hierarchical, centralised organisation, while its C2 operation is decentralised, based on auftragstaktik operations. As Zanini (1999) described it, “The pro-Iranian Hezbollah acts as an umbrella organisation of radical Shi’ite groups, and in many respects, is a hybrid of hierarchical and network arrangements” (p. 250).

In this case study, I explore Hezbollah’s IO strategy and the role played by web technologies and satellite channel (e.g., Al-Manar) in PSYOP during the 1996 to 2006 military confrontations with the Israeli forces. The emergence of WWW and satellite channels helped Hezbollah to end 18 years of Israeli occupation of south Lebanon, which ultimately led to Hezbollah’s victory in the 2006 asymmetrical war. As Schleifer (2006) stated, “The visual media proved one of Hezbollah’s most effective weapons” (p. 6). It is important to highlight the role of SMNs as weapons for C2 operation utilised by Hezbollah guerrillas. As Nissen (2015) argued:

Hezbollah also used social network media for command and control and to defend their main information distribution channel (Al-Manar TV) from IDF cyber-attacks. Information (propaganda products) was, besides being aired over Al-Manar TV, re-distributed regionally and globally through PowerPoint presentations, video-clips and photos with an attached story in e-mails, video up-load sites, social media and blogs. (p. 77)

Along with its main websites (hizbollah.org and www.almanar.com.lb), the Al-Manar satellite channel was instrumental in galvanising Arab opinion, by carrying out public relation campaigns against Israel and promoting Hezbollah’s ideology. Therefore, it is important to highlight its role as a weapon in the asymmetrical war against Israel.
Since its emergence in the 1990s, Al-Manar was critical to the information production and dissemination of Hezbollah’s propaganda for local and international audiences. Al-Manar worked hard to promote the ideology and narrative of Hezbollah being the ‘moqawama’ (i.e., the resistance) “to almost 200 million regional viewers” (Caldwell, William, Murphy & Menning, 2009, p. 5). As El Houri and Saber (2010) argued, “Throughout this decade the Hezbollah would focus on promoting a narrative of ‘resistance’ and developing their media capacities by introducing the ‘Channel of the Resistance’” (p. 72). Further, Conway (2007) highlighted the strategic role played by Al-Manar in shaping Hezbollah’s politics, suggesting that:

Al Manar has, since its foundation, been a television station devoted to the goals of Hezbollah, and although these have been subject to change over time, the overarching theme of resistance has persisted throughout. From its establishment in 1991 to the Israeli withdrawal from the south in 2000, the bulk of the station’s programming was aimed at sustaining and, if possible, strengthening the Lebanese public’s support for Hezbollah’s campaign of resistance against the IDF in south Lebanon, while at the same time pressuring Israeli viewers to push their government for a unilateral withdrawal. (p. 8)

The newly established Shiite political party borrowed from the revolutionary thinking of Khomeini of Iran but required the media strategy to establish legitimacy in the Arab world. This legitimacy was important as Lebanon had suffered under civil war and the Israeli occupation of southern Lebanon, the West Bank, and the Golan Heights. Hezbollah gained notoriety in the Arab world at a grassroots level, by intensifying daily attacks on Israeli targets in southern Lebanon. Therefore, it called itself ‘Mumanah’ and ‘Moqawamah’ (i.e., the resistance and protection party) against Israeli aggression. Hezbollah’s border operations
against Israel were documented by using video and broadcast on the Al-Manar satellite channel showing its victories against the Israelis. El Houri and Saber (2010) described this strategy as an “efficient strategy of representation by videotaping their military operations and exposing these images to the public. Hezbollah exploited the power of these videos to reshape the prevailing political, cultural, and military realities” (p. 71).

Since its emergence in 1985, Hezbollah’s warfare strategy was based on documenting its operations using video. As Schleifer (2006) observed, “The organisation’s motto could be summed up in the words: If you haven’t captured it on film you haven’t fought” (p. 6). Through the use of the video camera “Hezbollah demonstrated how it was possible, with only a few simple pieces of equipment and some creative thinking, to net huge military and psychological dividends” (Schleifer, 2006, p. 6). Most of the captured videos were posted to Hezbollah’s main websites (www.moqawamah.org and www.hezbollah.org) and broadcasted via Al-Manar satellite television. In section 1.9, I discuss the importance of internet technologies in the asymmetrical military confrontations between Hezbollah and Israel, between 1996 and 2006.

1.12 Information Dissemination During the 1996 and 2006 Lebanon Wars with Israel

Trying to end the daily rocket attacks on its northern border, Israel launched a comprehensive attack against Hezbollah guerrillas who had been fighting the Israelis in south Lebanon since 1985. IDF operations, ‘Grapes of Wrath’ (Gambill, 1998) or ‘Clusters of Anger’, included a series of coordinated Israeli raids against Hezbollah in the south of Lebanon, and its affiliates in the southern suburbs of Beirut.
At its first face-to-face confrontation with the IDF, Hezbollah succeeded in newscasting atrocities committed by the IDF and celebrating its own victories through videos posted to its two main websites and its satellite channel. As Zanini (1999) observed,

```plaintext
The internet [was] used as a propaganda tool by Hezbollah, which manages three World Wide Web sites—one for the central press office (at www.hizbollah.org), another to describe its attacks on Israeli targets (at www.moqawama.org), and the last for news and information (at www.almanar.com.lb) (p. 252).
```

Before the emergence of SMNs, terror organisations depended on their own media outlets; Al-Qaeda depended on Al Jazeera and Hamas depended on the Al-Quds satellite channels for information dissemination.

However, Hezbollah’s media platforms were vulnerable to hacking activity, which meant that their information flows could be disrupted. Technically speaking, Hezbollah’s adversaries could intercept its satellite channel, which meant the feed stream could be diverted or hacked, causing a downlink or feed stream jamming effect. As a result, satellite feed streams became a dysfunctional tool for information flows. This could also happen to web pages. Information flows can be easily hacked, defaced, and disrupted by adversaries.

The author experienced such events during the 1996 war in Lebanon, while working for the Worldwide Television News (WTN)\(^{34}\). During the ‘Clusters of Anger’ operation against Hezbollah in southern Lebanon in 1996, the WTN Amman’s bureau office received a 15-minute video taken by our correspondent in Lebanon, Assad Fighaly. The video depicted the

\(^{34}\) This news corporation was sold to APTV in 1998.
destruction of an entire primary school caused by IDF. The scenes showed the bodies of many school children, because the air strikes had targeted a refugee primary school in Qana. After we received the unedited material from a driver, who came to Jordan via the Syrian border, we contacted Eurosat to share the video as an exclusive story for WTN. We received a disturbing reply from Eurosat, who claimed to have received enough material about the Israel operation in southern Lebanon. If the material had been accepted by Eurosat, millions of viewers around the world would have been reached, generating a significant global effect. As Saad et al. (2011) noted,

The psychological impact was as significant as physical destruction. Information and reputation were very strong weapons, and both parts needed to exercise moral influence on populations, and model public opinion, if they wanted to win the conflict durably (p. 4).

The gatekeeping strategy of Eurosat had a great impact on information reach and effect. As Caldwell et al. (2009) argued:

Proliferation and accessibility have played havoc with old rules of the media game in at least two important areas, gatekeeping and agenda-setting. Before the widespread advent of the

---

35 Such videos could not be broadcast via Syria TV as the process was controlled by Syrian intelligence, requiring long approval times and carrying the risk of rejection by the censors.

36 Stationed in London, which is the main hub that receive satellite feed across the world. Eurosat has allocated five times a day to be informed to receive information from other satellite tv stations. Our contact point was via the Jordanian TV station.

37 WTN was competing with Reuters and AP in news feed.
new media, traditional editors and producers served as ‘gatekeepers’, determining what stories and features to publish in accordance with varied criteria. (p. 3)

The rejected material was filed and archived to preserve WTN’s material policy.

Nevertheless, Hezbollah managed to create many videos of the Qana massacres and post them to its websites and Al-Manar, which had been under heavy cyber-attacks at that time. This is how information sharing happened before the emergence of SMNs. However, 10 years later, a dramatic shift occurred in information dissemination tactics during the second major confrontation between Hezbollah and Israel in July 2006. The rise of social media platforms in 2004 had “abolished traditional gatekeeper and agenda setting roles” (Caldwell et al., 2009, p. 3).

Overall, the media logistics of Hezbollah during 1996 had been tested, forcing them to identify avenues for communication and dissemination that could not be easily hacked or intercepted. The jamming of its satellite feed and the hacking of its main hubs for information dissemination pressured Hezbollah to use the Lebanese government television station and other Arab independent satellite channels, such as Al Jazeera. Lesson on war logistics (e.g., military supplies) and some aspects of C2 were also learned (Kulick, 2006). Kulick (2006) argued that “the clashes of 1996 ended with relative success at the operational level, as the organisation was successful in launching Katyusha rockets into Israel up until the ceasefire”.

1.13 Social Media Networks During the 2006 Lebanon War

This era was marked with the emergence of three of the most influential SMNs—Facebook, Twitter and YouTube—which provided Hezbollah with a platform for communication. As Nissen (2015) argued, “The 2006 Lebanon war between Hezbollah and
Israel showed early on how social network media was successfully used in a contemporary conflict by a non-state actor to mitigate a conventional military disadvantage” (p. 77).

This war was initiated when Hezbollah launched a surprise attack against Israel, killing eight and abducting two IDF members (Caldwell et al., 2009; Kalb & Saivetz, 2007, p. 7) in retaliation to the killing of a Lebanese boy by IDF (as Hezbollah claimed) in southern Lebanon. However, for Hezbollah, this war was not mainly ignited for the killing of a child, it was “more than a battle against a mortal enemy; it was a crucial battle in a broader, ongoing war, linking religious fundamentalism to Arab nationalism” (Kalb & Saivetz, 2007, p. 5).

In this war, Hezbollah exploited social media platforms to achieve its IO objectives. As Nissen (2015) argued,

Hezbollah was militarily outclassed by the IDF in all areas, yet they managed to exploit tactical engagements between the IDF and Hezbollah fighters on the ground through an information-led strategy creating strategic effects through primarily social network media (p. 77).

Their information strategy was manipulated and carefully designed to serve propaganda agendas. As Caldwell et al. (2009) noted, “Hezbollah manipulated and controlled information within the operational environment to its advantage, using (at times staged and altered) photographs and videos to garner regional and worldwide support” (p. 5).

Israel’s strategic objective of this war aimed to totally paralyse Hezbollah’s C2 operations, cause damage to its military components, and end Hezbollah’s hostility against Israel.

However, these objectives were not achieved because Hezbollah succeeded to win the ‘battle of hearts and minds’ by directing its propaganda machine to atrocities committed by IDF. As Nissen (2015) argued, “Hezbollah essentially out-maneuved the IDF land campaign in the
information environment and thereby denied Israel the achievement of its strategic objectives” (p. 77). To do this, Hezbollah launched a successful IO strategy by harnessing many information environments and satellite channels to target international, Israeli, and local audiences with its message. As Nissen (2015) describes it:

From the physical battle to the information environment, Hezbollah succeeded in creating and sustaining regional and international pressure that eventually forced Israel to cease its operations before achieving its stated strategic objectives. Hezbollah heavily leveraged social network media to influence the political will of key global strategic audiences, including the Israeli population. Hezbollah ‘packaged’ (recorded/filmed, narrated and disseminated) tactical events to include both own successes and Israeli mistakes and major kinetic destruction of sites in Lebanon in a well-coordinated multi-channel cyber-strategy (p. 77).

During the 34 days of the 2006 war between Hezbollah and IDF, live broadcast and SMNs reported events closely. Propaganda was carefully crafted to demoralise the IDF and the Israeli public by showing images and videos of killed IDF members and Lebanese civilians, including women and children. Shakarian, Shakarian and Ruef (2013) noted that Hezbollah:

quickly and accurately reported the tactical situation and created professional media products that were disseminated through a variety of means—their respective Web sites and YouTube. Further, these products were created in a variety of languages, including Hebrew—which again illustrates the strategy’s main goal of influencing the opponent’s perception. (p. 35).

IDF tried hard to disable Hezbollah’s IO using DoS attacks against its websites and jamming its satellite streams. This operation created comprehensive information cyberwarfare between Israel and Hezbollah. As Shakarian et al. (2013), noted, “Military operations on the ground
were accompanied by various cyber war techniques on both sides. Notably, the Israelis conducted a denial-of-service attack on the Web site of Hezbollah’s television station, “Al Manar” (pp. 34–35).

1.14 Information Warfare—Hezbollah Versus Israel

It is important to consider the asymmetrical war between Hezbollah and Israel in 2006 from an information warfare perspective. As Shakarian et al. (2013) noted, “Hezbollah’s integrated approach to information warfare was central to their strategy. One of the main components was ‘cyber psychological operations’” (p. 35). These cyber operations aimed to win the ‘battle of hearts and minds’ of local and international audiences and demoralise soldiers, while part of Israel’s IO was to focus on making Hezbollah appear as a terror organisation. Saad et al. (2011) reported:

Hezbollah used all available means to make sure that every piece of image and testimony was carefully controlled and edited for Web dissemination. For instance, it showed in the way the Lebanese party used the images of the Qana incident, where scores of civilians were killed after an Israeli bombing. (p. 4)

As stated previously, fighting an unequal war with one of the most advanced militaries in the world required IO strategies that were reliant on media propaganda campaigns to generate a desired effect on local and international audiences. For instance, broadcasting images of killed IDF members, burned IDF military vehicles, improvised explosive device (more commonly known as ‘IED’) explosions, and live-tweeting sniper operations was part of Hezbollah’s strategy to achieve victory. Hezbollah fought PSYOP to demoralise IDF personnel and affect the way that the Israeli audience viewed the war, so they would
ultimately pressure their government to stop the war. Therefore, the maintenance of information flows from non-state actors can be essential in asymmetrical wars. As Saad et al. (2011) argued, “Psychological war took place on the Web through shocking pictures—dead children, destroyed buildings, bombings […] The enemy is demonized, and “martyrs” are revered, in order to create hatred” (p. 4).

However, the Israeli C2 operations were aware of Hezbollah’s PSYOP. Thus, they managed to attack its information infrastructure. Shakarian et al. (2013) reported that “the Israeli response of shutting down their opponent’s Web sites can be viewed similar to the supposed Russian intent of their 2008 Georgia campaign” (p. 38).

To maintain their flows of information, Hezbollah hijacked non-combatant internet protocol (IP) addresses (Shakarian et al., 2013, p. 38). The hijacking of IP addresses and broadcasting streams was essential for Hezbollah to maintain its flows of information and execute its IO strategy. Thus, to operate inside the information loop of Israelis and sustain their IO with dissemination tools, Hezbollah managed to hijack a South Texas cable operator (Hylton, 2006). As Hylton (2006) from Time Magazine reported, “The Texas cable company has an agreement with a New York–based satellite communications aggregator, which moves feeds to a variety of customers from throughout the world, including Lebanon”. She further explains:

Al-Manar was linked to the small cable company’s IP address through a telephone number. Hezbollah essentially added an extension on that telephone line allowing their traffic to flow. Hezbollah then gets the word out through e-mail and blogs that it can be found at that IP address and the hijack is complete. (Hylton, 2006)
Hijacked IP addresses enabled Hezbollah to establish websites to replace hacked ones. Hylton (2006) observed:

The IP address can be linked to a new domain name and that opens up the site to anyone who might search online for Al-Manar content. Hezbollah uses these Web sites to run recruitment videos and post bank account numbers where supporters can donate funds.

Having intercepted Hezbollah’s activity via the South Texas cable company’s communications, the US closed the portal (Hylton, 2006). Closing Hezbollah’s portals was part of a whack-a-mole strategy to hinder Hezbollah’s IO objectives. Hylton (2006) reported:

Hezbollah was just as quick to play the whack-a-mole game and a new site sprang up from an Indian Web-hosting company within hours. As long as the war drags on, these communication portals will be critical as Hezbollah tries to get its global message out across the world.

Shakarian et al. (2013) described the process of IP hijacking as “once detected [Hezbollah] was able to quickly hijack new IP addresses, which caused them to refer to their efforts as “whack-a-mole”—soon after one hijacked IP address was shut down, another one was corrupted” (p. 38).

---

38 This strategy was also used against ISIS, in terms of a mass suspension of Twitter accounts. It will be discussed in Chapter 5.
The quick response by Hezbollah’s hackers has been a game changer in cyber information warfare. That is, the speed with which they can hijack IP addresses allowed the organisation to maintain its information flows, despite hacking activity against its main information environments. Shakarian et al. (2013) described this tactic as ironically supporting “Hezbollah’s information operations (IO). It is feasible that one of the key enablers of Hezbollah’s “victory” was their ability to communicate their story faster and more effectively than the Israelis” (p. 35). Hezbollah’s websites played a critical role in reaching an Israeli audience and affecting their opinions. Schleifer (2006) observed, Hezbollah was able to surmount the in-built suspicions of Israel’s news reporters. Consequently, the IDF could only look on helplessly as material posted on the organisation’s websites would routinely appear the following day in the Israel media (p. 14).

That is, the speed and agility with which Hezbollah adapted to new information environments was a deliberate strategic and tactical operation to sustain their flows of information and outmanoeuvre their adversaries. The creation of a dynamic loop of information dissemination was part of their information-centric warfare. From a manoeuvre warfare perspective, this is what John Boyd called the ‘OODA loop’.39

To this end, Hezbollah’s cyber operations were successful. Israel opened investigation into how Hezbollah’s propaganda had affected Israel society, which pressured the IDF to halt its military operation and call for ceasefire before it achieved its military objectives. Although, during the 2006 war, the internet penetration rate and number of social media account holders

39 OODA loop (manoeuvre warfare model) developed by fighter pilot John Boyd. The acronym stands for Observe, Orient, Decide Act. will be discussed in detail in Chapter 7.
was very low, Al-Manar satellite channel and internet websites were pivotal in maintaining a dynamic loop of information dissemination. This was a significant component of Hezbollah’s IO strategy: inform the world of what was happening from Hezbollah’s perspective.

1.15 Hamas and Online Media

The Arabic word ‘Hamas’ means ‘zeal’; however, the movement has also been known as the Islamic Resistance Movement. The Council on Foreign Relations (as cited in Buke, 2008), in a posting entitled ‘Hamas’, described the organisation as “the largest and most influential Palestinian militant movement”. Hamas boosted its popularity among the Palestinian society through charity and social work, by helping poor families, caring for orphans, and assisting unemployed youth by creating job opportunities. As Zanini (1999) identified, “Hamas is loosely structured, with some elements working openly through mosques and social service institutions to recruit members, raise funds, organize activities, and distribute propaganda” (p. 249). Long before Hamas shifted its strategy against Israel by joining the first Palestinian intifada in 1978, it maintained a good relationship with the Israeli army. The Israeli government helped Sheikh Ahmad Yassin, the founder of Hamas, to establish a charity organisation and preach for social good in Gaza. Israel’s supporting of Yassin’s movement had a purpose: Israel believed that Hamas was an emergent power that could counter PLO’s hostility against Israel. This strategy worked for Israel for many years and succeeded to split the Palestinian power structures into Islamists versus secular groups (Tahhan, 2017).

According to the British Broadcasting Association (BBC, 2017), after Hamas had taken arms against Israel during the first Palestinian intifada in 1987, the US government identified it as a terror organisation. It has been reported that ‘between the years of 2000 to 2005, Hamas
carried out over 50 attacks that would cause the killing of over 280 Israelis, while in the same period almost 5,000 Palestinians have been killed by Israel' (as cited in Buke, 2008).

Weimann (2011) pointed out that Hamas “uses a wide assortment of media tactics and strategies, as do many other modern terror organisations”. Zanini (1999) highlighted Hamas’ online communication activity and claimed that “Hamas activists in the United States use chat rooms to plan operations and activities. Operatives use email to coordinate activities across Gaza, the West Bank, and Lebanon” (p. 251). The organisational structure of the Hamas network depended on its defected leaders and operatives to Syria, Jordan, Lebanon, and the US. Hamas strategically utilised the internet to facilitate leadership communication with other allies in Iran and Syria, and within Hezbollah. Zanini (1999) noted, “Hamas [comprised] splinter groups and factions with no centralized operational leadership” (p. 250).

Thus, the internet was a safe haven for Hamas’ communication with its regional allies, such as the Muslim Brotherhood political party in Egypt, Syria, and Jordan, and the Iranian government. As Zanini (1999) noted:

Hamas has realized that information can be passed securely over the Internet because it is next to impossible for counterterrorism intelligence to monitor accurately the flow and content of Internet traffic. Israeli security officials have difficulty in tracing Hamas messages and decoding their content. (p. 251)

The accessibility of SMNs in Gaza and the West Bank was a crucial tool that served the cause of Hamas during its confrontation with the IDF. That is, the Israeli military managed to blackout media in Gaza by banning the entry of global media television stations to cover military confrontations. As Ward (2009) observed:
With foreign press shut out, scarce electricity, and little internet infrastructure, the media
dynamics in Gaza centred on a handful of Palestinian journalists who worked across a range
of media formats to provide footage and primary reporting necessary for traditional and new
media alike. (p. 2)

Israel employed social media sites to build networks of recruited agents, who were operating
in Gaza and the West Bank. As Ward (2009) identified:

Social media [networks] have advanced to the fore in this round of fighting because of Israel’s
decision to impose a media blackout on Gaza. Days before the beginning of operation ‘Cast
Lead,’ foreign correspondents were barred from entering the territory. The Israeli government
even prohibited Israeli soldiers from bringing in mobile phones—by now the medium of
choice for leaks of embarrassing information the world over. (p. 2)

During this time, Hamas seized Gaza and dishonoured its peace treaty with Israel (which had
been signed by the Fateh movement). Thus, SMNs acted as a double-edged sword. While
Hamas used the platforms to share grievances and atrocities committed by Israel, Israel
utilised the platforms to spy on and recruit agents in Gaza. The recruited individuals played a
critical role as a source of intelligence during military confrontations and in the assassination
of Hamas’ leaders.

Leyden (2010) indicated that “Hamas has also accused Israel of using Facebook to recruit
Palestinian spies from among the Gaza strip community”. One of the disadvantages of social
media was that Israel was able to closely monitor the online activity of Palestinians, using
surveillance technologies. Leyden (2010) confirmed:
Israel has always maintained agents in the West Bank and Gaza, but Hamas thinks that fans of Facebook and similar services are revealing too much personal information on social networking which leaves them open to attempts to coerce them into becoming spies. It is suggested that Israel may be monitoring social networking sites to identify networks on contacts with links to either Hamas or local criminal networks.

1.16 Social Media During Wartime in Gaza

Military confrontations occurred between Israel and Hamas in 2008, 2012, and 2014. These confrontations were characterised by an extensive use of web 2.0 platforms from both sides. As Zeitzoff (2011) explained, “The Gaza Conflict saw the emergence of social networking and new media sources that vastly increased the speed and dissemination of information from the battlefield” (p. 942).

Both Hamas and the IDF established Facebook pages and created hashtags on Twitter to establish real-time information cyberwar. That is, as Zeitzoff (2013) noted, “The use of Twitter by Israel and Hamas during the 2012 Gaza Conflict marked the first time that conflict belligerents extensively used social media during an active conflict” (p. 12). An IDF spokesperson declared its intention on attacking Hamas via the microblogging platform, Twitter: ‘The IDF has embarked on Operation Pillar of Defence—@IDFSpokesPerson, November 14, 2012’.

The confrontation over Twitter started when the IDF (as cited in Zeitzoff, 2013) tweeted, “We recommend that no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead—@IDFSpokesPerson, November 14, 2012” (p. 2). Al-Qassam Brigade40 (as cited in Zeitzoff, 2013) replied to the

40 The military wing of Hamas.
previous tweets saying, “@idfspokesperson Our blessed hands will reach your leaders and soldiers wherever they are (You Opened Hell Gates on Yourselves)—@AlQassamBrigade, November 14, 2012” (p. 2).

The extensive use of social media—specifically, Twitter—by both sides in the 2012 Gaza–Israel conflict was unprecedented. Twitter is a social media platform for rapid, public, concise messages to be shared among networked followers (Zeitzoff, 2013, p. 3). Zeitzoff (2013) identified some purposes behind the use of Twitter by the IDF. He suggested:

1. It was in English, so the communication was likely directed at an elite, international audience. The subject of the IDF’s communication emphasized the Hamas rocket attacks and Israeli victimisation and were further used to justify to an international audience Israel’s military campaign.
2. Another strategic goal of the @IDFSpokesperson Twitter feed was to combat what it perceived as Hamas misinformation. (p. 7)

The use of social media by Israel was not limited to Twitter or Facebook; the IDF also utilised Flickr, Pinterest, and Tumblr to engage with international audiences in support for Israel. For instance, according to, the New Yorker columnist, Emily Greenhouse (2012), “The I.D.F. Flickr account parades Hamas’ rocket-launch sites alongside well-produced infographics announcing how many millions of Israelis are under fire, or within range”. The military’s newly created Tumblr shows leaflets in Arabic dispersed around the Gaza Strip, warning residents to “take responsibility for yourselves and avoid being present in the vicinity of Hamas operatives and facilities and those of other terror organisations that pose a risk to your safety”. The IDF also utilised Pinterest for propaganda purposes as Greenhouse (2012) observed, “Their Pinterest is all glory photos of I.D.F. soldiers who’ve ‘waited and trained long and hard’ receiving the ‘highly coveted red beret,” and shots of noble
humanitarian aid’. IDF’s Facebook page established a counting meter for rockets fired from Gaza targeting Israeli settlements. Greenhouse (2012) noticed, “The I.D.F. Facebook page posted, “400 Rockets from Gaza hit Israel in the last 3 days”. Meanwhile, Hamas used SMNs to report of “civilian casualties on Web pages, Twitter and Facebook pages in English, Arabic and Hebrew” (Hirschauge, 2014). The strategic use of hashtags by both sides of the conflict during 2008 and 2012 had catalysed a massive propaganda war. As Plede (2012) noted:

Twitter became a battleground for tens of thousands of regular people who had an opinion, challenged someone else’s opinion, or wished to share updates. Under the hashtags #GazaUnderAttack, #PillarOfDefence and #IsraelUnderFire, hundreds of thousands of tweets exchanged reports, opinions, and challenges to mainstream news reports and to each other.

To counter the narrative of Hamas’ influence on Twitter using #GazaUnderAttack, the IDF created #IsraelUnderFire to seek international support against Hamas’ rockets fired on Israel. The two hashtags attracted hundreds of thousands of supporters from Palestinian and Israeli people. Iftikhar noted (2014), “The conflict in Gaza has quickly become a “war of the hashtags.” Whereas Israel’s side of the story had dominated global media coverage for nearly half a century”. Media outlets reported that the hashtag #GazaUnderAttack had been used over four million times, compared to only 200,000 instances of #IsraelUnderFire. Other estimates indicated that there were over 11 million tweets of pro-Palestinian hashtags, such as #SupportGaza and #PrayForGaza, throughout the duration of the conflict (Iftikhar, 2014).

Since the 2012 confrontation, Israel and Hamas realised the importance of SMNs to win the battle of people’s hearts and minds. As Iftikhar (2014) stated, “In this most recent Israel/Gaza crisis, Twitter, Facebook, and YouTube have played a far more prominent role in shaping global public opinion than they did in previous Middle East conflicts”. Nevertheless, Hamas
is more desperate than Israel in harnessing SMNs, as it believes the mainstream media is biased and controlled by Zionists (Mason, 2014). As Ward (2009) identified, “Israel is using its military might to control media on the battlefield, while partisans of both sides strive to influence public opinion using social media” (p. 1). Hamas’ use of Twitter was not limited to #GazaUnderAttack; it disseminated information and reported casualties and destruction caused by IDF on trending hashtags such as #worldcup and #MalaysianAirline17. According to statistics from Twtrland,

An Israel-based start-up, there were 319,757 mentions of ‘Gaza’ on Twitter on Thursday, the day Israel started its ground war. That was more than the 270,292 tweets with a #worldcup hashtag during the World Cup final. There were 456,000 tweets about Malaysia Airlines Flight 17 over the last 24 hours as of about midday Tuesday (as cited in Hirschauge, 2014).

The use of trending hashtags is a strategy used by Hamas to expand the reach of its message to a wider audience.41

Moreover, the military confrontations were reportable via YouTube. Since 2008, during ‘Cast Lead’ operation against Gaza, Hamas’ media arms and citizen journalists in Gaza widely posted videos on YouTube as international media outlets were banned entry to Gaza. Hamas had been honing its own message on Twitter—increasingly taking responsibility for the sharing of ideas to come from in-house, instead of relying on outside activist groups (Hirschauge, 2014). Graphic videos and images of murdered Palestinians (many of whom were women and children) and destruction caused by the IDF air force were instantly uploaded to YouTube and Twitter by regular citizens of Gaza. These images were quickly

41 The hijacking of trending hashtags is also a strategy used by ISIS, see Chapter 4.
distributed by Al Jazeera, CNN, and the New York Times. For instance, Paul Mason (2014) from the Israel Channel 4 News described the bombing of Shwajaea,\(^{42}\) where tens of Palestinian civilians were killed, demonstrating that Hamas was dominating the social media war over Gaza. He noted that, “It is evidence of a massive change in the balance of power between social media and the old, hierarchical media channels we used to rely on to understand wars” (Mason, 2014).

Hamas used YouTube to spread propaganda and fear among Israel people by uploading videos depicting the launches of missile attacks on Israel. The BBC (2012) reported, “It [Hamas] posted a YouTube video purportedly showing the launch of a Fajr 5 missile towards Tel Aviv for the first time”. Within this chaotic sphere of online and on-ground conflicts between Israel and Hamas, there were winners and losers in this bloody war.

1.17 Winners and Losers—Information Warfare During Wartime in Gaza

During military operations, information played a decisive factor in winning the war. As the Israeli army depended on centralised C2 operations, information was coordinated by the Ministry of Defence central command. These operations required sophisticated military communication tools between commanders on the ground and in the operation centre. This is in contrast to guerrilla warfare, wherein guerrillas advanced their operation based on decentralised C2 warfare. Communication between guerrillas were pre-planned beforehand and to some extent they used ham radio (for re-planning or aborting missions), but mostly they depended on the current progress of the war, described as auftragstaktik. However, this perception changed with the emergence of ISIS, as they depended on information environments as C2 warfare. This was due to their large number of operations and the size of

\(^{42}\) Palestinian camp on the border of Gaza and Israel.
territory they controlled. However, winning a war cannot be determined by on the number of casualties or the scale of destruction caused alone. It can be decided through a total paralysis of the enemy’s C2 operations, forcing the enemy to concede defeat. Thus, the loser submits to terms of ending the war that are decided by the winners.

Information became the domain of the third-generation warfare; the use of information for propaganda and public relations were decisive factors in the winning and losing of the war. Iftikhar (2014) reported:

For the first time ever, it appears that Israel is losing the public relations war in their most-recent military escapade into Palestinian territories. The social media counter-narrative has been so overwhelming that the clearly threatened Israeli Prime Minister Benjamin Netanyahu had the audacity to claim that people in Gaza are using “Telegenically dead Palestinians” in order to bolster international support for Palestinians on social media.

Mason (2014) also observed that:

Its media is traditionally heavily skewed towards the pro-Israeli view. But now, for the first time in a major Arab-Israeli conflict, the American public has other sources of reality. All research says that young people everywhere regard Twitter as essentially a news service, and via your social network you can easily get served up words and pictures more impactful than anything on TV. By the time many Americans woke up on Sunday, these pictures were of dead Palestinian children.
Despite the crucial role played by SMNs during the Gaza–Israel conflict in raising international awareness of civilian casualties, there have been some setbacks for Hamas. For example, Twitter suspended several Hamas-affiliated accounts based on the reason that ‘the U.S. government brands Hamas as a terrorist organisation’ (Hirschauge, 2014). Some graphic content posted by both the IDF and Hamas has also been targeted and removed by YouTube. Greenhouse (2012) reported:

Both Twitter and YouTube temporarily removed content right after the attacks began—the @IDFSpokesperson account, the I.D.F. video showing the strike that slayed Jabari—but they’re back up, and Flickr has said that it will not be removing content from the I.D.F. photo stream.

While YouTube’s Terms of Service (TOS) state that “if your video shows someone being physically hurt, attacked, or humiliated, don’t post it”, guidelines are not rigidly enforced conditions of usage. Google, which now owns YouTube, has previously expressed “a bias in favour of people’s right to free expression in everything we do”. However, Twitter’s TOS explicitly ban “direct specific threats of violence against others”, including the recommendation from the IDF spokesperson’s account “that no Hamas operatives, whether low level or senior leaders, show their faces above ground” (Greenhouse, 2012). Further, the online war was not limited to hashtags. Hamas and Israel mobilised hackers to engage with the online battlefield. Nissen (2015) stated:

Both Hamas and the Israelis also mobilised ‘patriotic hackers’ and online activists to engage in a cyber-battle for control over the social network media sphere. This was done through ‘force multiplication’ activities, such as creating supportive online
communities and networks as well as through direct computer network attacks on, or hacking of, the opposition’s social network media accounts and platforms. (p. 78)

The Israel–Hamas war of 2008, 2012, and 2014 shows the importance of SMNs as tools to carry out IOs during conflict. For Hamas’ fight in an asymmetrical war, social media became tools of psychological, C2 operations. The instant upload of information during wartime to Hamas guerrillas was crucial, as this information helped them understand the location of their next target. During its military operations, Hamas recorded its surprise attacks against the IDF, which had a great impact on the morale of IDF soldiers. For example, in operation ‘Auz Nahal’ during the 2014 war, Hamas attacked an Israeli military base, killing all IDF in that military base, which generated a significant impact on IDF morale. This propaganda video was immediately uploaded to social media to achieve maximum effect.

To this end, both sides of the conflict have weaponised Twitter and YouTube as part of their propaganda and information warfare strategy to win ‘hearts and minds’ of the international community. Due to the pervasiveness of mobile phone and internet technologies, Hamas won the propaganda war. As Iftikhar (2014) concluded:

Because we are on the ground, and we are multitudes, and we have camera phones and social media. More terrifying to Israel than how Palestinians look on television should be how many of their supporters are plugged into social media. The truth is, revolutions will no longer be televised—they will be broadcast in real-time on Twitter, instead.

1.18 Conclusion
This chapter has discussed three terror organisations that have operated in the Middle East and Iraq and considered how they have used information as weapons to fight asymmetrical wars. It has also examined how these organisations emerged, leveraged, and flourished using digital media platforms and satellite channels. Al-Qaeda, Hamas, and Hezbollah have strategically weaponised social media platforms and internet technology as the logistics of their IO to pursue their political ends. These platforms were critical in the pervasiveness and leverage of these terror networks. These platforms allowed these organisations to maintain and control information flows in real-time. This chapter established how future terror organisation, such as Al-Nusra and ISIS, have used information as a weapon and engaged in sophisticated cyberwar in asymmetrical wars.
2 Chapter2 Post–Arab Spring Networking Dynamics—Information-Centric Warfare and Social Media Networks

2.1 Introduction

As explained in chapter I, ICT and social media platforms played a critical role as instruments of information warfare, utilised by terror organisations operated in the Middle East in the period between 2004-2009. In addition, this chapter outlines the first appearance of decentralised and distributed media operations in the MENA theatre – this is crucial in order to gain the necessary context for ISIS’ operations in that same theatre.

In this chapter, I examine how social media platforms orchestrated the new wave of social movements that erupted in the Arab world in the period between 2010-2013, with a focus on the Egyptian, Syrian, and Iraqi uprisings. This chapter argues that digital media logistics played a pivotal role in establishing a form of communication that lead to the emergence of ISIS during the Syrian and Iraqi uprisings. That is, the transformation and dynamics of social network emerged during the Arab spring uprisings led to the establishment of an organised form of terror networks.

The objective of this chapter is to examine the significance of the emergence of web 2.0 on the Arab Spring uprisings in regard to both state and non-state actors. The aim of this chapter is to highlight how the social media revolution began to display a darker side, as SMNs became tools for information-centric warfare. My argument is that SMNs aided in the establishment of political and ideological polarisation, which penetrated society and inspired political mobilisation. The rapid changes in the media environments during the Arab Spring uprisings divided Arab society at both the macro and micro levels. SMNs in general, and mainstream media in particular, have enhanced social fragmentations, inciting conflict
between liberals and conservatives, within homophilic groups, between ethnic and religious minorities and Islamists, and between family members (Shehabat, 2015). The effect of political polarisation has led to a divided society, comprising clashing of ideologies, and has incited information-centric warfare between anti- and pro-government actors (Krieger & Belliger, 2014, p. 61). In this chapter, I discuss the role of web 2.0 in some of the events from the Egyptian uprisings. Additionally, I explain how the emergence of new networking tendencies destabilised and challenged established social structures. I include analysis of how the utilisation of SMNs has shifted from ‘networks of outrage and hope’ to ‘networks of antagonism and hate’ into ‘networks of terror’. Finally, I examine the role of SMNs during the Syrian and Anbar (Iraq) uprisings, prior to the rise of ISIS.

2.2 Web 2.0 and the Arab Spring Uprisings

There have been many discussions about the role of social media in the evolution of the Arab Spring uprisings in late 2010 and early 2011 (Bruns, Highfield & Burgess, 2013; Comunello & Anzera, 2012; Gerbaudo, 2018; Howard et al., 2011). In the wake of the upheavals that became known as the Arab Spring, social media platforms (such as Facebook, Twitter and YouTube) were heralded as the catalyst that sparked, mobilised and coordinated the uprisings. Media outlets coined the terms ‘Facebook revolution’, ‘Twitter revolution’ and ‘YouTube uprisings’ to describe the prominent role of social media in these events. The use of internet and other ICTs by ordinary citizens for the purpose of organising social uprisings, achieving political goals (such as promoting democracy) have been examined extensively by scholars and political commentators (Campbell, 2011; Castells, 2013; Howard & Hussein, 2013; Khamis et al., 2012). Historically, SMNs and other ICTs have been noted for their role as medium of communication in facilitating the social movements in the last decade. For instance, the first reported use of SMNs by dissident groups took place in a civil revolt in
Moldova in 2009, widely known as ‘the first Facebook revolution’ (Zuckerman, 2009). The unrest in Iran in 2009 was also called ‘the first Twitter revolution’ (Sullivan, 2009). Further, in the last century, SMS (i.e., Short Messaging Service) was credited with playing a crucial role in toppling the Philippine’s former president, Joseph Estrada, in 1995 (Shirky, 2008). Similarly, cassette tapes were considered to have played an important role in the Iranian Revolution of 1979 (Shirky, 2008).

The role of SMNs during the first wave of social unrest in Egypt in 2011 has been the focus of empirical studies conducted by researchers and scholars (Campbell, 2011; DSG, 2011; Howard & Hussein, 2011; Lotan et al., 2011). Qualitative and quantitative evidence was captured during the events of the Egyptian uprisings that clearly demonstrates how pervasive of SMNs have empowered civilian activists while disempowering authoritarian governments. For example, Lotan et al. (2011) focused on Twitter feeds posted by digital activists during the Tunisian and Egyptian revolutions. Lotan et al.’s (2011) analysis involved comparing information diffusion by the state’s mainstream media with Twitter data that reached global audiences through individual activists and journalists. The study concluded that the revolutions were, indeed, ‘tweeted’. This study made clear, for the first time, how media could be produced and disseminated worldwide and compete with mainstream, state-controlled media. This study documented the power shift that occurred in favour of the Egyptian people as they generated global public support for their cause. In another study, Khamis et al. (2012) described how political activists have used new forms of communication—especially digital and online social media, such as Twitter, Facebook and the video-sharing portal, YouTube—as tools for highlighting the regime abuses of citizens, promoting citizen journalism, shaping public opinion and organising or mobilising citizenry.
to combat repression. They conclude that, “the balance of both political power and media power has shifted unpredictably and will continue to do so” (Khamis et al., 2012).

Seo and Ebrahim (2016, p. 231) studied how both sides of the conflict utilised SMNs to exchange political messages and concluded that dictators understood the role of social media in information warfare. For example, the Syrian government used social media to locate activists and the source of dissemination of misinformation. Similarly, in Egypt, political messages were exchanged between the military government and dissenting groups as part of C2 operations, which were aimed to intimidate and persuade. Comunello and Anzera (as cited in Nissen, 2015, p. 455) noted that governments generated social control through their direct management of media and application of surveillance technologies to intimidate protesters and decrease political engagement of grassroots movements.

The environment of conflict between dissenting groups and the government have made it difficult for anti-government movements to emerge. For instance, in Syria, Yemen and Libya where governments control the media, military, police and other security agencies, organising social protests was a difficult task. In many cases, most organised movements or protests were crushed by the military, which lead to the emergence of political violence. However, the Egyptian case was different, as the channels of communication between the government and dissenting groups were reinstated, military forces were not directly involved in public protests and the organisation of protests were organised via social media. This situation did not continue for long as the Muslim Brotherhood conceded power in 2013 after a democratic election. As a result, new networking and communication tendencies have emerged.
2.3 Networking Tendencies and Political Polarisation During the Arab Spring Uprisings

The primary data collected by Shehabat (2015) during political turmoil in Egypt revealed that SMNs have evolved through four distinct phases: outrage and hope, instability and distrust, disinformation and criticism, and antagonism and hate (p. 17). As these phases have coincided with three waves of social unrest in Egypt, the power dynamics between civilian activists and the Egyptian government have changed. Castells (2013) proposed that social networks can be sites of ‘outrage and hope’. Nevertheless, Shehabat (2015) argued that social media has developed into ‘networks of antagonism and hate’. This argument is made after an empirical analysis of the Facebook datasets of Egyptian liberals and Islamists, which shows SMNs have become platforms of clashing ideologies. This clash of ideologies on social media platforms has resulted in the emergence of political polarisation. Guerra et al. (as cited in Brooking & Singer, 2016) defined polarisation as “the social process whereby a social or political group is divided into two opposing sub-groups having conflicting and contrasting positions, goals and viewpoints, with few individuals remaining neutral or holding an intermediate position” (p. 1).

For example, in Egypt, the rise of social media platforms enabled marginalised individuals, homophily groups, and religious and political ideologies to evolve. Therefore, the function of SMNs is to strengthen dispersed societies, groups of common interest and religious minorities within networks. Socialists, Islamists, communists, liberals and other religious minorities (e.g., Copts) have established their own networks through digital media technologies. These groups bonded together and challenged existing political structures

---

43 Homophily stands for the tendency of people to choose to interact with similar others (McPherson, Smith-Lovin & Cook, 2001, p. 435).
during first social movements in 2011 and then turned against one another during the second and third waves of social movement between 2012 and 2013. The occurrence of this social rupture was a result of media polarisation, orchestrated by military and other religious and political minorities to gain political status in the country. The mechanisms of social media platforms enable the quick and effective enrolment processes of more active nodes to the network. These new nodes rejected and challenged the existing structure of political movements within the networks. For example, during the first wave of social unrest in Egypt in 2011, nearly all aforementioned groups were bonded together, as they shared common grievances against the military government. However, these groups were divided in the aftermath of the first democratic elections that led to ultimate triumph of the Muslim Brotherhood political party. This bifurcation also appeared and was expressed in SMNs—groups started to attract followers by establishing Facebook pages that reflected their objection and thus, these groups initiated a new social campaign against the Muslim Brotherhood. That is, new networked social subgroups emerged on digital platforms first, and then infiltrated society.

To this end, as new networked political polarisation occurred during the second and third waves of the uprisings between 2012 and 2013 (Shehabat, 2015), the status quo that has previously united all Egyptian people (e.g., radicals, moderates, Copts, liberals and socialists) through ‘networks of outrage and hope’ (Castells, 2013) was challenged and transformed by the emergence of ‘networks of antagonism and hate’ (Shehabat, 2015, p. 7). These latter networks presented their own ideologies, resulting in the social and political chaos that unfolded in contemporary Egypt and the rest of the Arab world.
In Section 2.4, I discuss how social networking platforms shaped the political polarisation, bifurcation and mobilisation that led to information-centric warfare between subgroups from social networks and between subgroups and pro-government actors.

2.4 Political Polarisation and Mobilisation Logistics

In this subsection, I highlight the logistical role of SMNs, Facebook and Twitter, in the political and terror mobilisation and polarisation of social movements that changed the Arab world. To examine how polarisation and mobilisation function in a networked context, I analysed datasets of Facebook networks of both anti-government and pro-government Facebook pages (Shehabat, 2015). My analyses revealed that polarisation in Egypt occurred during the period of government control over mainstream media and the utilisation of social media platforms (mainly Facebook). While mainstream media acted as the gatekeeper of news production, the Egyptian Government aimed to control society through the dissemination of pro-government propaganda and messages of fear and intimidation. With that in mind, the digital divide, computer illiteracy, accessibility and affordability of the internet have made mainstream media a critical tool in shaping government sympathisers, especially lower-class populations, in which access to the internet is limited. My analyses revealed that mainstream media always has a great impact on the older demographic, who consider television to be the most credible source of news (Shehabat, 2015).

Another decisive factor that generated polarisation during the Egyptian uprisings was the framing of social networks as distributed systems. That is, the dynamics of Facebook networks translated and enrolled actors to the network. The process of adding additional actors to the networks generated affect. Affect enhanced social participation, by encouraging interaction with the narratives disseminated on social networking platforms. Gibbs (2007,
p. 130) argued that visual media can generate affective responses. For example, images of the Egyptian government’s brutality against peaceful protesters in Tahrir Square generated a sense of solidarity, brotherhood and sympathy for the protesters.

As a result, marginalised groups, homophilous groups and individuals established connections through the use of social media platforms has created networked environments. In other words, spontaneous responses to disseminated content over networked environments leveraged these networks. For example, the largest network responsible for sharing common grievances, which worked as a catalyst for the 25th uprising was the ‘We Are All Khaled Said’ Facebook page (see Figure 1). This Facebook page has 3.8 million members.

![Figure 1. ‘We Are All Khaled Said’ Facebook page. Source: facebook.com.](image)

The interaction of networked people through this Facebook page led to a speedy response to calls for public protests. The new networked environment created by the ‘We Are All Khaled Said’ Facebook page formed a space for subgroups, individuals and homophilous groups to network with other like-minded groups by exploiting tenuous commonalities. Facebook environments promote social interaction through the ‘share’, ‘comment’ and ‘like’ features,
which serve to strengthen weak connections of groups and individuals by presenting the responses and engagement of the wider audience concerning the political and religious ideologies represented. Therefore, Facebook created a unique environment for advancing political mobilisation and participation. McPherson, et al., argued that “information flows over social networks have localised the behaviour of homophily groups”. In other words, the dynamics of information, shared across social platforms enabled individuals to connect and interact with other social entities in an ecology of social forms (McPherson, Smith-Lovin, & Cook, 2001). Thus, the mechanisms of digital networks enhance collective participation. Studies on existing large-scale web systems have revealed power laws in content creation (Capocci et al., 2008; Panciera et al., 2009). Hence, it is reasonable to conclude that the rhythms of networked gatekeeping during uprisings and protests would also reflect the dominant influence of a select group of users (Meraz & Papacharissi, 2013, p. 143).

Twitter also played a significant role as a logistical aid in supporting and enhancing political polarisation and inspiring collective action against Arab governments. Homophilous groups, ideological minorities, liberals and anti-Islamic brotherhood were motivated by Twitter. The use of hashtags such as #Jan25 and #Egypt were the main hubs for millions of tweets and created narratives, which were shared across other platforms and news channels. Meraz and Papacharissi (2013, p. 157) observed that, journalists, activists and actors can exclude mainstream media and engage directly with the public through the sociotechnical architecture of Twitter. A networked flow of information and activity through crowdsourcing stimulates fragmented and pluralised storytelling to actor nodes, who then sent, received and remixed information (Meraz & Papacharissi, 2013, p. 157). Personal conversations are characterised by hashtags that become part of responsive system (Meraz & Papacharissi, 2013, p. 140).
Therefore, Twitter was an enabler for networked framing and gatekeeping (Meraz & Papacharissi, 2013, p. 158). That is, through socio technical processes of hashtagging, retweeting, liking and replying enabled by Twitter, the SMN facilitated individual and group participation in information flows, which then became part of framing and gatekeeping processes (Meraz & Papacharissi, 2013, p. 158). According to Meraz and Papacharissi (2013, p. 158), it was through these reciprocal processes that individual’s contribution and engagement in information flows lead to polarisation. Meraz and Papacharissi (2013) defined networked gatekeeping as a ‘process through which actors are crowdsourced to prominence through the use of conversational, social practices that symbiotically connect elite and crowd in the determination of information relevancy’ (p. 158). Twitter functions (e.g., retweet, reply, like) and hashtags shape the conversationality and flow of news streams on Twitter, giving voice to marginalised issues and people, especially in situations in which access to media is restricted, controlled or otherwise not accessible (Meraz & Papacharissi, 2013, p. 140).

Thus, Twitter afforded an ambient news environment through engendering and fostering network processes (Meraz & Papacharissi, 2013, p. 158). Within this context, Meraz and Papacharissi (2013, p. 158) proposed that the gatekeeping of the networked environment enabled ordinary users to create a measurable impact through practices that blend broadcasting with social conventions.

To this end, these networked forms of communication have an asynchronous and synchronous effect on shaping ideological and personal polarisation, which defined new phases of the social struggle for power. The use social media platforms created polarised environments and also reduced the number of gatekeepers that were controlled by
Authoritarian Arab governments. Digital networking mechanisms enable homogeneous personal networks to network, dissolve and establish ties with other similar networks, which enabled the emergence of new patterns of relationships within heterogeneous societies. An examination of hashtag frequencies and usage across the arc of a public event like the Egyptian uprisings can provide an insight into how hashtags function to negotiate the framing and counter-framing of an event, both substantively and affectively, over time. It is worth noting that social media platforms do not just enable communities to network, rather they determine networks. Social media platforms facilitate individuals’ connection to networks and make the network structure of society more noticeable (Rainie & Wellman, 2012).

Further, the utilisation of SMNs in Egypt engaged the Egyptian population in local politics. The democratic nature of social networks created a space for public participation by removing divisions based on social class, ethnicity, gender and religion. This has included the engagement of marginalised members of society in public discussions that have directed the political agenda towards the promotion of democracy in the Arab world. However, networking mechanisms of Twitter and Facebook during political uprisings have changed the dynamics of networking tendencies and incited information-centric warfare between pro- and anti-government groups and between religious and ideological groups by redefining former networks of outrage and hope as networks of antagonism and hate, which facilitated the emergence of networks of terror.

2.5 Networks of Outrage and Hope

During the political uprisings in Egypt, Facebook played a central role in political triumphs against the government. Prior to the waves of unrest in Egypt, the Egyptian regime had held

---

*An early version of this subsection has been published, see (Shehabat, 2015, p. 19).*
power through fear, brutality and torture. Facebook was significant in dismantling the fear barrier and subsequently, became a medium for the expression of outrage. As Castells (2013) wrote, “People overcome fear by being together, and they were [together] in the internet social networks and in the urban networks formed in the squares. But to come together in throngs they needed a strong motivation, a mobilizing force” (p. 81). According to Castells (2013), “[O]utrage induces fearless risk-taking and there was extreme outrage against police abuse, against hunger rising in the country and against the desperation that led people to immolate themselves” (p. 81). As such, hope “c[a]me from Tunisia, it showed that it was possible to topple an entrenched regime if everybody would come together and fight uncompromisingly, to the end, regardless of risks” (Castells, 2013, p. 81). The world came to know Mohamed Bouazizi45because his act of desperation was broadcast globally using SMNs and this sparked hope in people who shared common grievances and encouraged them to act against their oppressors. Therefore, in the first wave of social unrest in Egypt people depended on social networks to express their outrage.

From this example it is evident that Facebook activism during the first wave of social unrest in Egypt resulted in political change and shifted power to benefit the users of SMNs (Shehabat, 2015, p. 23). However, this success and happiness did not last, because counter-revolutionaries harnessed Facebook and other social media platforms to dismantle the social unity that had been created. According to Mark Lynch (2014):

Just those ‘18 days’ created a bond of shared sacrifice and struggle which washed away differences of class, ideology and generation. This bond, though, couldn’t

45 Mohamed Bouazizi is the cart vendor who sparked the Tunisian uprising by burning himself in 2010 to protest poverty and police abuses.
survive the return to normal politics and unfortunately revolutionary actions just
became part of the currency of the politics of power. (p. 2124)\textsuperscript{46}

Despite the events that have occurred since, it cannot be denied that for a period the dominant networks were those of hope and outrage, which triumphed and challenged the long-held power of the regime in the favour of the civilian activists.

Narratives relaying the role of SMNs in the Egyptian revolution have upset state–society relations and revealed an imbalance at the social level, which has split society at large. While SMNs have empowered individuals by creating a space for political debate and helped to organise political action—or what Castells (2012) called ‘networks of outrage and hope’—, these networks have created a struggle for power between social actors who have established new forms of networks to challenge existing networks, appealing to multitudes to challenge other multitudes, which has ultimately led to the emergence of ‘networks of antagonism and hate’. Thus, these power structures have created a chaotic public sphere; this is reflected in the structure of the SMNs that had a central role in restoring the power of authoritarianism, such as in the case of Egypt in 2013. Castells (2013) argued that “it began on the internet social networks, as these are spaces of autonomy, largely beyond the control of governments and corporations that had monopolized the channels of communication as the foundation of their power, throughout the history” (p. 2).

Just as social media has been used to promote democracy and justice, it was employed to engender disinformation, propaganda and persecution. This counter use of social media has resulted in the emergence of two opposing groups: Islamists and liberals. The virtual

\textsuperscript{46} This is a kindle location number.
interactions between these two groups has transformed the networks of outrage and hope into networks of antagonism and hate.

2.6 Networks of Antagonism and Hate

Antagonism and hate are common emotional responses expressed during social conflict and they serve the function of establishing and maintaining group identities. According to Simmel (as cited in Gilbert & Parent, 2004), conflict sets boundaries between groups by strengthening group consciousness and awareness of each group’s separateness from other groups. Simmel (as cited in Gilbert & Parent, 2004,) argued:

[R]eciprocal antagonisms between groups preserve social divisions and systems of stratification. The distinction between one’s own group and outsiders is established in and through conflict. This includes conflicts between classes, nations, ethnic groups, and political parties. (p. 164)

The second wave of social unrest in Egypt (in 2012) has been marked with the emergence of a new tendency towards a fascism and extremism in opinion that Shehabat (2015) called ‘networks of antagonism and hate’ (p. 26). The transformation of networks of ‘outrage and hope’ into ‘networks of antagonism and hate’ divided the power between social actors and led to a second military coup on 3 July 2013. That is, ‘networks of antagonism and hate’ have emerged and replaced the ‘networks of outrage and hope’ as the Facebook landscape shifted to engage Egyptian community in the political struggle between seculars and Islamists.

47 An early version of this section was published, see (Shehabat 2015, p.26).
The difference between antagonism and hate is that antagonism is ‘active’ and thus, it often involves killing, while hate is expressed in people’s hearts. Since January 2011 protest, these social behaviours have been expressed in the Facebook pages of the revolutionaries and the counter-revolutionaries through the expression of social, class, ethnic and religious beliefs. Fahmy El-Howaydi, an Egyptian political analyst and columnist, called the year 2013 ‘the year of hate’ (Al Jazeera, 2013). In his weekly column for Al Jazeera Arabic, on 24 December 2013, El-Howaydi (as cited in Shehabat, 2015) wrote that “in the modern Egyptian history I didn’t find a paradigm to describe the current social and political divisions that split the society aiming to eradicate and destroy the other as I see today” (p. 26).

In deeming 2013 a year of hate, el-Howaydi (as cited in Shehabat, 2015) explained that this claim specifically referred to the degree of media polarisation that had arisen and was poisoning the minds of the Egyptian public. This hatred eroded the social ties that once existed between Egyptian civilian activists. In his column, el-Howaydi continued to outline the motives and the characteristics of this hate. He indicated that media platforms have supported campaigns of hatred against politically different groups (el-Howaydi, as cited in Shehabat, 2015). For example, he highlighted how opposition and disapproval had been expressed through the abuse of Copts and Shiites. The events of the third wave of social unrest are yet to end. As such, antagonism and hate continue to dominate the Egyptian media landscape. However, in Iraq and Syria political violence changed the dynamics of digital activism into a bloody struggle. The new struggle was reflected by parties of conflict through their digital activism. Images of beheadings, burnings, burying, drownings and shootings were disseminated on social media platforms. Since 2013, a paradigm shift has occurred in utilising social media platforms. That is, more Facebook pages, Twitter feeds and YouTube videos have been harnessed to promote terror.
2.7 Networks of Terror

As noted in sections 2.4 and 2.3, during waves of political turmoil in Egypt, SMNs were utilised by secular groups, homophilous groups, liberals, religious minorities and Islamists. However, the role of SMNs during the Syrian and Iraqi revolutions have entered a new phase of development. A new paradigm of political communication has emerged as political violence erupted in both countries. This new paradigm was formed by two factors:

- The social media cyberwar during the Syrian revolution.
- The emergence of terror networks during the Anbar uprisings, until the emergence of ISIS.

For each of these factors, I outline the transformation of SMNs, as instigated by revolutionaries to share grievances and facilitate political mobilisation, prior to the emergence of ISIS networks that promoted terror and spread fear through the world at large. To do this, I examine the role of SMNs during the political unrest in Syria and Iraq. The significance of this study is that ISIS terror networks were born from these uprisings.

2.8 Syrian Case Study\(^{48}\)

This subsection is focused on presenting a deep understanding of the pervasiveness of SMNs during the Syrian revolution. This section explores how Syrian rebels and pro-government individuals and organisations used information-centric warfare in the period prior to the eruption of political violence and the rise of ISIS’ terror organisation. In this case study...

\(^{48}\) An early version of this case study has been published, see (Shehabat, 2012).
study, I discuss digital activism and digital conflict between the Syrian Free Army (SFA) and the Syrian Electronic Army (SEA). I analyse the events of the Syrian uprising by focusing on the communication tools used by the rebels. In this case study, I examine closely at social media cyber-attacks, disinformation, propaganda and surveillance, as used by both the SEA and SFA to win the online front—an operation that is having a significant impact in battles on the ground.

2.8.1 Social Media Warfare—Syrian Free Army versus Syrian Electronic Army

The Syrian political uprisings—first instigated on 15 March 2011—facilitated a demand for freedom and political reforms. In early 2011, social media platforms had already been used to accelerate the downfall of both the Ben Ali and Mubarak regimes in Tunisia and Egypt, respectively. The Syrian Sunnies had been inspired by the ultimate triumph of the Tunisian and Egyptian uprisings, which had resulted in political change and the promotion of democracy. This uprising was uniquely characterised by the information-centric warfare that emerged as both the Syrian government (led by the SEA)\(^{49}\) and the Syrian rebels (led by the SFA) utilised digital media networks to represent acts of political violence. The involvement of hackers, misinformation, propaganda and digital surveillance on both sides of the conflict resulted in the first social media cyberwar, during the Arab Spring uprisings (Shehabat, 2012). My reflections are based on a close monitoring of SEA and SFA Facebook pages,

\(^{49}\) SEA described itself in its Twitter account, “We are not an official side and do not belong to a political party. We are Syrian youths who responded to the call of duty after our homeland, Syria, was subjected to cyber-attacks. We decided to respond actively under the name of Syrian Electronic Army SEA’ (SEA, 2013).
YouTube channels, Twitter feeds and other resources, such as news articles and satellite channels.

In this case study, I explore how Syrian activists have harnessed multiple communication technologies as the logistical means for war, including social media platforms (such as Facebook, YouTube, Skype and Twitter) and mobile phones (SMS, recorded video and live streaming) to achieve their aims. Namely, Syrian activists desired to expose the Syrian government’s brutality to the world, communicate with other rebels, create digital communities across the country, spread propaganda, coordinate military attacks, and disseminating news and information about the uprising.

2.8.2 Digital Logistics of the Syrian Uprising

The snowball effect of uprisings occurred in Tunisia and Egypt in 2011 has shaped protests in Syria. Protesters’ used SMN’s and other communication tools such as Skype and Mobile phones to document and promote their uprising. The high level of mobile phone use in Syria also played a pivotal role in publicising the government’s brutality (Shehabat, 2012). The incidents in Daraa and Homs were recorded and uploaded onto YouTube and broadcast worldwide. This was in stark contrast to the events of February 1982, when Hafez Al-Assad (the father of President Bashar Al-Assad) ordered a massacre in Hama following the rise of the Islamic Brotherhood in the province.

In Hama in 1982, local and international media were banned from documenting events. However, in Daraa in 2011, the killing of the 13-year-old boy, Hamzeh Al-Khateeb, provoked international outrage after his battered and tortured body was shown on a YouTube video. This event marked the first outbreak of active dissent on the internet within Syria for
decades. Syrian activists turned to Facebook, Twitter, and other internet tools (such as Skype and Yahoo Messenger live stream) to broadcast news and information about the uprisings. The first Facebook group page established to spread the word of the revolution was ‘We are all Hamzeh Al-Khateeb’. This page mimicked the famous Egyptian Facebook page ‘We Are All Khaled Said’, which had sparked the call for political mobilisation on 25 January 2011—an important turning point in Egyptian history.

In response to this social media activism, the Syrian government hindered the rebels’ information loop by disabling of mobile phone and internet connections in Daraa and Homs. As such, the communication tools of social media remained critical for the rebels. To restore communication technologies between rebels in Syria, proxy modems, satellite phones and international mobile phones SIM cards were smuggled in from neighbouring countries. Shehabat (2012) recounted that in southern Daraa, which is only few kilometres away from the Jordanian border of Ramtha, Jordanian mobile phone SIM cards were used by rebels to reconnect; in northern Idlib, Turkish mobile phone SIM cards were used (Shehabat, 2012, p. 3). Smartphones and the 3G wireless internet have also been a significant tool for the rebels; these technologies were so valuable that the Syrian government banned the use and import of iPhones into the country (BBC, 2011). Al-Thuraya Saudi satellite phones, powered by the Saudi Telecom Company, were used to report news to international satellite channels, such as Al Jazeera and Al Arabiya. Technologically savvy Syrians resumed their internet activism by using dial-up connections and proxy internet modems (Shehabat, 2012, p. 4). Freedom House (2015) reported:

Authorities prevented foreign media from accessing the situation on the ground, prompting many ordinary Syrians to take up mobile phones and small cameras to cover the deteriorating situation and post videos on social media. These citizen
Journalists have become vital in the quest to document flagrant human rights abuses by all parties to the conflict. (p. 2)

Social media had an influential role in the early stages of the uprisings. Notably it has shaped and brought Cyber communities into existence. Build solid alliances between communities and sustain flows of information. An example of cyber communities existed during the Syrian conflict was the Local Coordination Committee (LCC)\(^{50}\). Johnston indicated that over 70 (LCCs) initially existed to document the Syrian revolution, which then became coordinating protests and information disseminators (Johnston, 2017, p. 79). LCC’s mission also included keeping a count of the number of killings, diffusing propaganda and reporting to international agencies. The LCC was productive in spreading fear among Assad’s military and in facilitating defections.

The use of SMN’s in documenting the Syrian government brutal actions used against the rebels resulted in the divisions between communities that formed the Syrian Arab Army (SAA). Knowing that the majority that SAA consists of is the Sunni and other religious minorities such as Alawite, Druze, Christian and Ismaili sects. In other words, the SAA is a heterogeneous network of different actors. The defection of some Sunni soldiers in the Syrian Arab Army (SAA) led to the establishment of the SFA. Dryan Lee indicated that “The SFA was formed as a decentralized armed force that incorporated a diverse range of actors including local self defence units, defectors from the military, Islamists, and foreign fighters” (Lee, 2016).

\(^{50}\) As a digital community, this can be one person operating in another country. His job is reporting through the (LCC) website and Facebook page.
Therefore, SMN’s have been influential in mobilising public opposition amid a militarised uprising. Daily street protests in most of the country’s streets have been orchestrated and synchronised via Facebook pages and Twitter feeds. The use of hashtagging—particularly #Syria—has contributed to the coordination of protests and engaged the world press in events. It has been reported on Al Jazeera’s (2012) satellite News-hour program that over 600 street demonstrations, which were organised by social media platforms, broke out in one day. The vulnerability of use of SMN’s as weapons which enabled rebels to carry out information operations, information warfare and built its strategic narrative have forced the Syrian government to tighten its grip on internet usage by applying filtering and censoring technologies to closely monitor internet content that could potentially destabilise the government.

Ironically, in June 2011 in the middle of the uprisings, the Syrian government restored Facebook and YouTube. The government aimed to track activists, capture them and steal their usernames and passwords to spread propaganda, dismantle communication networks and to gain information about the social movements’ plans for pre-emptive strikes. This move by the government reflected Morozov’s (2012) theory of net delusion, wherein he argues that information technologies are in the hands of authoritarian regimes, not activists. As Morozov (2012) stated, “The internet may favour dictatorships rather than democracies” (p. xiii). To hamper the efforts of social media activists during the 2011 uprisings, the technologically savvy employees of the Syrian government have applied many strategies to paralyse information diffusion, hunt activists and destroy communication channels. These have included setting up a fake YouTube, Facebook interference, Skype encryption and others acts of information warfare.
2.9 The Fake YouTube

YouTube has been cited as an important platform in the Arab Spring uprisings, particularly in Syria. It has aided revolutionaries in many ways. First, it highlighted the governments brutality by documenting events via mobile phone technology, which led to the expansion of the geographical proximity of the uprisings by raising awareness among the Sunni sect. Second, it worked as the alternative press: an informative platform that disseminated information to most of the world news outlets. Finally, it captured tangible evidence of Assad’s crimes against his people. According to Alex Fitzpatrick (2012), “The world is watching the Syrian uprisings on YouTube”. The battered body of the 13-year-old Hamzeh Al-Khateeb was the first video uploaded on YouTube that showed the government’s ruthlessness. Those trying to view the video found a message saying, “This video has been removed as a violation of YouTube’s policy on shocking and disgusting content” (Melber, 2011). YouTube has posed a major threat to the government’s propaganda and stability. In revenge, the SEA cloned the YouTube website to trap Syrian digital activists (see Figure 2). However, the fake YouTube page attacks users in two ways. First, it requires you to enter your YouTube login credentials to leave comments. Second, it installs malware disguised as an Adobe Flash Player update (EFF, 2012), so that the attacker can control a computer’s contents.
2.10 The Facebook Interface

Facebook was considered the second most important social media site that the revolutionaries relied on to expose the Syrian government. The government has allowed Facebook to remain available for trapping Syrian activists. Syrian activists have harnessed the potency of Facebook pages in recruiting, coordinating and diffusing information to local and worldwide audiences. The most compelling Facebook pages have been ‘We are all Hamzeh Al-Khateeb’, the ‘The Syrian Revolution 2011’ and ‘Euphrates Revolution Network’. The ‘We are all Hamzeh Al-Khateeb’ Facebook page was shut down by Facebook administration on 30 August 2012, but restored on 2 September 2012 after a message was sent by the page administrators outlining the page’s purpose:

Dears Messrs [,] We demand that the respectful Facebook management return the page of the child martyr Hamza Al-Khatib (more than 500,000 fans) that have [sic] been deleted today, despite of being a great reference in publishing what really happens in Syria for the public opinion, press and human rights organisations and humanitarian [sic]. We ask you in the
Facebook pages that were established by dissenters and revolutionaries were directly targeted by the SEA to be reported as spam. The Facebook login page within Syria is ‘www.leged-rein.org’; a similar link was visible on revolutionaries Facebook pages, with prompts asking users to post and share ‘good news’ (see Figure 3). However, using this link would cause huge damage. According to the Electronic Frontier Foundation (EFF, 2011), this attack steals usernames and passwords and could potentially give an attacker access to all private information in your Facebook account.

The SEA may not be the only pro-government faction meddling with Facebook’s operations in Syria. In early May, mysterious forces staged a man-in-the-middle attack, wherein Facebook users who attempted to log in to their accounts were redirected to a fake Facebook login page. This allowed the attackers to harvest logins and passwords, giving them the ability to monitor and control those accounts. The attack targeted Facebook’s encrypted HTTPS version, and made use of forged security certificates.

![Figure 3. screenshot of Fake Facebook interface page. Source: The Atlantic (2011).](image-url)
2.11 Skype Encryption Tools

Skype has been an important tool for Syrian revolutionaries as it enables live reporting, especially to Al Jazeera satellite channel. Skype has also been important in facilitating communication between the coordination revolutionary divisions. As a result of this, the EFF (2012) reported that Skype has been directly targeted by the regime with a Trojan called DarkComet (RAT). The Trojan allows an attacker to capture webcam activity, disable notification settings for certain antivirus software, record keystrokes and steal passwords. It sends the collected sensitive information to the same Syrian IP address used in the attacks (Galbren et al., 2012).

Villeneuve (2012), senior threat researcher at Trend Micro, discovered a web page that advertises a software that purports to provide encryption for Skype. According to Villeneuve (2012), this page is hosted in Syria on [BLOCKED]encription.sytes.net and includes an embedded YouTube video that claims to be from an IT security laboratory to encrypt voice communications (see Figures 4 and 5).

![Skype encryption tool run by the Syrian Electronic Army. Source: Security lab 2012.](image)
2.12 Social Media Networks: Information-Centric Warfare

In their book, *Cyber War*, US government security experts Clarke and Knake (2010) defined cyberwar as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption”. In the Syrian case, there are three levels of information cyberwar waged. The first is the cyberwar between state and foreign organisations, such as the Al Jazeera satellite channel and Harvard University. The second form of cyberwar is the state versus individual actors, at both local and international levels. On 15 March 2011—the day the Syrian Sunnis demonstrated in Daraa demanding reforms and liberty—resulted in a truly sectarian war. Additionally, the army, which has been called *Humat el Dyar* (i.e., the protectors of the land) has also divided into sub-groups engaged in political and military conflicts. Finally, the third form of cyberwar was between foreign organisations and the state. Hacktivist groups, such as Anonymous and Telcomix, have themselves attacked the Syrian government, but they have also supplied information technologies to enable the revolutionaries to attack the Syrian government information resources. Thus, a massive social media virtual war is being carried out between the SEA and SFA to win the media war.

---

51 Attempts to use these links will lead to Syrian attackers to be in control of this communication.
SMNs have played a vital role in the protest movements that have taken place since March 2011. The revolutionaries’ coordination groups have established Facebook pages, Twitter accounts and YouTube channels so that they can communicate, coordinate and disseminate news and videos. The most powerful networks are ‘The Syrian Revolution 2011’ Facebook page (over 504,000 likes) and @revolutionsyria on Twitter (approximately 49,500 followers). As the battle on-ground escalated, so did the online frontier. The SEA launched an aggressive attack on the SFA Facebook pages, posting pro-Assad comments and reporting it for spam to Facebook administration. The SEA initially succeeded in shutting down ‘The Syrian Revolution 2011’ Facebook page, but it was later restored after contacts with Facebook administration. As such, #Syria has been targeted by TH3 Pro, the SEA special operations department who post pro-Assad tweets, but Twitter administration intervened and removed all comments posted by TH3 Pro (Shehabat, 2012).

In retaliation, the SEA Facebook page was reported for spam by the SFA. In a plea posted by the SEA, in which they asked for support to evade a shutdown by Facebook administration, the SEA urged sympathisers to join and post supportive comments. The SEA managed to retrieve the page under a different name, ‘Al-Nidal Al-Sory’ (i.e., struggle for Syria).

Shehabat (2012) has monitored the attempts of the SEA to establish new Facebook pages. The SEA moved their Facebook hacktivism in a different direction by targeting some of the world’s most prominent figures, media outlets and educational organisations who have been publicly supporting the freedom fighters. The SEA has since launched coordinated attacks on Facebook and Twitter directed at the Facebook pages of Harvard University (see Figure 6), The Independent newspaper (see Figure 8) and the US former president Barack Obama (see Figure 7). Comments such as those by Mais Latif, ‘leave us alone, we love Bashar’, and
Kamal Ibrahim, ‘please stay away from us […] we love Syria’, are typical of the many hundreds of comments directed to Obama, Winfrey, Sarkozy and others.

![Figure 6](https://example.com/harvard-hacking.png)

**Figure 6.** Screenshot of the hacking of Harvard University website by Syrian Electronic Army.


![Figure 7](https://example.com/obama-hacking.png)

**Figure 7.** Screenshot of the hacked Facebook page of Barack Obama. *Source:*

100
Figure 8. Screenshot of hacked The Independent by Syrian Electronic Army. Source: www.theregister.co.uk 27/11/2014.

Overall, SMN’s played a critical role in shaping of information warfare occurred between the Syrian government and rebels. This allows non-state actors to vigorously participate and have a meaningful impact in cyber warfare. Part of information operation carried out by some rebel groups such as Khalid bin Al-Waleed group and Al-Nusrah front that sheds light on Sunni-Shitte- Alawite divisions to recruit more Sunnies. Such groups highlighted Shitte and Alawite atrocities against Sunnies which frustrated Sunnies. This has changed the uprisings from a Syrian uprising to a Sunni insurgency. As Johnston (2017) puts it, “The violence of the Syrian uprising transformed Islamist speech from an uprising of the Syrian people to an uprising of Sunnis to fight the Syrian “Alawite” regime” (p.86). This tendency explains how ISIS became a game player in Syria after declaring Caliphate in 2014.

2.13 Iraq Case Study—Anbar Uprisings

52 Now known as Hayat Tahrir Al-Sham (HTS).
Nearly two years after the spark of the Tunisian revolution, the Anbar uprising began in July 2012. It was known as Anbar uprisings, not Iraq uprisings, as the protests only took place in the Anbar Province (northern Iraq). Anbar Province is a Sunni stronghold, which is also inhabited with other ethnic and religious Iraqi minorities, such as Kurds, Turkmans, Yazidi and Christians. Muslim Sunnis started to protest marginalisation, corruption and political exclusion by the Shiite government, ruled by Nouri Al-Maliki. The government’s arrest of the bodyguards of the moderate Sunni finance minister, Rafi Al-Issawi, in December 2012 led to widespread peaceful protests in Sunni provinces in northern and central Iraq (Katzman, 2013; Wicken, 2013). At first, the demonstrations were well-attended, with protesters demanding an end to political, civil and economic discrimination against the Sunni community (Sullivan, 2013).

However, the Anbar uprisings cannot be disconnected from the Syrian uprising. As such, political violence erupted in Syria as Sunni tribes of Iraq and Syria were geographically connected. As Al-Amin (2014) puts it:

There is a solid relationship between the uprising in Syria and uprising in Anbar even if the pragmatic aspect of this relation is limited to the citizens of Anbar receiving their cousins as refugees from Syria and sending their fighters to join the forces of the Syrian opposition.

To understand the connections between the Sunni insurgency in both Syria and Iraq and how IS fighters involved in the political violence erupted in Syria in the period between 2011-2014 a study of the influence of Al-Qaeda is to be addressed. In 2013, Al-Baghdadi nominated Abu Mohammad Al-Julani to establish the Al-Nusra front to lead Islamists against
Assad forces in Syria. Before the emergence of Al-Nusra, Abu Bakr Al-Baghdadi (who became Caliph Ibrahim) called his jihadist group ‘ISIS’. Hazem Al-Amin (2014) observed:

As clans in Anbar send their fighters to stand by their beloved ones against the regime forces in Syria, the ‘Anbar rebels’ adapt in their protests with the rebels of Syrian cities at a time when modern communication means, such as Facebook, Twitter and YouTube, helps clans along both sides of the border communicate, cancels what modern countries’ borders have severed regarding ties and restores wefts to the clan, its sheikh and its values.

According to Internet World Stats,53 in 2012, nearly 2.2 million Iraqis had internet connection, which equates to a penetration rate of approximately seven per cent of the Iraqi population. Despite the low internet penetration and participation in Iraq, Facebook was the most popular website in Iraq; however, its users were few in number (Al-Rawi, 2014; Berger & Perez, 2016, p. 10). According to Al-Rawi (2014), “Iraqi Facebook pages received much less attention. A survey of the most popular Facebook pages during the Arab Spring in Iraq revealed that most pages were established in early February 2011 and carried an obvious secular orientation”. The most popular Facebook page was ‘Support the Iraqi Youth Revolution’ (http://www.facebook.com/Supportiraq); it had more than 130,350 followers and was established on 9 February 2011. Its profile stated: “The Iraqi Revolution is a revolution to support the right in the face of injustice, corruption, and tyranny. The aim of the Iraqi Revolution is to eradicate Iraq from the corrupt people, occupation and its agents” (Al-Rawi, 2014).

However, Facebook activism was not used by grassroots movements alone. Iraqi insurgents were among the first active internet users because they needed to spread propaganda on their activities, gather popular support and seek funding. Several pan-Arab television channels, such as Al Jazeera and Al Arabiya, made use of the videos and announcements posted online by Iraqi insurgent groups to cover the events in Iraq (Berger & Perez, 2016, p. 6). Maliki’s government used several mainstream media outlets to discredit the cause of the protesters, by calling them ‘Al-Qaeda followers’ and ‘Saddam Hussein sympathisers’ (Berger & Perez, 2016, p. 21).

Maliki suspended the licenses of 10 television channels that criticised his crackdown on protesters who allegedly incited violence (BBC News, 2013). Once more, activists bypassed the government’s news blackout by posting updated information regarding the protests on Facebook and YouTube. Due to its widespread availability and use of SMN’s, the Iraqi government can no longer suppress public anger by means of controlling traditional media outlets (Berger & Perez, 2016, p. 21).

However, the rise of ISIS as a game player in Iraqi politics occurred after they took control of Mosul city on the 10th of June 2014. Under the leadership of Abo-Baker Al-Baghdadi, ISIS has become very organised as it managed to form its political structure by creating Islamic institutions (known as Dywan) such as, Dywan of education, Dywan of Hesbah (markets) and Dywan Al-Zakah (charity). It also, invested in creating of media outlets and information centres to carry out its information operation and to inform residents. Patrick Cockburn (2016) observed that “Its propaganda films frequently show non-Sunni Muslims being executed and its reputation for savagery may have helped demoralise the Iraqi security forces in Mosul”. The fall of Mosul has encouraged ISIS to control of Sunni strong hold territories
such as Diyala, Tikrit, Salahuddin and Anbar. However, after the fall of Mosul ISIS spokesperson abo-Mohammad Al-Adnani calls on ISIS fighters to be humbler. In his words “Do not let your egos fall prey to your recent military gains such as the Humvees, helicopters, rifles and military equipment”. Cockburn (2016) suggested that the speech is “interesting and significant because Adnani gives the first insight into how ISIS views its stunning territorial gains as well as its intentions in the immediate future”.

However, during the year 2014, ISIS strategy depended on spread of fear to gain territorial control. Adnani speeches were aimed at conquering of Baghdad. To spread fear among Muslim Shia, ISIS documented its biggest massacre of Shia army recruits in Speicher. On 12th of June 2014 ISIS released a video depicting the execution of 1700 Iraq recruits from Shia sect captured on camp Speicher. To maintain the morale of people in Baghdad, and to supress ISIS’ information operation the Iraqi government has shut down the internet and closed Facebook, YouTube, and Twitter (Cockburn2016). The shutdown of the internet however, created a sphere of panic and confusion in Baghdad. As Cockburn (2016) who claimed that the internet shutdown is creating a vacuum of information filled by frightening rumours that are difficult to check. The result is an atmosphere of growing panic in Baghdad with volunteers from the Shia militias being trucked to Samarra, north of the capital, to stop the ISIS advance.

---

54 Speicher is a military base near the Iraqi city of Tikrit.

55 The video is available on liveleak.
To this end, the military advances of ISIS and its brutality against other minorities depicted in its video releases resulted in the emergence and mobilisation of networked militants from different ideological sects. Although the year 2014 was marked with the proliferation of ISIS’ IO strategy, after the declaration of caliphate, ISIS has pushed the boundaries of its IO strategy to become more sophisticated.

2.14 Conclusion

In this chapter, I described the usage of social networks during the Arab Spring uprisings. I have argued that utilisation of SMNs by Arab revolutionaries have been subject to three major transformations in years between 2010 and 2013. That is, these networks were praised for their key role in challenging the political structures of some Arab governments and thus, were hailed as networks of outrage and hope.

However, this dynamic changed as subgroups opposed the outcome of democratic elections that led to the success of Islamic political parties (such as Ikhwan). These subgroups bifurcated social fabric (especially Egyptian society) and as a result this era was marked with the emergence of networks of antagonism and hate. In Syria and Iraq, sectarian war erupted between Sunni, Shiite and Alawite sects. As a result, a new wave of terror networks emerged. Al-Qaeda, Al-Nusra front and ISIS actively harnessed SMNs and other media environments to execute their IOs to achieve their political agendas.
3 Chapter 3: ISIS’ Information Operations—A Strategic Narrative Perspective

3.1 Introduction

The purpose of this chapter is to understand the complexity of ISIS’ IO\(^{56}\) and its objectives. This includes their tools of influence warfare,\(^{57}\) the use of multiple digital environments, the techniques of HD production, strategic narrative themes, propaganda and information warfare. The aim of this chapter is to create a conceptual framework to understand ISIS’ strategic narrative. Additionally, it is important to understand the role of ISIS affiliates and members in information aggregation, dissemination and generation. To do that, I applied thematic analysis to media produced by media wings and individual affiliates of ISIS networks. These themes were depicted mostly in HD video productions and digital magazines, such as \textit{Al-Naba},\(^{58}\) \textit{Dabiq} and \textit{Rumeyah}.\(^{59}\) To understand the conditions that surrounded and affected their information processes, it is essential to highlight the diversity of ISIS individuals (Ba’athists, jihadi from around the globe and local residents of Iraq and

\(^{56}\) The definition is provided in the introduction chapter on p.3.

\(^{57}\) As suggested by professor James Forest.

\(^{58}\) An Arabic version of the magazine produced by ISIS’ Al-Hayat media centre. It is widely shared on Justpase.it and Telegram channels as PDF files.

\(^{59}\) \textit{Dabiq} was the first ISIS produced magazine to communicate to non-Arabic speakers, with high-quality images, professional layout, and writing. It first appeared in 2014 and changed to Romyah in 2016. There is a political significance behind the change of its name. That is, Dabiq, according to Hadith of Prophet Mohammad, that great battle will occur between Kuffar (infidels) and Muslims in place called Dabiq (near Aleppo north of Syria). While Romyah which means Rome where also prophet Mohammad foretold his companions that it will be conquered by Muslims. The political message here is that ISIS planned to carry out its military operations in the West.
Syria). ISIS’ information strategy was amplified by their alliance with other global terror organisations such as Al-Qaeda, Boko Haram (Nigeria), Abu Sayyaf (Philippines) and Al-Shabaab (Somalia). Media wings had a critical role in shaping the information strategy, as every media outlet specialised in aspects of media production.

This chapter aims to explain the role of narratives in the IO strategy of ISIS networks within globally interconnected media environments. In this chapter, I briefly outline the political and religious aims of ISIS. Second, I explain the objectives of ISIS’ IO strategy. Third, I highlight the roots of ISIS’ IO and its strategic narrative to achieve its political and religious agendas. I analyse many elements of the ISIS narrative and how it served its political agendas. Finally, I examine the effects of the ISIS narrative on recruitment and radicalisation.

### 3.2 ISIS’ Organisational Structure, Politics and Religious Aims

As explained in the Background chapter of this thesis, ISIS was born from AQI, which responded to the US’s war on terror and occupation of Iraq in 2003. This subsection will highlight the political structure of ISIS, its origins and religious aims. ISIS’ religious aims must be considered because they are inherently connected with their political aims, as exemplified in the establishment of a caliphate. Declaring a caliphate required huge resources, such as logistics, new recruits, political structure and agenda. To execute its IO strategy, ISIS has adapted sophisticated narrative themes to garner support from Muslims around the world. To gain support from zealous Muslim youth, ISIS utilised and adapted Al-Qaeda’s pre-existing political structure, media wing and IO strategy by adapting Al-Qaeda’s political and religious ambitions, which has been inspired by Osama bin Laden’s vision to re-establishing an Islamic caliphate, ISIS swiftly achieved their objective and declared an Islamic caliphate in July 2014. However, ISIS’ separation form Al-Qaeda and the declaration
of Islamic caliphate created confusion among Al-Qaeda loyalists and other jihadi who questioned the legitimacy of new Islamic caliphate. The establishment of the Islamic caliphate bestowed ISIS a superiority over its original roots, Al-Qaeda. Abu Bakr Al-Baghdadi, as the instigator of Islamic caliphate, asked Al-Qaeda loyalists to pledge allegiance to Islamic caliphate and to offer him bay’ah as Caliph. The split between the Al-Nusra front and ISIS was as a result of Al-Qaeda’s leader, Sheikh Ayman Al-Zawahiri, denouncing the legitimacy of Al-Baghdadi. The decision of Al-Nusra to keep its loyalty to Al-Qaeda led to a military confrontation between ISIS and the Al-Nusra front in 2013.

Despite their conflict, it is important to mention that the common vision between Al-Qaeda and its new rival ISIS—despite the religious and political divide—was the establishment of an Islamic caliphate. This state must be ruled by a true Muslim leader (a caliph), who would appoint a Shura council60 to govern the Muslim world based on teachings of Qur’an and Sunna of the Prophet Mohammed. According to Osama bin Laden, this vision can be achieved through declaring of global jihad against Western invaders. To recruit jihadi and inspire Muslims around the world, bin Laden invested in three main narratives: grievances, utopian society and jihad. Schmid (2014) noted that a basic grievance bin Laden stressed upon in his speeches was that “the Muslim world is in chaos because of a Zionist–Christian alliance. This alliance is responsible for most, if not all, that is wrong in Muslim countries and the way Muslims are humiliated, discriminated and mistreated in the world” (Schmid, 2014, p. 6). To restore the dignity of Muslims, ISIS spokesperson Abu Muhammad Al-Adnani (as cited in Ingram, 2015) asserted:

---

60A small number of advisory committees to advise the Caliph when taking a political decision.
So rush O Muslims and gather around your khalifah [caliphate], so that you may return as you once were for ages, kings of the earth and knights of war. Comes o that you may be honoured and esteemed, living as masters with dignity. (p. 743)

For Al-Qaeda, the only way to restore dignity and achieve victory against the Zionist–Christian alliance was by declaring global jihad. As Schmid (2014) stated, “Every true Muslim has to engage in a holy jihad against the invading Crusaders to defend the faith and the Muslim lands from enemies near and far in order to achieve victory and humiliate the oppressors” (p. 6). Additionally, Al-Qaeda created a vision of the good society (Schmid, 2014, p. 6). In this vision for society, political structure depended on “a single political entity—the caliphate—that replaces corrupt, apostate rulers under Western influence, by rule under sharia (Islamic Law) wherever there are Muslims so that Allah’s will be done and order is restored” (Schmid, 2014, p. 6).

Since their establishment, ISIS has borrowed this same strategy, but invested more in creating a similar media narrative to achieve its political agendas. The first step to establish its caliphate was to build a solid political structure to enforce governance and supremacy (see Figure 9).
This political system was based on the sovereign authority of its caliph, who has the power to enforce sharia law for the purposes of controlling society. This vision was depicted in a propaganda publication entitled *This is the Promise of Allah* by the Al-Hayat Media Centre. The publication provided information about the future plans of the organisation and gave an indication of goals of the Daesh [ISIS] information strategy’ (Strategic Communication Centre of Excellence [StratCom], 2015, p. 4). To this end, ISIS adapted a sophisticated IO strategy that utilised HD video production techniques to execute well-constructed narratives to achieve its political agendas.

### 3.3 The Strategic Deployment of High Definition Productions

As argued in Chapter 2, since the rise of the Arab Spring uprisings, the utilisation of SMNs by Arab revolutionaries has changed dramatically. The dynamic usage of social networks has highlighted governments’ cruelty against civilians and has catalysed for political mobilisation but has also evolved into a tool for promoting fear and terror. The events of the Iraqi and Syrian uprisings shifted to a sectarian war, followed by rise of the Al-Nusra group in Syria.
and ISI, who both pledged allegiance to Al-Qaeda. These terror organisations strategically harnessed SMNs and other dissemination tools reliant on internet technologies. Ultimately, ISIS and its supporters utilised many means of ICTs and SMNs to spread its message, promote its ideology and maintain its network structure and connectivity. For this purpose, ISIS realised the significance of establishing a ministry of information to control and direct messages to serve its ambition: establishing an Islamic caliphate under the motto of ‘remaining and expanding’. Schmid and Janny de Graaf (1982, as cited in Architte, 2012) famously argued that “terrorism is communication: for the terrorist the message matters, not the victim” (p. 29). This appears clearly in type on messages produced by ISIS. The versatile of producing messages depicting violence and brutal scenes, ISIS aims to get attention to enlarge its audience base. That also explains how their message was mediated so quickly as mainstream media collaborated in disseminating of some videos that depicted brutality. For example, in January 2015 FOXNEWS broadcasted 2 minutes of the burning of the Jordanian pilot. It also kept the ISIS video on its website for a few months.

However, ISIS attracted unprecedented media attention on 19 August 2014 after it produced its first beheading video titled Message to America. The 4.40-minute video captured the speech of both the US photojournalist James Foley and the United Kingdom (UK) ISIS jihadist, Mohammed Emwazi.\textsuperscript{61} In this video, ISIS utilised what are arguably professional tools of media production, including high-quality cameras, multiple angle screenshots, professional montage and use of sound devices. Overall, this marked the first time a terror organisation had produced high-quality video through its own media outlet (Rose, 2014), giving an indication of ISIS’ production sophistication and ability to harness new tools of

\textsuperscript{61} ISIS member from the UK known as Jihadi John.
dissemination. Before this, media reported two accounts of beheading videos produced by Al-Qaeda in 2002 and 2004. Daniel Pearl and Nick Berg appeared in Al-Qaeda’s unsophisticated video productions; Al-Qaeda operatives used single analogue (i.e., VHS) camera in uncut scenes of the beheadings. The videotape was sent by mail to Al Jazeera satellite channel.

Unlike the unedited Al-Qaeda videos that preceded it, for the first time, a terror organisation produced sophisticated HD, vivid images. The significance of this production aimed to show the power of ISIS’ network and to send its radical message to potential recruits to encourage their migration to their utopian state. As Giroux (2005) noted:

> The culture of fear and the spectacle of terrorism become indistinguishable, everyday life under goes a structural and political transformation, fusing sophisticated, electronic technologies with a ubiquitous screen culture while simultaneously expanding the range of cultural producers and recipients of information and images. (p. 2)

However, according to Ewan (2014) from the Chicago Sun-Times, these videos have been “growing in sophistication, using animated graphics and editing techniques apparently aimed at embellishing the audio to make a victim’s final moments seem more disturbing”. Ewan (2014) observed that these videos were uploaded online and disseminated by traditional media and other web-based platforms, such as blogs and shock sites.

Overall, ISIS’ communication strategy can be interpreted as rapid processes of HD propaganda video productions, created by its own media production arms, and distributed via its SMNs and other unpoliced platforms, such as JustPaste.it, archive.org and Sendvid, for information dissemination. ISIS has four aims for their HD production: spread a culture of fear among its enemies, show the power of their networks, achieve its territorial ambitions
and spread their radical ideology. ISIS’ priority is to spread a culture of fear among its enemies, especially Shiite militants and the Iraqi and Syrian armies. The aim is for ISIS to terrorise and demoralise its enemies, to earn some concessions concerning their political legitimacy and free their prisoners (Clarke, 2003). As Castells (2009) in his book *Communication Power* noted:

> Political violence is a form of communication by acting on the minds of people through images of death to instill fear and intimidation. This is the strategy of terrorism, which resorts to spectacular manifestations of random destruction to induce a permanent state of insecurity among targeted populations. Violence, broadcast over the communication networks, becomes the medium for the culture of fear. (p. 417)

Horror has always been used as tool of propaganda. The use of political violence aims to send messages of fear throughout society to achieve political agendas. For example, in 1948, Israeli Haganah\(^\text{62}\) attacked some Palestinian villages, killing almost everyone there, which forced the Palestinians to flee from main cities (e.g., Yafa and Haifa). In 1968, during the Vietnam War, the US troops attacked My Lai, killing over 500 unarmed Vietnamese civilians. In 1988, the government of Saddam Hussein launched a chemical attack on the Kurdish city of Halabja in Iraq, killing thousands of people. These horrific acts served to send political messages of fear throughout their respective societies.

ISIS’ second objective in their use of HD productions is to show the power of their networks. They desire the world’s attention regarding their message. Their message aims to encourage

\(^{62}\) Haganah is a Hebrew term meaning ‘Defence’. It was a Zionist military organisation representing the majority of the Jews in Palestine from 1920 to 1948. (source: https://www.britannica.com/topic/Haganah).
other jihadi to join their cause, as it appears most recruited jihadi are foreign fighters. As Kelly (2014) identified:

> ISIS’ online propaganda campaign effectively targets disenfranchised westerners. It lures them into a false sense of purpose by contrasting the West’s often intolerant perceptions of Islam with the idealisation of a caliphate, and then throws in Hollywood-style action in its execution.

Similarly, Schmitt (2015) observed, “The online messaging has aimed to create a competing narrative that strikes an emotional chord with potential militants weighing whether to join a violent extremist group”.

Third, HD productions assist ISIS in achieving its territorial ambitions to contain the Sunni provinces, as they claim in their video productions that they are the Sunni defenders. Finally, ISIS exploits HD productions to spread their radical ideology (i.e., a global networked radical ideology), in which ISIS can disturb the security of the coalition forces of what Atwan (2015) called an “ideological sleeper cell” (p. 127). This was evident in recent attacks in Saudi Arabia, Canada, Australia and the US as self-radicalised individuals committed acts of terror to disturb the security of these nations. As Giroux (2005) noted:

> As a result of the emergence of new technologies of diffusion, culture becomes more globalised as it is newly hybrized and organised through technologies that redefine its meaning, the power of its reach and the influence it has in shaping diverse and loosely connected audiences […] it also has become a powerful force for the production of public spheres engaged in the production of global landscape of violence, fear and insecurity. (p. 15)
One of the technologies that played a key role in spreading radical ideology and encouraging acts of terror against Western targets was Telegram (see Section 6.3). Ultimately, it was the sophistication of HD videos that proved to have a greater effect, and be more convincing, than messages posted to Twitter and shared across other information environments. According to Architte (2012), “It is often argued that videos are more radicalizing than text”. Katz (as cited in Architte, 2012), the Director of the Search for International Terrorist Entities (SITE) Institute in a statement prepared for the US Congress in 2007 stated that “the propaganda in jihadi videos is compelling, convincing, and able to be accessed in a growing number of languages” (p. 18).

Overall, the deployment of HD media productions is part of ISIS’ IO strategy. That is, HD videos helped to maintain network structure and flows of information by enrolling more actors to the network. HD videos helps to maintain internal cohesion and messaging. Externally, it aided in spreading fear and recruiting more actors (see Section 4.12).

3.4 Understanding ISIS’ Information Operations

To understand processes of ISIS’ IO strategy it is important to identify organisation objectives, political and religious structure and its purpose of endurance. Since its emergence, ISIS was transparent about the nature of its existence as outlined by the famous Friday speech of Abu Bakr Al-Baghdadi (as Caliph Ibrahim) in the Great Mosque of Al-Nuri, Mosul on 29 June 2014. The speech highlighted many aspects of causes of destruction of the Ottoman Islamic caliphate. This speech was also significant because of Al-Baghdadi’s declaration of Islamic caliphate under his leadership. Al-Baghdadi’s declaration of Islamic caliphate achieved three main objectives. First, it united all Sunni Muslims in one geographical
location under the umbrella of Islamic caliphate. Second, it built a sovereign Islamic state that had an army, Welayats and constitutions. Third, it declared the intention to conquer and subdue the land of infidels. To achieve such objectives, ISIS ran a sophisticated IO strategy, dependent on their strategic propaganda narrative. Winter (2017) underlined the aim behind ISIS’ use of strategic propaganda. He argued:

The Islamic State [ISIS] has three information principles. First, present an alternative narrative, a comprehensive offer of existence; second, counter the ‘intellectual invasion’ being conducted by the mainstream news media; and, third, launch propaganda ‘projectiles’ against the enemy. Combined, these three facets form the foundations of the group’s propaganda strategy.

However, before I explore the strategic narrative of ISIS networks, I will define the term IO. The US Department of Defence (DOD, 2017) defined IOs as “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own” (p. 113).

ISIS’ IO involves the collection and dissemination of information to establish competitive advantage over its opponents. Specifically, ISIS managed to swarm information environments with propaganda utilising social network platforms’ dissemination dynamics (e.g., the hijacking of trending hashtags). The purpose of ISIS’ IO in swarming information environments was to influence Muslims—through ISIS’ processes of sophisticated production, new approaches to information dissemination techniques and employment of strategic narrative themes—to rally behind the new caliphate. To understand these processes, it is important to highlight the strategic logic of their IOs.
3.5 The Strategic Logic of ISIS’ Information Operations—A Strategic Narrative Perspective

To highlight the origins of ISIS’ IO strategy it is important to understand the events that characterised the trajectory of this strategy. These events include the Arab Spring uprisings and Al-Qaeda’s use of digital information environments and sophisticated propaganda strategies. From the Arab Spring uprisings, ISIS learned that the use of strategic narrative by Arab activists tipped the balance of power and diminished barriers of information control by the Arab governments (see Section 2.1). From Al-Qaeda, ISIS understood the need to have a compelling story to gain support and enlarge their audience; however, ISIS managed to use sophisticated media production techniques and targeted new information environments for dissemination purposes.

To understand the logic of ISIS’ IO and the use of a strategic narrative, two infamous publications must be discussed: Management of Savagery: The Most Critical Stage Through Which The Umma Will Pass (herein, Management of Savagery) and Oh Media Correspondent, You Are a Mujahid Too. In these two publications, ISIS crafted and defined its media production policies, strategic narrative and propaganda to achieve its political and religious ambitions. To understand the roots of ISIS’ IO and strategic narrative an in-depth analysis of the latter media publications is presented.

In Management of Savagery, Al-Qaeda’s thinker, Abu Bakr Naji (2006) expressed the necessity of adapting a powerful media strategy to compete with and defy the media of ISIS’ adversaries. According to Naji (2006), this media strategy had three aims. The first aim was

---

63 Charlie Winter described this booklet as a guide for information warfare (Winter, 2017).
to recruit some military personnel from the “army of infidels”\(^\text{64}\) to convert them into mujahedin. Second, the media operations must justify all savage behaviour, such as killings and all other capital punishments. Third, the media operations must be transparent on all actions, including the recognition of their own error. With this Naji (2006) aimed to represent Al-Qaeda as an honest organisation to its followers; by revealing the lies and tricks of Al-Qaeda’s enemies, Naji hoped to establish a strong impression of Al-Qaeda’s truthfulness. To achieve this media strategy, Naji (2006, p. 43) suggested that new media committees should be established from enthusiastic youth willing to serve the new state.

The *Management of Savagery* booklet was adapted by ISIS as the ultimate strategy with which to establish their own state. As ISIS inherited a legacy of corruption, chaos and disorder in the territories they controlled (a result of the secular governments who abolished Islamic laws), it was deemed necessary to act mercilessly to control the society. The steps to establish a caliphate, as outlined in the *Management of Savagery* publication, is shown in Figure 10.

---

\(^{64}\) According to Naji, the armies of Arab tyrants serving Western interests are “armies of infidels”.
The second publication and media production is *Oh Media Correspondent, You Are a Mujahid Too*. This publication was produced by Al Himma bookshop; it is a 55-page pocket-sized book, so it could be kept and distributed easily among followers. This publication presented two main media strategies: defensive (reinforcing) aims to counter the propaganda strategy of adversaries and offensive (suppression) aims to show strength through disseminating messages of fear.\(^{66}\)

---

\(^{65}\) Al Himma is the publishing agency for ISIS books.

\(^{66}\) These strategies will be discussed in Chapter 7.
In *Oh Media Correspondent, You Are a Mujahid Too,*\(^{67}\) ISIS aims to encourage every Muslim who cannot join physical jihad to be media jihadist. ISIS first identified (based on the Hadith and some verses of Qur’an) that media jihadi and actual jihadi in the battle field have the same divine reward. In this publication, the authors highlighted ways to use media for jihad. According to teachings about jihad (i.e., *Fiqh Al-Jihad*) in the Qur’an, jihad of infidels has three aspects. The first of these aspects is jihad of the tongue. That is, the use of words either written or spoken to fight enemies. This strategy of jihad had great psychological effect their enemies by the spreading of messages of fear. For example, Nashir Political Service posted on its Telegram channel:

```plaintext
Some people might think that what we say on the media is just words and not fighting. But our words if sometimes accompanied by wisdom they will be just like a bomb that can be heard in the heart beats of any unbeliever. Some words you write or the news you report might settled [sic] in the heart of Nice\(^{68}\)[such as] Knight when he carried his operation which terrified not only France but also Europe.
```

The second aspect of jihad, as it applies to media, is that media can be used as the catalyst for jihadi mobilisation. The use of media channels to call for jihad and show the atrocities committed at the hands of an organisation’s adversaries is also the duty of mujahedin. The third purpose of jihad is to infuriate the enemy. This can be done by disseminating counter narrative measures to defy the propaganda of their adversaries by showing the victories and strength of their state. However, to achieve the objectives of media-mujahedin, guidelines were established on how to use many means of media productions and channels of

---

\(^{67}\) ISIS also produced a video production under the same name.

\(^{68}\) He referred to the Nice attack in France (August 2015), that resulted in killing 80 people.
dissemination. That is, the enrolment of many network actors such as multiple digital media environments can facilitate jihadi’s mobilisation.

In the *Oh Media Correspondent, You Are a Mujahid Too* video production,69 ISIS drew attention to the war within SMNs after the degrading operation had taken place. In the video, the presenter said, “Let fight them in Twitter […] they spend millions of dollars to hinder the outreach of our message”. The video also claimed that every post or message sent in digital media influences on Muslim youth: “It may affect their decision and join us or at least this post will raise awareness about the ongoing war between the army of infidels and Islam”. According to Winter (2017), the producers of this video aimed to provide:

Advice as to how Islamic State [ISIS] media operations should actually be constructed. In so doing, they shed light on the very essence of its propaganda strategy, a tripartite approach to communication that has given the group an edge over its rivals and transformed its war against the rest of the world.

Further, the notion of media-mujahedin was also highlighted in Al-Qaeda’s publication produced by the Al-Fajr media centre.70 In it, the author (as cited in Prucha, 2011) argued, “Internet is a battlefield for jihad, a place for missionary work, a field of confronting the enemies of God. It is upon any individual to consider himself as a media-mujahid, dedicating himself, his wealth and his time for God”(p. 46).

---

69 This video is available on: http://www.dailymotion.com/video/x3vmb3r.

70 Issued by Al-Fajr on May 6th, 2011.
Clearly, the publications *Management of Savagery* and *Oh Media Correspondent, You Are a Mujahid Too* reflect ISIS propaganda strategy and media tactics. These publications informed their information warfare strategy, aimed to counter their adversaries’ propaganda and raise awareness about the important aspects of jihad. These publications have exclusively contained all media strategies of ISIS, particularly how to execute IO and mobilise media correspondents and digital logistics to achieve a counternarrative media strategy against their adversaries. The analysis in this chapter discusses what these publications present and the implication for ISIS’ IOs. Analysing the content of these publications leads to an understanding of the ISIS’ sophisticated media strategy, strategic narrative and propaganda themes, methods of production, influence of reach and objectives of messages.

### 3.6 The Strategic Narrative of ISIS Networks

The study of the strategic narrative of ISIS aims to understand its message, the audience it targets and the medium it uses. As Roselle, Miskimmon & O’Loughlin (2014) argued, strategic narrative “directly addresses the formation, projection and diffusion, and reception of ideas in the international system” (pp. 9–10). Therefore, the purpose of creating a strategic narrative, as Nissen (2015) argued, is that “it offers a framework through which conflicts past, present and future can be structured in order to help establish and maintain power in the international system and to shape the context and the system itself” (p. 45).

In this chapter, I use Roselle et al. (2014) definition of strategic narrative: A strategic narrative is “a means for political actors to construct a shared meaning of international politics and to shape the perceptions, beliefs, and behaviour of domestic and international actors” (Roselle et al., 2014). It is also important to point out that “a narrative is a system of stories that share common themes, forms, events, and participants, and create expectations for
how those elements can be assembled to satisfy a desire that is rooted on conflict” (Halverson, Corman & Goodall, 2011).

To better understand the common themes, shared stories and participants and events of ISIS networks, I highlight key findings of scholars and policymakers who examined the strategic narrative of ISIS’ networks to establish a counterpropaganda strategy (e.g., Milton, 2016; Nissen, 2015; StratCom, 2015; Winter, 2015a, 2015b; Zelin, 2015; see Table 1).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Methodology</td>
<td>Content analysis of visual propaganda posted on Twitter</td>
<td>Content analysis of 892 digital artefacts posted on Twitter</td>
<td>Content analysis of 9,000 visual and documents posted to Twitter</td>
<td>Visual propaganda content analysis</td>
</tr>
<tr>
<td>Narrative theme</td>
<td>Governance</td>
<td>Utopia</td>
<td>Governance</td>
<td>Religious issues</td>
</tr>
<tr>
<td></td>
<td><em>Daw’a (preaching)</em></td>
<td>Victimhood</td>
<td>Justice</td>
<td>Political messages</td>
</tr>
<tr>
<td></td>
<td><em>Hisbah (moral policing)</em></td>
<td>Military (jihad)</td>
<td>Religious practice</td>
<td>Social issues</td>
</tr>
<tr>
<td></td>
<td>Military</td>
<td>Brutality</td>
<td>Life in the Caliphate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Belonging</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Findings of scholarly research on ISIS’ strategic narrative. Illustrated by the author.

This analysis aims to capture the communication effects and strategic propaganda of ISIS’ narrative themes by referring to the work of scholars who used different methodological approaches, different time frames and different media content. The findings of these studies will be compared to my own findings, in which I used different methodological and content analysis approaches. As Miskimmon, O’Loughlin and Roselle (2017) noted:

This approach to strategic narratives indicate that they are not just single stories, but several stories that together make up—or support—the narrative, and that all actions
taken as a part of a strategy are ‘storied’, thereby becoming part of a larger overarching strategic narrative, and that these actions have communicative effect.

Communication effect can be radicalisation, recruitment processes and lone wolf attacks. For example, in Picture or It Didn’t Happen: A Snapshot of the Islamic State’s Official Media Output, Zelin (2015) examined the totality of ISIS’ media productions during a sample week: from 18 April to 24 April 2015 (p. 85). His analysis was based on visual and textual content posted by prominent ISIS accounts on Twitter. Zelin (2015) categorised his key findings into four main themes—governance, daw’a (preaching), hisbah (moral policing) and military. His week-long data collection revealed that 88 per cent of ISIS content is visual (63 percent is pictures, 20 percent is video, 5 percent is graphic) “as opposed to text-based propaganda” (Zelin, 2015, p. 84).

Using the tracking of hashtags methodology, Winter (2015a)—in Documenting the Virtual ‘Caliphate’—examined 892 items of ISIS’ digital media content on Twitter. His analysis involved a 30-day survey of ISIS’ media outputs such as Al-Hayat, Al-Itisam and Ajnad media production arms. To understand ISIS’ IO and its media strategy with evidence-based analysis, Winter (2015a, p. 5) collected some videos, photo essays, news bulletins, audio statements, posters and theological essays from 17 July to 15 August 2015. His research revealed that six main media narratives were dominating ISIS productions. These are utopia, military, brutality, belonging and victimhood.

The North Atlantic Treaty Organisation (NATO’s) StratCom (2015) report, DAESH Information Campaign and Its Influence, examined the information strategy of ISIS between 2014 and 2015. To understand ISIS’ information and communication strategy, StratCom (2015) employed six methodological approaches including: visual framing, brainstorming in
syndicates, eye tracking, social media analysis, and media and effect analysis. Their research shows that the visual propaganda of ISIS comprises three main narrative themes: political messages, which accounted for 48 per cent of the visual propaganda; religious messages, which accounted for 38 per cent of the visual propaganda; and social issues, which accounted for 14 per cent of the visual propaganda.

In another report, *Communication Breakdown: Unravelling the Islamic States Media Efforts*, military analyst Daniel Milton (2016, p. 21) analysed over 9,000 videos, photographs and picture reports that had been embedded in Twitter, posted between August 2015 and August 2016. Milton (2016) found that more than 50 per cent of the analysed data was focused on themes outside the battlefield, such as religious practices, justice, governance and life in the caliphate. Only nine per cent of the releases “show the commission or aftermath of executions or battlefield killings” (Milton, 2016, p. iv). Figure 12 and 13 shows the results of Milton’s findings.

![Figure 12. Milton’s findings about the media form used by ISIS in their Twitter posts. Source: Milton (2016, p. 30).](image)

![Figure 13. Milton’s findings about the content of ISIS’ Twitter posts. Source: Milton (2016, p. 30).](image)
Overall, all media content produced by ISIS, including visual, audio, document, photo, meme, or Twitter and Facebook posts share a similar narrative. The difference is the percentage of shared themes through visual propaganda as they vary depending on political and religious circumstances surrounding the caliphate. The role of outside actors who digitally aided ISIS with media productions reflected on victories and setbacks of ISIS.

I have included my reflections on the studies that highlighted ISIS’ IOs and narrative themes in line with al-Baghdadi’s speech, who first defined the objectives of ISIS’ IO based on the publications *Management of Savagery* and *Oh Media Correspondent, You Are a Mujahid Too*. Additionally, I highlight my findings from my own textual analysis, using the NVivo analysis tool, of six examples of *Dabiq* and *Rumiyah* ISIS magazines (see Figure 14).

*Figure 14. Word cloud findings of the analysis of six of Dabiq and Rumiyah ISIS magazines created by the Author.*

The publications of six *Dabiq* and *Rumiyah* ISIS magazines were downloaded from the archive.org platform. These publications were published by al-Hayat Media Centre and were written in English. The publication dates of these magazines were between August 2016 and March 2017. The aim of this analysis is to capture the media narratives of ISIS that targeted
non-Arabic speakers. As shown in Figure 14, the main media narratives highlighted *Tawhid* (i.e., the idea of no God, but Allah), praise for the IS, the need to establish a caliphate, other important aspects of jihad against their enemies (e.g., crusaders and *rafida*) and call for Hegira to the Islamic caliphate. However, these textual analysis findings will be explained in correlation with other scholarly findings examined in Section 3.6 (see Figure 15).

Based on the process represented in Figure 15, the strategic logic of ISIS networks required in-depth analysis of ISIS’ IO objectives and principles. As stated in Figure 15, ISIS’ IO aims to achieve three objectives: re-establish a caliphate, unite all Muslim Sunnis under the newly established caliphate, and stay and expand (i.e., *baqiya wa Tatamadad*).
3.7 Re-Establish the Caliphate

Since the demise of the Ottoman caliphate in 1923, and its substitution by a secular Turkish government, Al-Qaeda—under the leadership of Osama bin Laden—was the first organisation who proposed to reinstate a caliphate. Bin Laden withdrew his plan, as he worried that this would benefit the US, as the mujahedin could be easily targeted if they were stationed in one geographical space. However, ISIS disowned Al-Qaeda and declared the caliphate after the seizure of Mosul. Winter (2017) asserted that:

The restoration of a ‘caliphate’ is a religious duty—as are the draconian laws and vicious terrorism that the Islamic State [ISIS] practices. It presents a diagnosis for real and imagined Muslim woes and a prescription: to embrace its assault on Syria, Iraq and, eventually, all other Muslim states.

To understand the principles guiding ISIS’ strategic narrative to re-establish a caliphate, I classified findings into two main categories: offensive and defensive operations. This classification was based on current empirical studies by scholars and experts in the field (e.g., Milton, 2016; StratCom, 2015; Winter, 2015a) and content analysis of ISIS’ media productions in primarily Arabic publications, such as Management of Savagery, Oh Media Correspondent, You Are a Mujahid Too and the content analysis of Dabiq magazines. As Winter (2017) explained:

The Islamic State [ISIS] uses offensive information warfare to attack not only military targets, but civilian ones, too. After all, in its eyes, there is no such thing as a civilian status beyond the caliphate’s boundaries. Thus, its media ‘missiles’—be they video executions or mass-mediated terrorist attacks—are calibrated to strike disengaged publics as much as they are towards hitting engaged militaries.
The main objective of the strategic narrative’s defensive operations was recruitment, including encouraging Muslims to migrate to the land controlled by ISIS; calling Muslims to pledge allegiance to the Caliph,\(^71\) recruiting individuals for jihad and establishing a global caliphate.

To achieve the primary and ultimate objective, ISIS carried out sophisticated media propaganda campaigns to promote a new caliphate. As Afzal and Wallis (2016) noted, “ISIS’ content contains carefully-chosen informational cues aiming to present a romanticized view of the caliphate” (p. 76). To do that, ISIS employed experts in media production techniques, who selected narratives carefully. Using the data collected from social media platforms (e.g., Twitter), encrypted applications (e.g., Telegram) and anonymous sharing portals (e.g., JustPaste.it), I observed that the media narratives of ISIS’ promotion of the caliphate was underpinned by three themes: utopia, supremacy and the sharing of grievances (representations of victimhood). These themes were depicted in what Atwan (2015) identified as ‘propaganda HD’ (p. 8), as evidenced in the following videos produced by ISIS: *Message to the US Government*, *Healing of Believers’ Chests* and *Clanging of Swords*. The reason behind the HD production was suggested by Milton (2016): “The group placed on quality production as a means of appealing to the public. Indeed, while Islamic State [ISIS] media products today are known for their high-quality production value” (p. 4).

\(^{71}\) Based on a Hadith of the Prophet Mohammad, “Whoever removes his hand from obedience (to the ruler) will meet Allah with no proof for himself, and whoever dies without the pledge of allegiance (to the ruler) upon his neck dies a death of jahiliyya” Narrated by Muslim.
3.7.1 Utopia

In his monograph, *Documenting the Virtual ‘Caliphate’*, Winter (2015a) argued, “The relative importance of the utopian strand of Islamic State’s [ISIS’] propaganda is inevitable and necessary” (p. 30). In 2014, ISIS showed its utopian society depicted in a series of propaganda videos, *Mujatweets*, produced by Al-Hayat Media Centre (see Figure 16). In *Mujatweets*, ISIS aims to recruit jihadists and encourage other Muslims to migrate to newly established Islamic caliphate. The main narrative in these videos was the representation of a beautiful life under the re-established caliphate. These videos were characterised by images of busy markets, children in playgrounds, clean hospitals and free health care, and peace in the streets of Raqqa and Mosul. These videos were widely celebrated and shared across SMNs, mainly YouTube. As Winter (2015b) observed, “The idea of the utopia ‘caliphate’ runs strongly throughout all the organisation’s messaging. Its constant presence makes sense: Islamic State’s [ISIS’] establishment and implementation of the ‘caliphate’ is the organisation’s unique selling point” (p. 28).

---

72 The term *Mujatweets* is a combination of ‘Mujahideen’ and ‘Tweets’. *Mujatweets* are short HD videos, ranging between 1.30–3.00 minutes, presented by foreign recruits in many languages, mainly English, French, and German.

73 *Mujatweets* is series of episodes start episode #1 and ends episode #8. Some of these videos are still available on YouTube.
The utopian narrative was effective; it resulted in convincing thousands of Muslim youth to migrate from Western and Arab countries to join ISIS (see Figure 17). Ibish (2014) described this narrative as healthy because it was not challenged by ISIS’ adversaries. This vision of utopian Muslim society was described by Ibish (2014) as “universalism in an undifferentiated and gigantic caliphate across the Islamic world, without distinctions among individuals except their degree of zealotry”.

Other propaganda productions, such as *From the Land of Khalifah* (see Figure 18) and *Welcome to the Land of Caliph*, focused on other aspects of the utopian Islamic society under
the Islamic caliphate. The focus was on migrating to the land of the caliphate, as many migrant jihadi said, we “live in dignity and peace under the rule of sharia law”. One foreign fighter from the UK said, “We don’t need their democracy [], we only need Sharia that’s why I am so happy to migrate here”.74

Moreover, ISIS’ printed publications and digital magazines, such as Dabiq and other online publications, also focused on a utopian life under the Islamic caliphate. Media narratives in such publications visioned the societal impact of the Islamic caliphate constitution (known as Dywan) in building the state, paving the streets, observing markets, and caring for livestock and land. According to one media operative (as cited in Winter, 2017):

Propaganda must simultaneously address and water down the negative aspects of living under the Islamic State [ISIS], while also conveying a rose-tinted image of its

---

74 From ‘The Land of Khalifah’ video, 2015.
positive facets. In this way, the Islamic State can sell itself as a utopia to which Salafi-jihadists can go to live as heroes, rather than an insurgent group to which new adherents go to die as martyrs.

The utopian theme in the ISIS narrative was presented during operation We Are Coming Nenawa, which was initiated in October 2016 to liberate Mosul. The power of the utopian messages is highlighted by Ibish (2014): “This simple message resonates because it is coherent, idealistic and fills a void. But most of all, it promises, and appears to be delivering, tangible and striking political and military successes”.

The utopian narrative comprises 52.57 per cent of the media narratives of ISIS (see Figure 19). Winter (2015a) stated, “Islamic State’s [ISIS’] emphasis on the utopia narrative is unambiguous: over half of the propaganda events in the Shawwal dataset (469 of 892) convey it above all else” (p. 30). Winter's (2015a, p. 32) content analyses revealed that the utopian narrative can be refined into seven categories: economic activity, religion, social life, justice, governance, nature and landscapes (see Figure 20).


Winter (2015a) concluded:
The most prominent narrative, by far, is that of utopia. At once the most appealing promise of the group and the most difficult to convince observers of, there is a predictably disproportionate emphasis upon it. Islamic State’s [ISIS’] media strategists ensure that its utopia is sold as a comprehensive project, where the economy flourishes, ‘Islam’ is implemented, wildlife thrives, rule of law prevails, and the government governs. (p. 39)

To attract women in joining and migrating to the Islamic caliphate, ISIS established ‘Umm Network’ on Twitter. According to Liang (2015), the content shared in Umm Network’ is:

Meant to make extremism a normal lifestyle decision. Pictures of kittens and design footwear are tweeted as well as extremist rhetoric and descriptions of the ‘good life’ in Syria. The network gives nursing and cooking advice for those wives who want to keep their jihadists happy, and it provides information on Shariah, weapons use, and social media tools so that they can contribute to the IS recruitment campaigns. (p. 6)

3.7.2 Supremacy

There were three aspects to the supremacy narrative depicted in ISIS’ media productions: the primacy of Muslim identity, the application of sharia law and the functioning of the state. ISIS propaganda has shown many aspects of state authority, power and control in the territories they control (i.e., Welayats). The first sign of sovereignty was the declaration of Abu Bakr Al-Baghdadi as Caliph. The legitimacy of the new Caliph, as stated in ISIS’ media productions, is derived from the teachings of the Prophet Mohammed and the legacy of the Rashidun caliphate after the prophet’s death. The use of the black flag, stamped with Prophet Mohammed’s signature, sends a powerful message to many people in the world that Islam is
returning to its original form, power and dominance. The significance of Al-Baghdadi’s declaration of caliphate resonates by dividing the Muslim world based on identity. This identity is derived from a Salafi perspective, which rejects non-Islamic behaviour and practices, such as Sufism, Tabligh and Ikhwan. As Ingram (2015) observed, “IS’s [ISIS’] central media units bombard its transnational audiences with messages that fuse narrative, imagery and symbolism to emphasise the primacy of one’s Muslim identity over all others” (p. 742).

Moreover, the application of sharia law (e.g., hudud, see Figure 24) in its original form, based on the teachings of the Qur’an and Sunna (including the issue of passports and establishment of its own golden currency yet) are another sign of ISIS’ supremacy (see Figures 21–23).

Figure 21. ISIS flag. Source: Nashir political services.

Figure 22. Caliph Abu Bakr Al-Baghdadi.

Figure 23. ISIS passports and golden dinar. Source: Nashir political services.
As Ingram (2015) explained, “IS [ISIS] now devotes a significant portion of its IO activities to portraying its governance apparatus as multidimensional, sophisticated, bureaucratised and well resourced. This prioritisation is reflected in IS’ IO output” (p. 737).

One of the most important elements of their IO to show supremacy through the integration of physical acts of violence within their IO. Denning (2005) argued, “They make audio and video recordings of the incidents for distribution over the [i]nternet and on television. Their violence becomes theatre, staged for its psychological impact, and replayed over and over again in the media as IO” (p. 5).
3.7.3 Sharing Grievances and Representations of Victimhood

ISIS represented notions of victimhood as a key narrative to establish unity among Muslims under the newly established caliphate. In its media productions, End of Sykes-Picot (see Figure 25) and Smashing the Borders (see Figure 26), Al-Hayat media productions showed atrocities, economic setbacks and poverty after the dismantling of the Ottoman caliphate and subsequent appointment of Arab leaders who were allied to the West. These grievances occurred as a result of the US and European meddling in the Middle East. The Sykes-Picot Agreement was an agreement signed between England and France on 16 May 1916, which divided the regions of the Ottoman Empire between England and France. This agreement was responsible for establishing the current borders of the Middle East. The creation of artificial borders has dismantled the unity of the Muslim nation, which resulted in direct intervention from the UK, France, the US and Russia in Iraq and Syria. Ultimately, this intervention caused millions of casualties and led to the current refugee crisis. Miller (2016) contended:

In the propaganda video, IS was echoing and amplifying the sentiment that Sykes-Picot is a symbol of foreign meddling, but the militant group was also modifying this message for their own purposes, and crucially accusing Muslim leaders of complicity in these crimes, a key theme of IS propaganda.

Caliph Abu Bakr Al-Baghdadi announced, “This blessed advance will not stop until we hit the last nail in the coffin of the Sykes-Picot conspiracy”.

139
3.8 United Sunnis

United Sunnis, under the banner of Islamic caliphate, is one of the objectives of ISIS’ IO strategies. As Winter (2017) noted, “If presented with the “right” information and the “correct” narrative, they contend, Muslims everywhere will inevitably end up rallying around the caliphate’s banner”.

Three strategic narratives can be observed from this objective: share grievances, raise political awareness and recruitment. As clearly stated in Figure 27 these strategic narratives aim to share common grievances (including representations of victimhood), express Muslim
identity and raise political awareness. Ultimately, this objective can be achieved through the process of recruitment. Common grievances and raising of political awareness were tools used to recruit new jihadi and migrants to ISIS’ lands.

![Diagram of Unite Sunnis with circles for victimhood, political awareness, and identity]

*Figure 27. The main narratives aimed to unite Sunnis. Illustrated by the Author.*

The main narrative theme that ISIS used to unite Sunnis was victimhood. Fernandez called this theme ‘urgency’. To present this theme, ISIS depicted atrocities committed by Shiites’ militancy, by showing images and videos of:

[Sunni Arab] Muslims … being slaughtered now. Syria’s children are being killed by the *(Rafida)* apostates now. There is a plot now by the Shiites in Iraq, Syria, and elsewhere to utterly destroy the Sunni Muslims. The Shiites have already taken the Sunnis’ dignity and political power and are now on the march to take everything else. *(Fernandez, 2015, p. 11).*

Ingram (2015) also observed that:

---

75 Rafida, according to Sunnis, are Majoos (fire worshippers) who embraced Islam under Shia sect to destroy Islam from the inside.
ISIS’ narratives portray them as the champion of Sunni Muslims (in-group identity), its enemies as evil Others (Shias, Christians, non-conformist Sunnis) who are responsible for Sunni perceptions of crisis, and ISIS as the only source of solutions. The result is a competitive system of meaning that acts as a framework through which ISIS’ audiences perceive and evaluate the conflict and its actors, generate meaning and legitimise actions. (p. 736)

In one of his speeches, Abu Bakr Al-Baghdadi (as cited in Ingram, 2015) affirmed Muslim Sunni identity when he stated:

O soldiers of the Islamic State [ISIS], do not be awestruck by the great numbers of your enemy, for Allah is with you … I also remind you to attend to the Muslims and the tribes of Ahlus-Sunnah (the Sunnis) with goodness. Stay awake guarding them so they can be safe and at rest. Be their support … Know that today you are the defenders of the religion and the guards of the land of Islam. (p. 742)

It is important to acknowledge that Islam is the identity of all Muslims. This identity is constructed on Islamic principles of wall’a (i.e., alliance to Allah and his messenger only) and Barra’a (i.e., abolish all alliances and associates with infidels). Therefore, as Arab countries are allied with the infidel West, ISIS encouraged all Muslim migrants to its land to declare Walla’a and Barra’a by burning their passports (see the propaganda films, Message to People of Jordan, and One Nation (see Figure 28), which had both ideological and symbolic significance.
The third strategic narrative asserted the need for political awareness. It highlighted the corruption of Arab governments, including their alliances with ‘the enemies of Allah’ (e.g., the US and Israel), their application of non-Islamic laws and the true believers they held captive in their jails (e.g., Saudi Arabia). Therefore, ISIS called Sunnis to unite and execute jihad against their rulers. Moreover, ISIS drew attention to the role of Iran and its ambitions to control Syria, Iraq, Yemen, Lebanon and the Arab world. Such political messages were depicted in video productions (see for example, Revenge of the Desert and The Fertile Nation) see Figures 29 and 30.
3.9 Stay and Expand

As part of its marketing strategy to recruit more people to the land of Islamic caliphate, ISIS adopted the motto *baqiya wa tatmadad* (i.e., stay and expand). To establish a legitimate Islamic caliphate, the expansion of territories is a religious duty and requirement. However, most of ISIS’ political and social messages depicted the term ‘baqiah’. To achieve stay and expand objectives, ISIS used psychological operations that included the dissemination of political and social messages aimed to radicalise, recruit and spread fear (see Figure 31).

*Figure 31. Diagram representing the relationship between fear, recruitment and radicalisation.*

*Illustrated by the Author.*
Giroux (2005) noted:

The culture of fear and the spectacle of terrorism become indistinguishable, everyday life under goes a structural and political transformation, fusing sophisticated, electronic technologies with a ubiquitous screen culture while simultaneously expanding the range of cultural producers and recipients of information and images. (p. 2)

Further, Giroux (2005) clarified:

As a result of the emergence of new technologies of diffusion, culture becomes more globalised as it is newly hybrized and organised through technologies that redefine its meaning, the power of its reach and the influence it has in shaping diverse and loosely connected audiences […] it also has become a powerful force for the production of public spheres engaged in the production of global landscape of violence, fear and insecurity. (p. 15)

The violence, fear and insecurity, as suggested by Giroux (2005), were used as a strategic narrative by ISIS to justify its actions and acts of terror against Western people in their homeland. Being exposed rapidly to ISIS’ information was thought to speed the process of recruitment and enhance radical views of Muslims living in the West (see Figures 32 &33).
Figure 32. Screenshots of messages disseminated via Nashir Telegram channel.

Figure 33. Screenshot of propaganda messages to support stay and expand narrative. Source: Nashir Political Services.
The NATO StratCom (2015) argued that the information strategy of ISIS intended to “become a global state that unites Muslims around the world, and lines of effort” (p. 29). This objective can be achieved through processes of radicalisation, recruitment and spreading fear. Williams argued:

Islamic State’s [ISIS’] media effort has several aims that target both sympathetic and hostile audiences. One goal is to recruit supporters (…) A second goal is to generate fear among its opponents, which has very specific advantages on the battlefield. A third goal is to assert its legitimacy and gain acceptance of its status as a state.

In this context, it must be stressed that the bulk of Islamic State’s publications target Muslim societies around the world; however, they also attempt to influence disbelievers (Lakomy, 2017, p. 41). The strategy of establishing Welayats (i.e., provinces) in every Arab country, including Afghanistan, Russia, Pakistan and the Philippines, and constitutions in every Welayah aims to control social and economic systems. However, the ambition of ISIS is not limited to only these countries but aims at conquering the West as shown in their map (see Figures 34 and 35).

Figure 34. Screenshot obtained from Stay for the End Times video production.
3.10 The Communication Effect of ISIS’ Strategic Narrative

As established at the beginning of this chapter, I have analysed the strategic narrative aims of ISIS. The purpose of this analysis is to explore the communication effects of ISIS’ IO. In this subsection, I aim to highlight the two main communication effects: radicalisation and recruitment. I aim to examine how these effects manifested in ISIS’ IO objectives. Most importantly, I discuss the role of internet technologies in the processes of radicalisation and recruitment.

However, this subsection will not discuss how and why an individual is radicalised or recruited. Instead, I will highlight the role of SMNs and other information environments in spreading ISIS’ strategic narrative and how this has affected the influx of jihadists to the land of the Islamic caliphate.

3.11 Recruitment and Radicalisation

Recruitment and radicalisation are an integral part of ISIS’ PSYOP to achieve its political and religious agendas. As Denning (2005) argued, “The purpose of PSYOP is to induce or reinforce foreign attitudes and behaviour favourable to the originator’s objectives” (p. 3).
Although terror organisations do not refer to it as PSYOP, they appear to understand and employ psychological operations\textsuperscript{76} (Denning, 2005, p. 3).

Denning (2005) defined psychological operations as “planned operations that convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behaviour of foreign governments, organisations, groups, and individuals”. The first part of this definition is the most important when discussing the radicalisation and recruitment of foreigners.

In this subsection, I am discussing the PSYOP that aimed to enhance and accelerate the process of radicalisation and recruitment. However, these operations can also be called propaganda (Taylor, 2002, p. 50). There is no doubt that ISIS used propaganda as an IO strategy to leverage its networks around the world. These operations targeted local and international supporters by disseminating emotive messages and grievances, wherein the atrocities of the West—especially those committed against Muslim women and children—were depicted. James Comey (2015), Director of the Federal Bureau of Investigation (FBI), claimed that:

ISIS has managed through its high-volume Internet recruiting, via videos, memes, Tweets, Facebook, WhatsApp and Telegram accounts to contact and penetrate across international boundaries to recruit Americans. According to the FBI, ISIS recruitment in the U.S. has resulted in the actual and attempted recruitment of over 200 individuals residing in the U.S. traveling to Syria to join them.

\textsuperscript{76} See for example Hezbollah and Hamas PsyOp against Israel during military confrontations in section 1.6
By examining the numbers of recruited foreign fighters who joined ISIS in 2014, it can be argued that ISIS’ IO was successful. As Gartenstein-Ross, Barr and Moreng (2016) noted:

ISIS has employed several common themes and narratives in its global propaganda efforts. One theme that is omnipresent in IS’ [ISIS’] global propaganda is a ‘winner’s message’, which portrays ISIS as an unstoppable military force capable of defeating all enemies. This narrative has been particularly effective in persuading jihadist organisations and prospective foreign fighters that IS has staying power in the region. (p. 4; see Figure 36)

Figure 36. Country of origin for the foreign fighters who joined ISIS in 2015. Source: Statista.com.

To understand the phenomena and processes of recruitment, first we must understand radicalisation. In my view, based on my observations, I am arguing that in some cases, radicalisation leads to recruitment. In other words, an individual cannot be recruited unless he is retaining a radical view. These views can be obtained from many sources, such as radical preachers, friends or family (brother, father, cousin, etc.) who have radical views.
Additionally, individuals can be exposed to information available on the internet and other social media platforms by radical preachers. Adopting radical views through the use of media sources is known as self-radicalisation. There are many factors that influence self-radicalisation. This includes social, economic and religious factors. Further, regular exposure to radical messages that have been posted by charismatic Muslim clerics, who are primarily involved in global jihad business (such as Al-Awakili, bin Laden and Al-Zarqawi), can influence the processes of self-radicalisation. However, to completely understand the processes of radicalisation, an in-depth qualitative methodology approach, including semi-structured interviews and social network analysis of participants, would be required.

Based on Figure 36, the influx of foreign fighters who travelled to Syria and Iraq after the establishment of the Islamic caliphate demonstrated that ISIS’ PSYOP was effective. That is, the strategic planning of IO, in terms of dissemination tactics and produced content, was successful. This success will be discussed using the OODA loop information warfare model (see Section 7.3). As represented in Figure 36, more than 7,000 recruits came from non-Arab countries, which is significant. By directing its IO strategy aims at establishing the Islamic caliphate as its ultimate goal, ISIS’ propaganda had a successful effect on young Muslim men and women, who became willing to join. This effect was attained by using a strategic narrative, in which ISIS suggested that migrating to the caliphate was obligatory for all Muslims. This notion was based on the Hadith of the Prophet Mohammed, who said that ‘who dies without a pledge of allegiance, he dies the dead of ignorance’. In Figures 37, 38 and 39 propaganda messages encourage the migration to the Islamic caliphate.

---

77 These numbers are probably lower than it is estimated. As these statistics are based on government and other statically based organisations.
Figure 37. Screenshot of Inside video production.

Figure 38. A message to encourage Muslims to migrate to ISIS’ lands. Source: Nashir News Agency.
However, to understand what radicalisation is or who radicals are can be as difficult as defining ‘terrorism’. Warnes and Hannah (2008) defined radicalisation as “the process whereby individuals transform their worldview over time from a range that society tends to consider to be normal, into a range that society tends to consider to be extreme” (p. 2). Nasser-Eddine et al (2011) suggested that “the terms ‘radicalisation’ and ‘radicalise’ are used to denote: revolutionary thought or actions; shifting from peaceful activity to violent ‘extremism’; becoming sympathetic to militant action; recruitment; becoming hyper-conscious of critical issues and willing to act violently” (Nasser-Eddine, Garnham, Agostino & Caluya, 2011, p. 13).

Further, Ingram (2015) has explained the role of ISIS’ narrative in recruitment process by suggesting that its: The ability of ISIS in producing pragmatic and perceptual factors of

---

Figure 39. Screenshot of a message sent via Telegram to encourage migration to ISIS’ land. Source: Nashir News Agency.

Data collection
Forwarded from
O nation of unbelievers, O Crusaders O atheists;
To this day, we still establish a state that brings together all Muslims from the Arabs, the Ajam, the immigrants and the supporters.
A state that establishes the religion of God in the earth.
A state that will shock you and destroy your thrones. State prepares the generation after the generation of mujahideen to be the spears that stab your hearts. After a while, you will see another generation of Mujahideen that will make you forget what our generation made you suffer.
God is supporting us over you whatever you mobilized and bombarded, this is the promise of Allah to us, God will help us to get your necks, your weapons, your money and your homes. Glory be to God, His Prophet and the believers.
narrative that effectively adapted by its political and military apparatus has designed a system to support rational- and identity-choice decision making in its audiences (p. 736). Ingram’s (2015) views were also reflected by Shaheen’s (2015) study, Network of Terror:

One of the important aspects of ISIS propaganda efforts on SMNs is the ability to produce information Hollywood style materials that can attract the tech-savvy younger generation who are more likely to respond to such concepts. (p. 11) These propaganda efforts had successfully thrived in the minds some of the Muslim youth through rapid processes of information disseminations of grievances. In other words, an influence warfare operation carried out by ISIS resulted in an increase in the number of recruits. It is important to emphasise that the notion of influence warfare not only captured the way information operations occurred in terms of its impact on recruitment, but also how it influenced the opinion of possible recruits to join ISIS.

Moreover, McDowell-Smith, Speckhard and Yayla (2017) explained the mechanisms of the use of social media in the recruitment process, examining recruits in the US who joined ISIS suggesting that: The common method of recruiting in the U.S. is through the feedback mechanisms of SMN’s who is asking questions about ISIS, tweeting, liking or otherwise endorsing the group and then to swarm in on the person with a great deal of personal attention paid via the Internet (see Callimachi, 2015 and Driscoll, 2015). When an American is seduced into the group they are invited to go offline or into encrypted apps where they either are discussing a homegrown attack or seduced into traveling to Syria and Iraq for Jihad. (p. 58)

Overall, to establish the Islamic caliphate, ISIS required a devoted population who offered their allegiance to Caliph Abu Bakr Al-Baghdadi. This vision was reflected assertively in
their propaganda materials. ISIS’ propaganda aimed to encourage other jihadi to join their cause, as it appeared that most recruited jihadi were foreign fighters. As Kelly (2014) identified:

ISIS’ online propaganda campaign effectively targets disenfranchised westerners. It lures them into a false sense of purpose by contrasting the West’s often intolerant perceptions of Islam with the idealisation of a caliphate, and then throws in Hollywood-style action in its execution.

Also, Schmitt (2015) observed that “the online messaging has aimed to create a competing narrative that strikes an emotional chord with potential militants weighing whether to join a violent extremist group”. The strategic narrative of recruitment and radicalisation is formed as a result of what Architti (2013, p. 10) called collective construction of narrative, which ISIS understand very well.

3.12 Conclusion

In this chapter, I highlighted ISIS’ IO strategy, aims and objectives. The information presented in this chapter was derived from prominent ISIS publications and video productions, including Management of Savagery and Oh Media Correspondent, You Are a Mujahid Too. I explained the strategic narrative of ISIS’ networks aims, which led to the establishment of the Islamic caliphate. I discussed the role of digital media in amplifying their message. As Archetti (2013) stated, “The relational understanding of narrative which has been illustrated helps mak[e] sense of the social and political impact of communication in the 21st century” (p. 8). However, to understand the processes of message assemblages and
flows of information across digital information environments, it is important to further examine the digital media logistics of ISIS’ networks.
Chapter 4: Promoting a Terror Narrative—ISIS’ Information Logistics

4.1 Introduction

Following the analysis of ISIS’ IO and its strategic narrative (see Chapter 3), the purpose of this chapter is to explore the construction processes of terror messages, including its assemblages and flows of information across digital networks. In this chapter, I analyse the dynamics and function of tools that helped the generation and dissemination of these messages. These tools are logistics. Often, the word ‘logistics’ is associated with military equipment or supply chains. However, in this chapter, logistics will be defined as the digital products, media tools and services that helped ISIS create and disseminate its messages. In other words, logistics are the materials used to form message assemblages, information flows and media of communication. Understanding the medium of communication is essential to understanding the message. In this chapter, I aim to answer the thesis’s primary question: Does the change in the means of access to new software and hardware logistical tools give ISIS superiority in information environments and prevent attempts of degrading its digital capacity?

To answer this question, I will examine the role of information as logistics within terror organisations from two perspectives: the framing of information and the transmitted object. While the former refers to acts of representation, the latter refers to the physical logistics of assembling and disseminating information. To do that, I adapted Raber’s (2003) model of information as paradigm.

The aim of this chapter is also to understand how ISIS deepened its roots in the information environments, which helped to maintain, shape and structure the organisation. Examining the
logistics of message assemblages and the channels of information flow within ISIS’ networks will lead to an understanding of the following:

- Message assemblages and mechanisms of information flows (including information retrieval and reproduction).
- The network logistics of the terror organisation (including digital and physical media logistics).
- Digital manoeuvre warfare that has occurred in the information environments.
- The marketing strategy of terror organisations (e.g., the production of HD horror propaganda videos as part of their PSYOP has become a marketing tool for promoting their terror narrative across networks).
- IO objectives and how these served ISIS’ political agendas in establishing the Islamic caliphate.
- The pervasiveness of the terror narrative across the digital spectrum.

To identify message assemblages and flows of information, it is important to trace and map networks of actants as suggested by Latour. Thus, the argument of this chapter is derived from ANT as a theory and methodology that explains the association between human and non-human actors in the network through processes of translation and enrolment. However, examining all media logistics and traces of message assemblages is almost impossible, due to the large terrains of logistical tools (digital and physical) harnessed by ISIS. In this thesis, I will highlight the most important software and logistical tools that have had a significant role in sustaining information flows and maintaining ISIS’ networking structure. These include Twitter, Telegram and anonymous sharing portals (JustPaste.it, Sendvid and dump.to). Telegram and anonymous sharing portals will be closely analysed in Chapter 6. Twitter is closely analysed in this chapter.
In this chapter, I attempt to scale and comprehend the volume of information sent across digital media platforms. Second, I explain the paradigm shift\textsuperscript{78} in ISIS’ logistics of information through the three aspects of Raber’s (2003) problem with information. Third, I highlight the produced content and channels of dissemination, including an analysis of the most circulated propaganda videos across media networks. Fourth, I draw parallels between ISIS’ propaganda media outlets (such as Al-Hayat and Al-Itisam) and mainstream media (such as Fox News and Al Jazeera), which together promoted ISIS’ narrative. To understand these parallels, I propose the concept of the collaboration networks of adversaries. Finally, in this chapter, I examine the content of production and evaluate how it empowered the terror network and maintain its structure. In this chapter, I answer the following questions:

- What media strategies have ISIS obtained to compete with its adversaries?
- How does ISIS maintain flows of information in the rapid changing environment?
- How has the ISIS gained control of the media narrative?
- How has media production logistics deepened the collaboration of networks of adversaries and empowered the terrorist’s narrative?
- How was the message of terror mediated so quickly?

The analysis of information content and information logistics infrastructure leads me to conclude that ISIS continues to empower its network.

### 4.2 Understanding ISIS’ Information Logistics

\textsuperscript{78} ISIS is distinguished from all other terror organisations in utilisation of digital media tools, information environments, producing HD media productions, swarm dissemination process of digital productions across digital media platforms, and manoeuvring to survive degrading operation.
ISIS has produced, and is still producing, significant amounts of data, including thousands of documents shared across anonymous sharing portals, millions of tweets, private and public messages across Twitter, thousands of sophisticated and simple video productions, blogs and messages via encrypted communication channels (e.g., Telegram and WhatsApp). Winter (2015b, p. 3) observed that ISIS produce an average of 38 propaganda materials (including videos, audio and texts) every day.

Due to the sheer volume of data produced by this network, we are witnessing a paradigm shift in terror communication. Making sense of such information requires frameworks and methodological approaches that include social network analysis, digital ethnography approaches, big data analysis and content analysis.

The processes and mechanisms of producing and disseminating such data are termed as logistics. Understanding the information and network logistics of ISIS would help its adversaries to counter its message. As argued earlier (see section 3.1), digital logistics assisted ISIS in crafting its message and maintaining its information flows and networking structure. The role of logistics is to produce, coordinate and transmit data and things (e.g., equipment and military services) from point to point. This includes tools of production and dissemination—hardware and software. Software tools include social media platforms, phone applications, sharing portals, photograph editing software, and video and editing programs. Hardware tools include cameras, computers, uniforms (such as the black and red uniforms in ISIS’ propaganda videos), symbols or icons (such as ISIS’ black flag), video editing machines, media points and centres, and filming devices. Overall, every digital and physical entity used by ISIS to produce and disseminate information is considered logistics.
However, according to Rossiter (2015) logistics “is not only an adaptive technology able to accommodate contingency. It is also a technology of penetration, seeping into reserves of life that exist beyond the world of supply chains” (p. 142). Media had a critical role in the war—and arguably, won the war—and as such, has become the new domain of warfare. This warfare includes the dissemination of propaganda, PSYOP, disinformation and distortion using internet technologies—particularly, social media platforms. ISIS has capitalised on the wide engagement with ‘participatory media’ (Jenkin, 2006), wherein digital media has become the new social operating system (Krieger & Belliger, 2014, p. 9). This new social operating system engaged communities in sharing information and enabled social networks to emerge. However, some of these social networks are also terror networks. Terror networks have utilised digital media logistics as digital weapons to boost its strategic narrative and execute its IO. As Afzal and Wallis (2016) argued, “Social media can be weaponised to support influence warfare operations; in turn, the ways in which hostile actors undertake information operations can provide insights into their own strategic objectives and organisational structures” (p. 77). Nissen (2015) proposed that “in contemporary conflicts … web-pages, internet-based web-television, social network sites (e.g., Facebook and Twitter), blogs and upload services (e.g., LiveLeak and YouTube) are being used as sophisticated weapon systems” (p. 10). However, to understand the sophistication of message assemblages, objectives of IO and the planning of ISIS’ flows of information, it is important to explore the logistical operation of this organisation.

Disregarding the sophistication and complexity of message assemblages, ISIS’ IO is based on a clear strategy (see Sections 3.4 and 3.5). The mapping of information logistics is required to understand the large quantity of information that has saturated digital media platforms. Through this mapping, ISIS’ strategies to optimise its information to construct centralised
and distributed messages can be understood. The logistical tools helped ISIS to assemble messages and maintain the flow of information at an operational level. Within this chapter, I will discuss overt logistical tools (e.g., Twitter and YouTube) and covert logistical tools (e.g., JustPaste.it and Telegram). The interaction between the overt and the covert logistical tools generates a dynamic loop of information as a result of interconnectivity and convergence between information environments. For example, disseminated data over Twitter was generated by JustPaste.it software. The content generated using covert logistical tools can be transmitted, coded and reproduced by another overt logistical media tool. Peters (as cited in Neilson, 2012) described what he called ‘logistical media’, which “arrange[s] people and property into time and space’. These are ‘prior to and from the grid in which messages are sent […] Logistical media establish the zero points of orientation, the convergence of the x and y axis’ (Peters, as cited in Nelson, 2012). Case (2013) argued, “Logistical media gesture to the roots of the transmission model of communication—the sender-message-channel-receiver-feedback model—to the foundational work in military science, network theory, telecommunications, and cybernetics” (p. 380).

That said, the feedback loop of information leaves traceable hyperlinks known as ‘signs’ for others to follow (see Figure 40). These signs are regarded as information signs (Raber & Budd, 2003). Information signs can also be physical, such as the black flag and red and black outfits used in ISIS propaganda videos. These signs are also known as a ‘pheromone trail’, which is intended to be followed by other network affiliates to coordinate the assemblage of messages, and optimise, retrieve and reproduce information through stigmergy.

---

79 Part of a large extended network that operates outside the geographical space of the physical network.

80 Stigmergy “is a term used in biology, from the work of French biologist Pierre-Paul Grasse, to describe environmental mechanisms for coordinating the work of independent actors” (Robb, 2007, p. 124). This
stigmergy work helps in maintaining the loop of information that brings the network into existence.\textsuperscript{81}

On a tactical level, the covert media logistics (e.g., anonymous sharing portals, and Telegram, WhatsApp and Signal applications) maintained an information feedback loop of information flows in the aftermath of the degrading operation. Overall, the categorisation of information logistics as overt and covert helps to understand assemblages of messages and trace of network actants. The feedback loop of ISIS’ networks aims to swarm Twitter with unprecedented and rapid processes of information, which creates a global reach for ISIS by

\textsuperscript{81} However, this mechanism will be discussed in detail in Chapter 7.
generating a network effect. It also enables ISIS to accomplish its strategic ambitions. As Neilson (2012) argued:

This seems a truism in the light of the developments of twentieth-century warfare and the civilian logistics revolution. Today it seems common sense that strategic decisions are limited by the resources at hand and tactical manoeuvres unfold within a situation defined by lines of information and supply.

These lines of information supply were enabled by access to the internet and via the use of communication templates, which makes information logistics visible.

To explain the key role of information in the formation of terror messages, the maintenance of information flows, establishment of networks of affiliates and enhancement of the connectivity of terror movements, I will apply Raber’s (2003) approach to information.

4.3  Understanding the Paradigm Shift in ISIS’ Logistics of Information

Raber’s (2003) three-paradigm approach to information explains the phenomenon of the paradigm shift in terror communication that occurred as a result of the rise of ISIS. Further, it explains how ISIS managed to leverage its networks by creating networks of affiliates around the world. The three paradigms are the physical paradigm, cognitive paradigm and social informatics. The importance of this approach was expressed by Skinner (2011), who argued that researchers must “examine these movements through the paradigms to better understand how participants seek and organize information, and how they leverage technologies to increase the impact of protest activities”. To build communication channels between welayats
and individuals, and create networks of affiliates around the world, ISIS invested in its IO strategy by swarming digital information environments.

This approach provided an understanding of how information was transmitted and retrieved across information environments; the volume of information disseminated; the dynamics of video productions; the processes of recruitment and radicalisation; the internal and external communication between ISIS members and affiliates; and how audiences perceived and interpreted information.

4.4 Physical Paradigm

The physical paradigm focuses on transmission, storage and retrieval through the development of mechanised processes; these processes are largely separate from individual interpretation or social contexts (Raber, as cited in Skinner, 2011, p. 6). The physical paradigm regards information as a physical object, which is recorded in ‘texts’ and other forms of media (e.g., video and audio). These objects can be “stored, optimised, coded, transmitted and retrieved when needed” (Skinner, 2011, p. 6). Images, texts, audio and video—regardless of medium—are regarded as tangible forms of information (Raber & Budd, 2003). Information is a sign, which may contain and text and content (Raber & Budd, 2003).

Social media platforms and other digital sharing portals have the mechanisms to envision information as transmitted objects, which enables information movements across multiple digital media environments. That information can be stored and retrieved (Skinner, 2011, p. 7). The assemblages of ISIS’ messages and the capacity of their information flows depend on these mechanisms. For example, the use of the hashtag as a message retrieval system
explains the pervasiveness of ISIS messages. Twitter’s hashtags mechanism permits the grouping of instant updates, which helps users to locate specific information almost instantly. Additionally, a simple search for ISIS information on archive.org or through the Google search engine will lead to stored information and archives of ISIS content.

Further, Cloudflare\textsuperscript{82} was accused of hosting ISIS content and thus, being a logistical tool in the proliferation of ISIS information. This service stores communication, texts, training materials and propaganda videos that can be retrieved any time (Appleweed, 2015). In May 2017, I identified over 2,000 HD video productions of ISIS on Scribd’s online service. These videos can be downloaded instantly after an annual fee of US$25 is paid (see Figure 41).

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figures/isis_videos.png}
\caption{Screen shot shows ISIS videos on scribd.com.}
\end{figure}

Developing on the idea of information as a physical object, Skinner (2011) raised important questions for the examination of social media platforms:

\begin{quote}
How do we define and classify ‘objective’ information when reading tweets or Facebook posts? Can we create a system to locate this information through summarizing vast numbers of tweets and pulling out only information about events
\end{quote}

\textsuperscript{82} A hosting company based in California.
that is corroborated by multiple participants? What shortcomings are there to this approach? (Skinner, 2011, p. 7)

Within the context of this study, additional questions have arisen. For example:

- How do jihadi and ISIS affiliates retrieve, generate and disseminate content across the digital networks?
- How do potential recruits and international audience interact with ISIS information flows?

These questions, along with Skinner’s (2011) questions, are beyond the scope of the physical paradigm and require a new approach: the cognitive paradigm.

### 4.5 Cognitive Paradigm

The questions identified in Section 4.4 cannot be answered through the physical paradigm, wherein information is understood as an object that is transmitted across a medium of communication (regardless of whether the medium is digital or non-digital). To answer these questions, the nature of the information itself must be determined, by focusing on how audiences’ value and engage with information. Therefore, the cognitive paradigm arose from criticism of the physical paradigm, which has been defined by Raber (2003) as “premised on the assumption that we can distinguish between tangible, formal objects, and expressions that possess the quality of being informative and intangible cognitive phenomena of knowing and being informed” (Raber, 2003, p. 91).

Interpreting information can determine individual participation and engagement; this can be achieved by surveying individuals to assess how they appraised information (Skinner, 2011, p. 9). In case of ISIS and its affiliates, the interpretation of ISIS’ terror messages can be
analysed to assess how this information affected recruitment, radicalisation and lone actor operations. Skinner (2011) noted:

Using the cognitive framework, researchers can survey or observe users and collect data about where they look for media related to different aspects of the protests. Such an approach allows us to ask questions about how people choose and appraise news sources, or whether those who saw the original videos versus the edited video have different perceptions of what happened. (p. 10)

This also explains the effect of producing HD videos, digital migration to Telegram, and other anonymous sharing portals to find news, and how Amaq and Dabiq media agencies became the most credible news source.

According to Skinner (2011), the cognitive paradigm also allows us to examine how activists, journalists and other parties engaged with the issues. Such work could draw heavily from Jenkins et al.’s (as cited in Skinner, 2011) notion of participatory cultures, which have “low barriers to participation and engagement, strong support for sharing, and informal mentorship” (p. 10). The cognitive paradigm could also be useful for understanding the use of trending topics on Twitter, which increases presence and broadens message input and output. Therefore, the cognitive paradigm explains ISIS members hijacking of trending hashtags on Twitter.

Further, the cognitive paradigm explains how the traffic on #IslamicState and #Khilafah reduced dramatically. That is, this theoretical approach explains the effect of the degrading operation on ISIS’ Twitter networks, as the number of participants (represented by the like,
reply and retweet functions) and consequently, the volume of information and traffic was reduced.

4.6 Social Informatics

While the physical and cognitive paradigms engaged with information as an object that individuals interact with, these paradigms failed to acknowledge how we interact with each other (Skinner, 2011, p. 11). Sawyer and Jarrahi (2014) claimed social informatics is ‘part of socio-economic research that examines the ways in which technological artefact and human social context mutually constitute the information communications technology ensemble’. Moreover, Sawyer and Rosenbaum (2000) consider this approach to include three orientations for studying ICTs: the normative (recommending alternatives to current models used by developers, information professionals, and policymakers), the analytical (creating theories related to technologies by conducting empirical studies), and the critical (studying a variety of perspectives related to these technologies). These three orientations could be applied to the study of social media and terrorism. The normative approach would be useful for those hoping to develop or disseminate more effective social media tools; the analytical would be useful for discussing trends in social media use and building relevant theories; and the critical would allow researchers to examine how social media use is viewed by non-users and how revolutions are discussed within social media (as cited in Skinner, 2011, p. 12).

As the social informatics approach explores the consequences of the use of ICTs on individuals, it is useful for understanding how media of communication (e.g., Twitter) have become tools to promote terror. Social informatic explains how loosely connected individuals become enmeshed in networks, how networks are established and how the public become exposed to terror messages. Understanding the intricacies of the effect of ICTs individuals,
enables researchers to understand how SMNs (e.g., Twitter) has been exploited for the purposes of radicalisation and recruitment and how individuals are inspired to conduct acts of terror on behalf of ISIS.

Social informatics allows researchers to examine social media use and determine how individuals are connecting to each other and staying updated about the events around them (e.g., through the use of encrypted communication channels, such as Telegram and WhatsApp). It has also been suggested that the tenacity of these movements is due, in part, to the fact that people are recording everything, including footage of events that may not have been caught by mainstream news crews (Madrigal, 2011). Social informatics would help researchers understand how exposure to information—which has been disseminated through social media and other digital media technologies—shapes individuals’ perspective (especially in regard to the processes of radicalisation and recruitment). Therefore, understanding this element of logistics may lead to how radicalisation and recruitment occurs. This approach defines individual disseminators and creators of terror content as social informants and seeks to explain their influence on potential recruits (e.g., Turjoman Sawtry and Shami Witness).

4.7 Social Media Platforms as Logistics

SMNs and other ICTs have been noted for their role in mediating terrorist communications and in galvanising social movements in the last decade (Aday et al., 2012; Castells, 2013; C. J. Cox, 2006; Garrett, 2006; Jefferson, 2007; Khamis et al., 2012). Prior to the September 11 terror attack on the US, Al-Qaeda harnessed the internet to mediate its communication via email to a global jihadist movement and its sympathisers around the world (Levin, 2011). Al-Qaeda’s use of digital information sharing and communication tools such as email, Paltalk
video chat and the WWW helped them to coordinate attacks, recruit jihadi, mediate communication, spread their ideology and raise funds (Sageman, 2004; Weimann, 2010). The proliferation of social media platforms, especially Twitter and Facebook:

> With 284 million and 1.35 billion monthly active users worldwide (in the 3rd quarter 2014), respectively, [has meant that] the terrorism communication landscape can be radically reshaped by the speed, reach, affordance, and ease of uploading voice, text and imagery data via mobile devices for immediate visualisation effects. (Chatfield, Reddick & Brajawidagda, 2015, p. 3)

In Section 4.8, I will focus on Twitter as the most prominently used social media platform for ISIS’ communication. However, it is important to note that when examining the logistics of ISIS’ network, Twitter is only one node in a wider social media ecology (Conway et al., 2017, p. 7).

### 4.8 ISIS’ Information Operations on Twitter

Twitter has permitted a new means for terror communication. The information distribution mechanism of the microblogging social media platform has become ISIS’ hub to mediate communication and disseminate terror messages. ISIS has even claimed Twitter as their own platform (see Figure 42).

*Figure 42. The Caliphate Twitter.*
As discussed in Section 3.6, part of ISIS’ IO strategy is to swarm Twitter to control the narrative in this platform. This would explain the increase of the traffic on Twitter in the period between 2013 and 2014. Berger and Morgan (2015) claimed that since the emergence of ISIS:

Twitter’s user base grew by approximately 30 percent in 2013, while ISIS’ user base nearly doubled. The Twitter user base grew 20 percent in 2014; the number of ISIS supporters on Twitter nearly tripled during the same period (within the limits of the sample). This [is] reflective of strong growth, but also reflects anecdotal observations of increased adoption of social media by jihadist extremists starting in 2013. (p. 17)

In Sections 4.9–4.11, I aim to highlight the importance of the Twitter platform in enhancing ISIS’ IO and explain how ISIS utilised Twitter to form of its message across other platforms. The information presented in these sections is obtained from ISIS’ Telegram channels and other pro-ISIS accounts on Twitter. There are two motives underpinning ISIS’ utilisations of Twitter as their main domain, which I refer to as intuitive and technical.

### 4.9 Intuitive and Technical

In the Sections 4.9.1–4.9.3, I outline the trends in the infrastructure and mechanisms of sharing information of Twitter.

#### 4.9.1 Dissemination Mechanisms—Retweet, Reply, Like and Hashtag

Twitter’s dissemination mechanisms have allowed ISIS to exploit the platform to enlarge its audience base and expose its information and propaganda to most of Twitter account
holders. Using these mechanisms effectively has enabled ISIS to generate and diffuse an estimated 90,000 tweets every day. Daily tweeting was encouraged by ISIS’ commander and spokesperson, Abu Mohammad Al-Julani. He claimed that participating in Twitter and sending messages across other digital media environments is partaking in jihad. As stated in Figure 43, Al-Julani commands his supporters to “make your computer as a bomb, be present at Twitter, upload information to Twitter, write, upload and diffuse. Don’t corner yourself on Telegram”.

![Figure 43. ISIS encourage its followers to use Twitter to disseminate, tweet and upload.](image)

Winter (2015a) suggested that “hashtags—which Twitter neither suspends nor blocks—are now Islamic State’s [ISIS’] preferred vehicle for dissemination. By using an organically defined set of tags, Islamic State’s official disseminators can simultaneously be effective and low-key” (p. 11). ISIS uses what they call Twitter bombs, which redirect trending hashtags to Twitter websites and material related to ISIS. In the autumn of 2014, there were at least 45,000 Twitter accounts used by ISIS supporters; 73 per cent had an average of 500 followers, while others had up to 50,000 followers. The Al-Battar Media Group—with 32,000 followers—seeks to mobilise Twitter members to support ISIS by translating ISIS’ releases through independent media wings (Liang, 2015, p. 5).
4.9.2 Interconnectivity and Networking

The infrastructure of Twitter enables connectivity by default. This potential for connectivity was the reason ISIS established itself in this platform. Its basic function and purpose of use is based on sending a short, 140-character message. These messages are being communicated using dissemination mechanisms highlighted in section 4.9.1. To enhance connectivity, third-party bots have been established to tweet on behalf account subscribers. ISIS has harnessed this function—as part of its IO strategy—to encourage individuals to engage with real fighting through the systematic presentation of flows of information.

Svetoka (2016) reported:

> Daesh [ISIS] does not rely solely on their ‘media soldiers’ and volunteers to create and distribute content, but constantly look[s] for the ways to maximise their presence on social networks by using technological solutions. Automatically created content distributed by bots or apps provides a cheap and easy option for dramatically increasing Daesh reach. (p. 37)

One of the most infamous bots used by ISIS is ‘The Dawn of Glad Tidings’.

Prucha and Fisher (2013) claimed,

> Twitter functions as a beacon for sharing short-links to content dispersed across numerous digital platforms … Today’s social media zeitgeist facilitates emergent behaviour producing complex information-sharing networks in which influence lows through multiple hubs in multiple directions.

Alexander Towbridge (2014) observed that “the use of automatically generated content, by spamming (e.g., ‘Twitterbombs’—sending out thousands of similar messages at once) or fake
identities (e.g., trolls, sock puppets, bots) … [seeks to] spread a message and minimize alternative voices”.

The NATO StratCom (as cited in Svetoka, 2016) observed that to enhance their networking via Twitter:

Daesh [ISIS] is adding geo-locations to its hashtags (e.g., ‘State of Homs’ or ‘State of Raqqa’), which allows members to ‘disseminate target information to specific regions and any independent actor to share information within their region using a combination of Islamic State [ISIS] hashtags as well as geographic keyword tagging’. (p. 16)

Another tactic used by ISIS members to stay connected is the use of event-specific hashtags (see Figure 45). For example, ISIS members encouraged followers to swarm Twitter using #CloseIncirlik.

Moreover, Twitter enabled the creation of groups—similar to Facebook, Telegram and WhatsApp (see Figure 46 for the ‘Baqiya Family’ group). According to Amarasingam
ISIS members established a network called Baqiah\textsuperscript{83} Family. It is hard to say how large the Baqiya family is, but one estimate gave them 40,000 members, and growing. The vast majority are aged 20–28, but quite a few are 18 or younger, male and female.

\textbf{Figure 46.} A message to join the ‘Baqiya Family’ group and a message from Usudul Islam to ‘Baqiya Family’.

\textbf{4.9.3} Convenience—Anonymity, Mobile Phone Applications and Ease-of-Use

One of the intuitive dynamics of Twitter is its convenience. This includes the availability of the mobile phone app, the one-to-one messaging service and text upload functions. Propaganda videos and text were mostly uploaded from anonymous sharing portals, such as JustPaste.it and Sendvid. As explained earlier, the convergence of digital media entities, through the use of information signs to direct audiences from platform to platform, has increased interactivity and maintained flows. As NATO StratCom (2015, p. 39) noticed, ISIS

\textsuperscript{83} Baqiah is an Arabic word means staying.
uses Twitter as an umbrella platform that connects the various sources into one easily searchable, browsable information index. Berger and Morgan (2015) reported:

Smartphone usage among ISIS supporters, according to primary app used for tweeting … [suggests that] among users of the three most popular phone types, 69 percent had downloaded a Twitter client from the Google Play store or Google.com. Another 30 percent used a client downloaded from the Apple iTunes store, and about 1 percent had downloaded a client from Blackberry.com. (p. 26; also, see Figure 47)

![Smartphone Usage](image)

*Figure 47. Mobile phone usage among ISIS supporters. Source: Berger and Morgan (2015).*

Anonymity also makes Twitter a convenient platform to use for ISIS. ISIS members’ identity is always kept secret through the use of pseudonyms (such as Shami Witness, Asad Caliphah and ibn Dawlah), which allows them to evade capture and persecution. While this section has addressed the mechanisms, information loops and dynamics of the Twitter platform and how ISIS utilises it, it is also important to assess ISIS’ objectives in adopting Twitter as its primary network for its IO.

### 4.10 Objectives of Usage
The mechanisms of message generation and distribution that are possible via Twitter have defined ISIS’ usage of this medium. Through their communication—and particularly, under the hashtag #elzamthagrak (i.e., stay in your domain)—two main organic reasons have emerged for ISIS’ adoption of Twitter as its main hub for communication: first, the partaking in media war and second, the spread of propaganda to enhance the processes of recruitment and radicalisation.

4.10.1 Partaking in Media War

Figure 48 demonstrates how ISIS has used the media as their battlefield—media has had a critical role in the winning and losing of wars. According to Al-Qaeda leader Ayman Al-Zawahiri, half of the war is fought in the media. Twitter presented a unique battlefield, in which ISIS chose to fight. As stated in Figure 48, ISIS outlined the main purpose behind use of Twitter. When translated, it says that the more ISIS affiliates are active on Twitter, the more the US lose the media battle. Liang (2015) observed, “ISIS has become the world’s first social media war where there are some individuals who are tweeting almost 200 times a day and whose tweets are attracting tens of thousands of followers” (p. 6).

Figure 48. Message forwarded by @Kawasir_AlNashr on Telegram channel.
The importance of the media war was also highlighted by Nashir Political Services, as they described the media as the strongest weapon in the present time (see Figure 49).

Ultimately, as stated in the *Oh Media Correspondent, You Are a Mujahid Too* publication, the jihad of the tongue is as important as physical jihad. This notion was expanded to encompass Twitter and therefore, Twitter has become the preferred medium to conduct the jihad of the tongue (see Figure 50).

*Figure 49. Message forwarded from Nashir Political Service, Telegram channel.*

---

84 A multi-language ISIS Telegram channel.
4.10.2 Radicalisation and Recruitment

A study of ISIS’ Twitter networks can help to explain how and why the number of ISIS fighters has grown from 2,000 fighters in 2012, to 40,000 fighters in 2014. According to Berger and Morgan (2015), there are 46,000–90,000 ISIS Twitter accounts and almost every account has approximately 1,000 followers. According to Schmitt (2015), these accounts produce almost 90,000 tweets per day, including responses to other social media platforms. ISIS’ huge account base on Twitter, combined with the volume of disseminated information across the Twitter platform, has profoundly contributed to ISIS’ processes of recruitment and radicalisation. These processes were accelerated by two factors. First, ISIS used web links (i.e., information signs) to its own web pages, on which more information was available, allowing individuals to stay connected. This also safeguarded ISIS’ digital base, to protect against account suspensions from Twitter. Second, the use of multiple languages targeted potential recruits from the West to commit an act of terror on behalf of ISIS. For instance,
John Appleweed (2015) noted, “1 in every 5 ISIS supporting twitter accounts select[ed] English as their primary language”.

To achieve one of its IO objectives (radicalisation and recruitment), ISIS aimed to “generate affiliates in your houses, and we will turn them to Mujahedeen, we will raise them on the footsteps of prophet Mohammed” (see Figure 51). Svetoka (2016) explained how ISIS utilised the mechanisms of Twitter’s platform for radicalisation purposes, suggesting that:

Daesh [ISIS] uses Twitter as a connecting medium for all of its distributed content all over the web—videos, photos, messages, and press releases posted in uncontrolled and unsupervised sites (such as JustPaste.it or archive.org). By using these pages, Daesh can reach supporters who have previous knowledge of the locations of those messages, however for recruitment and publicity they must share the links to these pages in public domains, such as Twitter. (p. 34)

Figure 51. Message of recruitment disseminated to ISIS’ Twitter feed.
4.10.3 Spread of Propaganda

ISIS strategically used its Twitter platform to spread its propaganda. Videos, texts, memes, infographics, links to its magazines and other media is widely shared across the platform. Horror videos—live broadcasted from the battlefield—depicting victories and utopian messages representing a wonderful life under the Islamic caliphate are uploaded daily by ISIS followers. Kelly (2014) observed ISIS’ threefold branding on Twitter, claiming that brand one is “ISIS as the goodwill guys”. Several of their Twitter feeds often depict soldiers playing with children, distributing food, performing social services and hanging out with kittens. They strive to showcase the humanity of ISIS, mixed in with Western familiarities. Fighters also tweet about how much they love Disney movies and strike grinning poses with jars of Nutella (see Figure 52). The second aspects of ISIS’ brand on Twitter “is action-man themed”. It matches traditional ideals of masculinity with the glorification of war. It portrays the conflict as honourable, which is typified by the sale of ISIS hoodies and t-shirts online. Through this aspect of their brand, ISIS present themselves as charming freedom fighters.

Figure 52. Propaganda material posted to Twitter for recruitment purposes.

The third aspect of the brand “depicts ISIS eradicating evil in the name of Allah, reminding its followers to honour the supposed peace a global caliphate would create, which vindicates
the barbaric means the terrorist organisation takes to reach its ultimate end” (Kelly, 2014). This type of propaganda is specifically designed to reach naive, uneducated Muslim youth living in the West. The use of popular memes as propaganda “aimed to infect ignorant receivers with jihadist concepts, to recruit them or only to improve the organisation’s image among the youth” (Lakomy, 2017, p. 42). Conversely, infographics “were designed to reach more demanding and conscious audiences, who usually need illusionary facts and statistics, in order to strengthen or to change their attitudes” (Lakomy, 2017, p. 42). Thus, the Twitter had a key role in ISIS’ execution of its IO strategy, as the medium permitted the proliferation and distribution of ISIS propaganda.

4.11 How ISIS Games Twitter

ISIS’ affiliates and members used Twitter in unprecedented ways to execute its C2 operations and maintain its information flows. ISIS swarmed Twitter to establish centralised Twitter accounts, create an abundance of independent affiliates accounts, utilise active hashtags, create bots to sustain and increase information flows (Klausen, J., Marks, C., & Zaman, T., 2016), and add logistic aid to reproduce and retrieve data. ISIS games (i.e., manipulates) Twitter in many ways.

4.11.1 Use of Active Hashtags

Part of ISIS’ propaganda strategy is making use of active hashtags to enlarge its audience base (see Figure 53). As discussed in section 4.3, the mechanism of hashtags enables wider distribution across the Twitter network. For example, after the Nice attack in June 2015,

85 Memes are combinations of a picture combined with a short text message.
#PrayForNice was trending and therefore, ISIS encouraged its followers to disseminate its messages of fear using the same hashtag (see Figure 53). Twitter and Facebook are your domain #suicidewithoutbelt.

![Data collection](image)

*Figure 53. An example of active Twitter hashtags after the terror attack in Nice, France.*

As demonstrated in Figure 53, followers were instructed to use the #PrayForNice hashtag, because it was trending and would permit the spread of fear to the crusaders. They were also instructed to upload their material in French. Through hashtag activism, or *hashtivism*, ISIS has demonstrated agile hashtag use. Fisher (2015) reported:

> ISIS has used tactics which are familiar to digital marketers, such as organizing hashtag campaigns on Twitter to generate internet traffic and working to get those hashtags ‘trending’ by piggy-backing on hashtags around unrelated events, such as those about the World Cup or the iPhone 6, which they add in their messages about Islamist propaganda, to increase their reach still further.
Kelly (2014) also noticed that ISIS:

hijack[s] trending hashtags, flooding topics like the #WorldCup2014 and Scottish independence with pro-ISIS messages. They enlist the help of their supporters to tweet at certain times of the day using particular hashtags (see Figure 54). Often these campaigns distort the results of Arabic Twitter accounts like @Activehashtags, which promote each day trending tags. It results in ISIS propaganda effectively spreading into hundreds of thousands of Twitter feeds around the globe.

![Figure 54. An example of active Twitter hashtags after a terror attack in Germany. Source: Gazo Telegram channel.](pic.twitter.com/FjqqltxxX6)

Further, Nissen (2015) explained the dynamics of use of trending hashtags and its purpose. He claimed that:

The strategy also relies on having these ‘disseminators’ using hashtags crafted to look like grass-root initiatives exploiting ‘astro-turfing’ techniques, in some cases also hijacking existing hashtags, and thereby lending third party credibility to the narrative. Not least ‘hashtag hijacking’ where IS uses # of trending topics to get
attention from audiences how would normally not search for IS content or # (Nissen, 2015, p. 50).

4.11.2 Command and Control Operations

As part of its C2 operation, ISIS established a centralised Twitter account to communicate its messages to a multitude of independent actors across the Twitter platform. For that purpose, the most prominent media arms of ISIS have deepened it roots in the platform. For example, Al-Hayat, Al-Itisam, Ajnad and Al-Furqan were responsible for maintaining flows of information. Hundreds of propaganda videos were produced by these media wings and shared using on Twitter. According to Liang (2015), Al-Hayat Media Centre “was responsible for posting almost 40,000 tweets in a single day as IS [ISIS] marched into Mosul” (p. 6).

In addition to centralised Twitter accounts many ISIS leaders and affiliates established their own accounts on Twitter. For instance, Chatfield et al. (2015) used social network analysis to understand ISIS’ then phenomena of tweeting propaganda. By focusing on ISIS’ content generator and disseminator, known as @Shamiwitness, Chatfield et al. (2015) noted that @Shamiwitness increased user benefits by:

(1) by controlling network operations to increase intrinsic benefits through enhanced information quality, reputation, and other value-added services to attract new account holders (network size) and (2) by increasing extrinsic benefits. In order to increase the extrinsic benefits, @shamiwitness, for example, can entice his social-media
network users to actively engage by issuing their own tweets, replying to his tweets or retweeting his tweets to their own ‘followers’.\(^8\) (p. 6)

This dynamic has helped ISIS, by leveraging its network audience (see Figure 55).

![Data collection](http://web.archive.org/web/20160814184303/https://justpaste.it/gg5)

http://justpaste.it/xbhp
http://justpaste.it/xbho
http://paster.org/m/jczuw/
http://copytaste.com/au?498

\textit{Figure 55. ISIS shows how to connect multiple accounts in one platform.}

Another dissemination tactic used by ISIS to leverage their network audience to great effect is the use of content that is translated in multiple languages. As Berger and Morgan (2015) noted:

As far as content, many users tweeted in more than one language, sometimes as part of ISIS social media strategies to direct messages at external target audiences, such as when it publicizes the beheadings of Western hostages. Tweets also frequently featured a mix of languages, such as English hashtags attached to Arabic content. (p. 14)

\(^8\) Who are not members of the @shamiwitnes network but belong to separate social-media networks.
4.11.3 Manoeuvre Warfare

To prevent suspension and sustain its flows of information ISIS managed to set rules for its members and affiliates to follow. These rules were marked with #suicidewithoutbelt. Figures 56, 57, 58 and 59 summarise the ways ISIS implemented its information manoeuvring operations on Twitter. These tactics include:

- Guidelines on how to open Twitter accounts without using a phone number.
- The hiding of location, through a fake location strategy.
- Guidelines to prevent detection and tactics to follow affiliates.
- Supply of ready Twitter accounts via @bankansar.
- Filtering accounts and removal of intruders.

Joseph Shaheen (2015) observed how ISIS members manoeuvred in Twitter to prevent detection and avoid suspension. He noted:

Other Daesh [ISIS] methods to avoid counteractions on Twitter include: - Using independent actors to amplify the central message created by Daesh originators, while maintaining the independent nature and behaviour of these individual actors. - Signalling to each other in order to avoid the discovery of Daesh accounts. - The use of symbols and other tricks in account information and posts to avoid detection. This is why strict reliance on automated image detection becomes unsustainable. - Speedy and adaptive recovery after account closure—to regain the previous levels of influence new accounts include requests such as asking others for 1,000 retweets of the new account. - Using system vulnerabilities, for example being able to change usernames and their URLs in Twitter. (Shaheen, 2015, pp. 17–20)
Overall, so far, this research explored the role of information and its logistics in assembling and diffusing messages of terror. This chapter has also examined the mechanisms of information logistics and the ways it has aided ISIS’ flows of information and networking. Further, this chapter has identified that Twitter as a medium of communication has been central to ISIS performing, assembling and leveraging messages.

However, understanding digital logistics—as both a physical material and in its association with human actors—requires a methodological approach to identify how digital media logistics (i.e., network actants) established networks and how these networks transformed the message of ISIS. For this purpose, I will use ANT.

4.12 Actor–Network Theory

To this point, this thesis examined the role of digital media logistics in enabling of information warfare and IO in conflicts occurred during Israel–Gaza–Lebanon wars, the Arab spring uprisings, Al-Qaeda and ISIS. To understand how networks such as Hezbollah and Hamas won the information war against Israel and how networks of rebels emerged so quick in Syria and Iraq, and how ISIS depended on digital media platforms, tracing and mapping of information logistics is important. As Mitew (2008) argued, “Only a mapping tactic that opens its eyes for the intensities performed by heterogeneous entities, neither subjects nor objects, will be capable of displaying the full spectrum of logistics upholding an otherwise impossibly ephemeral homogeneity”.

87 Latour (1999) himself had argued that ANT is not a theory of the social, subject or nature but a “very crude method to learn from the actors without imposing on them a priori definition of their world building capacities” (Latour, 1999: 20). However, in 2005, he reconsidered ANT as theory.
This thesis argues that information logistics helped in creating decentralised C2 operations, IO and enabled information warfare by enrolling information environment and other digital logistics to the network. This also helped in creating distributed networks, which permitted the exchange of information between human actors, as the function of these networks enabled information generation and dissemination in a dynamic loop. The program of ANT is a key to understanding the logistics of ISIS’ networks. Thus, understanding networking means, as Krieger and Belliger (2014) noted, “understanding those normative principles that guide those particular communicative activities that build, maintain, and transform networks. This is where new media studies come in” (p. 9).

However, as this thesis proposed in the first use of ANT as a framework to understand terror networks, Callon (1986) suggested that a network is built through a four-step process of translation: problematisation, interressement, enrolment and mobilisation. The first step in building a network is problematisation, which he described as the stage in which an actor makes itself indispensable to others. Callon (1986) stated that in this stage, the primary actor attempts to identify the problem and define the role of actors within the network. In reflection on ISIS, the problematisation is how to declare caliphate. Before ISIS, Al-Qaeda was hopeful to declare caliphate, but worried about its consequences (see Section 3.7).

The second process of establishing a network is by negotiating with other actors, which is interressement. This means interesting and attracting an entity by coming between it and some other entity (Law, 1987). During this stage the primary actor will need to impose the identities and define the roles of the other actors so that they will achieve their own goals when they join the network. In the case of ISIS networks, this is the most important stage. To establish a caliphate, ISIS must define their identity by negotiating process with locals to
accept the idea. Intéressement can be achieved through ‘seduction, force, and persuasion’ (Callon, 1986).

If intéressement was successful, this leads to the third set in ANT: enrolment. Enrolment occurs when actors accept the roles they have been given and enrol in the network. When defined interests, goals and identities are established, the mobilisation process emerges.

According to Krieger and Belliger (2014), establishing actor networks “requires processes, performances, socio-technical rituals, and enactments […] They are driven by the dynamics of making connections, of binding things together, of extending associations, of “translating” and “enrolling” actors into networks”. As Ashino (2010) explained, “In order to exchange data among heterogeneous materials databases, however, some kind of translation table for materials data is essential” (p. 59). The innovation translation approach draws on the sociology of translations, more commonly known as ANT. The core of this approach is translation (Law, 1992), which can be defined as: “the means by which one entity gives a role to others” (Singleton & Michael, 1993, p. 229). The enrolment process leads to the establishment of irreversible networks; however, to do that, Callon (1991) suggested that “actants needed to be organised”.

Understanding the agency of non-human actors—such as digital artefacts, information environments, toolkits and techniques—is necessary to trace network actors. Additionally, understanding network assemblages, mechanisms for the flow of information and logistics is essential in identifying network actors. As Krieger and Belliger (2014) contended, “Flow

---

I proposed this as the second fold of my argument.
opens up black boxes and transforms purely functional intermediaries into actors, participants, and mediators. When interactions among large numbers of actors become the rule and knowledge reconfigures itself into a cloud” (p. 144). To understand why and how ISIS, as a terror organisation, interacts with multiple digital media environments to assemble and disseminate its message was identified by Stern and Modi (2010), who argued that “terrorist[s] respond to changes in their environments by changing their mission and changing their shape. What is important in such events is that information logistics is essential in disseminating messages of terror” (p. 282).

In *Interpreting Networks*, Krieger and Belliger (2014) described networks as communicative action “in the sense of making connections and associations’ and therefore, communication is made possible by and is dependent upon media” (p. 9). In examining Latour’s program of ANT, Krieger and Belliger (2014) argued that it is important “to follow the actors in their laboratories, in the rainforest, in the factory, and describe how they make associations, connections, relations, and assemblies linking actors together up to the level of global collectives” (p. 38).

To establish the accounts of ANT, it is important to understand the key aspects of human and non-human object relationship. For this purpose, I have divided the logistical operations of ISIS into two categories: software and hardware logistics (see Figure 60).

From an ANT perspective, the associations between hardware and software logistics produced actants (Latour, 2005, p. 54). They are conceptualised as actants because they simultaneously act and are acted upon (Latour, 2005, p. 54). Actants, whether human or non-human, always have agency, which refers to the ability to make a difference in the
interactions between networks (Latour, 2005, p. 71). In other words, agency means “that they make a difference: hitting a nail with and without hammer, boiling water with and without a kettle, fetching provisions with or without a basket” (Latour, 2005, p. 71). Agency and action can be associated with human and non-human elements (Latour, 1999). This also applies to digital media tools, mobile phone applications, malware, military clothing and weapons in the context of action taken by ISIS jihadi. To apply this to ISIS’ terrorism, an individual jihadist who has access to digital technologies, weaponry and video production equipment may commit an act of terror. According to Latour (as cited in Architte, 2012, p. 10), “Action is therefore not the property of humans only but of associations of actants”. Accordingly, one of the main strengths of ANT is that it allows the tracing of actors in a network, based on their actual role in the flow of agency.

Figure 60. Diagram of ISIS’ logistics. Illustrated by the author.
In case of ISIS, the enrolment of media production experts (such as cameramen, post-production editors and producers) and the establishment of media production outlets (such as Al-Hayat and Al-Furqan) is essential to enrol actors in the network. These instances illustrate the dynamic and mutual influence between humans and non-humans. Further, they demonstrate the indeterminacy of the actant; at times an actant is “a power which enrols and dominates or, by contrast, an agent with no initiative which allows itself to be enrolled” (Callon, 1999, p. 182).

From ANT perspective, new sharing media technologies serve as information intermediators. Laura DeNardis (2014) argued that ANT “would perhaps refer [to] this phenomenon as regimes of delegation carried out by technical intermediaries that are often “black-boxed” and overlooked by end users” (p. 257). According to Krieger and Belliger (2014), “The more intermediaries there are [.,] the larger network becomes. The larger network becomes the more stable and therefore the more real it appears” (p. 113). In a further elaboration by Krieger and Belliger (2014) they stated that “the larger [the] network, the more effort is constantly going on to mobilize, translate and enrol actors, to create associations, and add intermediaries” (p. 113). Building an actor network means making associations, connections and links between as many heterogeneous elements, regardless of whether these elements are human or non-human, individual or collective, or subjects or objects (Krieger & Belliger, 2014, p. 114).

In this context, the black box is a conceptual metaphor developed in ANT to describe the network assemblages that function so well that their internal logistics are opaque from the

---

89 I will analyse auxiliary media such as Telegram and Anonymous sharing portals from black-boxing terminology. See 6.4.
outside (Callon, 1986, p. 31). Black boxes are created through what ANT terms as “acts of translation”, in which actors are first enrolled in the network and then work to stabilise it from the inside, which creates the appearance of a monolithic assemblage (Besel, 2011). From the perspective of the case studies in this thesis, the black box concept highlights how ISIS maintains its networking structure by adaptively shifting operations to lesser known online sharing portals (see Section 6.6). Opening a black box allows us to examine the ways in which “a variety of social aspects and technical elements are associated and come together as a durable whole” (Cressman, 2009, p. 6). The notion of opening and examining a black box is possible, because when focusing on a black-boxed entity that is seemingly homogenous from the outside, ANT sees “processes, performances, socio-technical rituals, and enactments […] driven by the dynamics of making connections, of binding things together, of extending associations, of “translating” and “enrolling” actors into networks” (Krieger & Belliger, 2014, p. 9). The same could be said for the role of online sharing portals, mobile phone applications and other technical assemblages enrolled in the networks of ISIS affiliates.

Thus, the rapid processes of information production and dissemination of propaganda videos is another network strength ISIS maintains in the Twittersphere. This network strength is dependent on the establishment of network connectivity and controlled flows of information. From a networking perspective, ‘flow’ can be described as:

on one level … the movements of contents through the various connections within the network. Flow in this sense refers to the fact that everything is moving through networks in one form or another, goods, services, money, people, information, etc. On another level […] flow refers to unpredictable activities and influences of all actors within a network. (Krieger & Belliger, 2014, p. 142)
As Latour (2005) stated, “A network is nothing more than the “trace left behind by some moving agent”. Networks should not be understood as stable social structures, but as “flows of translations”’ (p. 132).

It can be argued that these new sharing portals created a new terror socio-sphere. According to ANT, this socio-sphere “consists neither of objects nor subjects, but actors, and mediators. The affordance of digital media makes it increasingly difficult to deny any actor voice in the collective” (Krieger & Belliger, 2014, p. 187). These new sharing portals empower ISIS’ message to a large extent. From an ANT perspective, the new sharing portals enhance connectivity in the network by adding more actors and mediators, which becomes “more viable in global network society” (Krieger & Belliger, 2014, p. 188). Therefore, it can be said that ISIS has created a new paradigm shift in terror communication that established a global network of affiliates who acted on its behalf in the world at large. To understand the physical and cognitive paradigms, the highlighting of logistical media actors and content produced by these media outlets is essential.

4.13 ISIS’ Media Outlets

ISIS has established many media outlets, such as Al-Hayat, Ajnad and Al-Itisam, and harnessed the power of the existing media outlets of its predecessor Al-Qaeda, such as Al-Furqan media. ISIS has also established a radio channel (Albayan), English magazines (Dabiq and Rumeyah) and a 24-hour internet television station (Khaliphalive.tv). Further, beside the establishment of terror mainstream channels, through which ISIS maintains its network structure and flows of information, ISIS also adapted a new network strategy by establishing an arm in every province or territory they subdue. Every Welayat (e.g., the
territories in Raqqa, Syria; Barqa, Libya; and Sinai, Egypt) is responsible to produce their own media contents in alignment with ISIS’ propaganda to serve its political agendas.

In this section, I highlight the productions of these media outlets that acted as physical logistical media production tools. The media outlets did this by producing terror videos that helped ISIS in creating a global network of affiliates and maintaining their information flows (see Figure 61).

Al-Hayat was established in May 2014 and was based in Raqqa\(^90\) of Syria, the second largest province controlled by ISIS in 2014. Al-Hayat Media Centre is considered the mouthpiece of ISIS, which is akin to the relationship between Al Jazeera and Al-Qaeda. However, Al-Hayat also acted as a ministry of information for ISIS. Al-Hayat Media Centre introduced itself on its WordPress blog (as cited in Atwan, 2015) as:

The media wing of IS [ISIS] English Media centre is addressing Muslims in several foreign languages […] its versions of high-quality and highly sophisticated technology … match global media channels […] although they hope the beginning of modern [sic]. Al-Hayat has adapted [a] 21[st] century approach to spread[ing] jihadist propaganda and shown unique ability to use western media style to their advantage … under the leadership of Ahmed Abosamra, a self-radicalised individual of Syrian origins, who was born in France in 1981. Abosamra[,] who is an IT and telecommunication graduate[,] returned back to Syria during the Syrian revolution in 2011, then he joined the Islamic State in Raqqa in 2014 were he masterminded the slick, high-production videos for Al-Hayat media outlet.

---

\(^{90}\) I invite the reader to consult the timeline of the ISIS operation provided in this thesis on page xvii.
Al-Hayat release regular one- to two-minute short films called *Mujatweets* (an abbreviation of mujahedin tweets), which depicts the daily life of mujahedin (i.e., holy warrior) while on and off duty. They also represent a utopian image of life under Islamic caliphate. Many *Mujatweets* episodes show foreign fighters expressing their happiness, encouraging others to join their cause and explaining why all Muslims should make Hegira (i.e., migration) to the Islamic caliphate. The most popular episode on YouTube was “Why Did You Come to Jihad, Uncle?” (which no longer exists, as Google waged war against ISIS use of YouTube channels to promote its propaganda videos). Most *Mujatweets* propaganda videos were recorded in many languages, such as French, German and Russian, allowing a broad audience to access and accept the invitation to live under the utopian Islamic caliphate. Additionally, Al-Hayat was behind the release of *Dabiq* online magazine.
After Google launched its massive operation to counter ISIS’ propaganda messages, YouTube deleted all accounts associated with Al-Hayat media productions and other ISIS affiliate productions.

The Al-Hayat Media Centre is ISIS’ media wing that produces video content. In July 2014, Al-Hayat distributed 11 releases in English (a new release every 3 days), which were shot in HD with proficient editing and consistent branding. Even after ISIS fighters die, they are kept alive by continuous images, videos and statements. Before ISIS launched its attack on Mosul, a city of 1.5 million people, it released a film called *The Clanging of the Swords IV* (Liang, 2015, p. 6).

Al-Furqan was originally the mouthpiece of Al-Qaeda and was established by Abu Musab Al-Zarqawi in Iraq in 2006. It served under ISIS after they took control over Mosul in April 2014. The establishment of Al-Furqan Media’s production in November 2006 aimed to target Western audiences as the produced materials was translated into multiple foreign languages, particularly English and French. Later, their media production was focused on jihadist *Nasheeds*. Al-Furqan has produced whole television series glorifying ISIS’ achievements, such as the films *The Land of Epic Battles* and *Flames of War*. It has produced its infamous production called *Cubs of Caliph*, which depicted child fighters executing Russian and Israel spies in slick HD video production. It also shows the Australian terrorist, Khaled Sharouf, and his children holding up severed heads. In February 2015, Al-Furqan produced the video of a captured Jordanian pilot, Muath Al-Kasasbeh, being burned alive. Al-Furqan is considered the production arm of Al-Hayat Media Centre; all of its video content is first disseminated by Al-Hayat Media Centre.
Al-Itisam also served under Al-Hayat Media Centre. Al-Itisam is based in Syria and responsible for gruesome HD productions. Most of their HD production can be found online at https://akhbardawlatalislam.wordpress.com. The most recent production is called *Defeating Safawies*. Al-Itisam also is responsible for press releases and communication from the Caliph’s office to local residents. In many ISIS videos, particularly the ones presented by John Cantlie, I have observed Al-Itisam kiosks, where local residents can obtain information and press releases.

Ajnad is based in Iraq and was established in 2014. It specialises in producing jihadi *Nasheeds*. Jihadi *Nasheeds* production is very important during wartime, to spread the spirit of jihad when presented alongside graphic images of propaganda videos. Lemieux and Nill (2011) have highlighted the role of music in jihadi propaganda, particularly its role in presenting individuals with lyrics that compel them to “engage in deeper processing and consideration” (p. 144). Steve Rose (2014) also observed:

> The more violent images from ‘The Flames of War’ have also been edited into a rapid-fire, steroidal action montage accompanied by a recruitment Nasheed, or hymn. The song lyrics sweep across the screen, karaoke-style in Latin-script Arabic and English: ‘Brothers rise up! Claim your victory! Let’s go! Let’s go for jihad!’ It takes a while to register that the song itself is in German.

### 4.14 Propaganda Videos—Content Analysis

---

91 British journalist hostage of ISIS.
In this section, I highlight the most popular HD propaganda videos produced by ISIS’ media outlets between 2014 and 2015. I aim to explain how video production logistical tools were harnessed to produce powerful and sophisticated videos. In this section, I explain how ISIS created a paradigm shift in terror communication, by enlisting new digital and physical logistics that impacted the world. These logistical tools include cameras, post-production techniques, editing software, graphics, cast and sound effects. As Steve Rose (2014) observed: These films were simply made, they are most likely shot on standard equipment, such as Canon’s 5D or 7D—easy to operate and to keep in focus. They use radio microphones for sound. Effects and graphics and image-manipulation generated by tools like Adobe Premier; even phone apps can do a super slo-mo [slow motion] effect.

Arguably, the most important videos circulated by both online media and mainstream media were *Message to America* (see Figure 62), *Flames of War* (see Figure 63) and *Healing of the Believers’ Chests* (see Figure 64).

4.14.1 *Message to America*

![Figure 62. Screenshot from Message to America propaganda video.](image-url)
The structure of the video is simple. It opens with former US president Barack Obama speaking of air strike operations in Iraq against ISIS, to protect the US’s interests and save Iraqi innocent people. The second shot shows James Foley encouraging his family, friends and loved ones to revolt against the US government, which he calls ‘his real killers’. The third shot shows Jihad John, who stated:

This is James Wright Foley, an American citizen of your country, as a government, you have been at the forefront of the aggression towards the Islamic State [ISIS]. You have plotted against us and have gone far out of your way to find reasons to interfere in our affairs. Today, your military air force is attacking us daily in Iraq, your strikes have caused casualties among Muslims.

The fourth shot shows the beheading of Foley and the video finished by showing another American hostage, Steven Sotloff, present another direct message to Obama: “the life of this American citizen depends on your next decision”.

This was the first video produced by ISIS. The 4.40-minute video shows sophisticated use of high-quality cameras, multiple angle screenshots, professional montage and use of sound devices. Overall, for the first time, a terror group used a good-looking cast for both the victim and the terrorist, which indicates the intentionality in production and ISIS’ ability to harness powerful tools and take the world by surprise.
On 19 September 2014, ISIS released a 55-minute documentary-style film, produced by Al-Hayat Media Centre. It was titled *Flames of War*. The trailer for the video, which was originally posted to the internet archiving site archive.org on 16 September, featured footage of former US president Barack Obama saying, “combat troops will not be returning to fight in Iraq”. The film cut to its title card which said, “Flames of War: Fighting has just begun”. The film is professionally edited and highlights the ISIS’ seizure of the Syrian Army’s 17th Division base near Raqqa. The film opens with a narrator authoritatively declaring that the establishment of the Islamic caliphate has allowed the Muslim community to “unite under one call, one banner, one leader”. Svirsky (2014) observed:

> The film utilizes romantic imagery carefully crafted to appeal to dissatisfied and alienated young men, replete with explosions, tanks and self-described mujahedeen winning battles. Anti-American rhetoric provides the voice-over to stop motion and slow-motion action sequences. The use of special effects such as bullet-time is interspersed with newsreel footage.

According to Svirsky (2014), “This up-to-date, sophisticated cinematography combined with the bloodthirsty message makes the film *Flames of War* reminiscent of Hitler propagandist
Leni Riefenstahl’s 1935 film, *Triumph of the Will*. The film finishes with a written statement from Caliph Abu Bakr Al-Baghdadi, who refers to the US as the “defender of the Cross”. The message appears to indicate that the group believes US combat forces will be sent to Iraq.

Kiefer (2014) presented an analysis of *Flames of War*:

The film shows long slow-motion shots of black-clad young men with beards and shoulder-length hair who effortlessly withstand the shock waves of heavy mortar rounds. Given these images, it is little wonder that IS [ISIS] fighters are celebrated as ‘lions’ and ‘heroes’ in the social networks of the neo-Salafists.

A final message is read aloud and flashed on the screen. At one point, it reads: “A proxy war won’t help you in Sham just as it didn’t help you in Iraq. As for the near future, you will be forced into a direct confrontation”. The film concludes with a message: “the sons of Islam have prepared themselves for this day, so wait and see, for we too are also going to wait and see.”

### 4.14.3 Healing of the Believers’ Chests

*Figure 64. Screenshot from Healing the Believer’s Chests propaganda production.*
ISIS released a 22-minute video on 2 March 2015, titled *Healing the Believers’ Chests*. This film showed captured Jordanian air force pilot, Moath Kaseasbeh, being burned alive in a cage. This video is considered one of the most gruesome videos produced by ISIS, which has incited global outrage, including some extremist Muslims who denounced the method of killing. In this video, ISIS producers—for the first time—used different production tactics, including cast, graphics, cameras, post-production, Photoshop software, computer-generated images (CGI) and sound effects. The 22-minute video is sophisticated, to the extent that the excessive use of CGI makes some film analysts believe the video is fake. The films open with Al-Kasasbeh speaking directly to a camera, condemning his government for taking action against ISIS. During the interrogation, a professional use of infographic data is displayed adjacent to sophisticated and eye-catching scenes. Although the message is negative, professional producers use of multiple camera angles and a well-presented cast made the film akin to a Hollywood production. The burning scenes, which were about 2.30 minutes in length, were the most watched and circulated on SMNs and mainstream media. Slow-motion effects, sound effects and graphics give global range and power to its rhetorical appeals to its target audiences. Overall, this sophisticated media production was successful in delivering its compelling message to a worldwide audience.

### 4.15 Going Viral—Disseminating the Message of Terror

In this section, I explain the information loop of ISIS networks. Raber’s (2003) information paradigm is used to understand the mechanism processes of transmission, storage and retrieval in physical and material informational objects. Examination of these mechanisms may lead to understanding the viral nature of terror messages. In their book, *Going Viral*, Nahon and Hemsley (2013) defined a viral moment as:
A social information flow process where many people simultaneously forward a specific information item, over a short period of time, within their social networks, and where the message spreads beyond their own [social] networks to different, often distant networks, resulting in a sharp acceleration in the number of people who are exposed to the message. (p. 16)

The authors pointed out the parallels between viral events and the gatekeeper's network in Twitter, which they called “Occupying Twitter: a retweet network’ (Nohan & Hermsley, 2013). Nohan and Hermsley (2013) noted that ‘viral events are not new. What is new is that a viral video, a news story, or a photo can reach 40,000 people in hours, even minutes, instead of days” (p. 2). Further, Nohan and Hermsley (2013) outlined the connections between the emergence of the new information ecosystem—assembled by information flows on SMNs—and viral videos. They contended that virality can both reproduce and transform existing social norms and institutions.

As such, the question arises: how and why have ISIS’ propaganda videos gone viral mere seconds after their release? This question can be answered by what Nohan and Hemsley (2013) have argued are gatekeeping networks within digital spheres (such as Twitter, Facebook and Google) or physical spheres that are controlled by mainstream media networks (such as Fox News, CNN and Al Jazeera). In case of the ISIS messages, both gatekeeping networks—within digital and physical spheres—have collaborated to disseminate messages of terror.

It also must be addressed that anti-ISIS powers, who have worked hard to counter ISIS’ message, have ironically served ISIS’ rationale, as the terror narrative dominated and controlled flows of information. Pippa (as cited in Freedman & Thussu, 2012) argued:
The role of SMN’s as a tool of terror communication has added another larger complexity in media coverage of terror events as terror organisations provided their point of view and challenged the ‘one-sided messages’ of fear to opponents. In his own words ‘the mass media frame in any society is only one factor affecting public opinion, which is also affected by real world indicators and by personal experience and interpersonal communication’. (p. 13)

To understand the collaboration between networks of adversaries, a study of the norms of network relations, network structures, information logistics infrastructures and hybrid online interaction (particularly on Twitter) is essential. To understand the oxymoronic relationship, it is necessary to study the producers of messages and ascertain whether individuals, media outlets or affiliate networks influence the message. Further, it is essential to understand whether the message is centralised or decentralised, how it has been established and maintained, what tools have been used and who the mediators are. Social network analysis is providing answers to these questions. Therefore, ISIS strategically maintains a strong presence on SMNs—particularly Twitter—to control information flows. Mapping of ISIS’ online activity may lead to clear understanding of the overlapping elements of their information logistics infrastructure.

From a virtual networking perspective, “the going viral moment” in relation to ISIS’ propaganda videos happens in a three-step process. First, ISIS’ Twitter accounts followers—including myself—observe that ISIS’ network affiliates start tweeting about important productions that are to be released soon. Second, these tweets are instantly retweeted by many ISIS affiliates, which ensures the hashtags and topics trend on Twitter until the moment the video is released via JustPaste.it, sendvid.com or other Arabic anonymous platforms, such
as Manbar.me and Nasher.me. These retweets reach hundreds of thousands of people and many thousands of other media outlets that disseminate the uncut content of these videos. Finally, the disseminated videos can be downloaded and archived on anonymous virtual clouds like dump.to (e.g., www.dump.to/Esdarat and www.dump.to/Ismedia) to keep a digital legacy of their production. These videos can be stored on archive.org, Google Drive or many other websites affiliated with ISIS. For instance, I have observed that ISIS-affiliated Twitter accounts had been holding discussions among its supporters, in which they asked for ways to “kill the captured Jordanian pilot”. An Arabic Twitter hashtag started by ISIS, ‘Suggest a way to kill the Jordanian pilot pig’ (اقترح طريقة لقتل الطيار الأردني الخنزير#), has been widely shared among its followers. The hashtag had been shared over 1,000 times among ISIS’ supporters, who suggested several brutal ways to kill the pilot. Some of the ideas included beheading or burning Al-Kasabeh alive.

Another important factor of ISIS’ ‘going viral’ moment is what I call the collaboration networks of adversaries. News-thirsty media networks and other online media networks that have millions of viewers unwittingly disseminated ISIS’ messages of terror. For example, the first video released by ISIS, Message to America, was first captured and disseminated by the think tank called SITE. The US Department of State has its Twitter site ‘Think Again Turn Away’ (which was established in 2014, to counter ISIS’ messages) links to ISIS-related news stories and occasionally releases its own videos. The site delivers the same propaganda contents that ISIS’ affiliate networks deliver. Further, Fox News defended its choice to broadcast the full-length video, Healing of the Believers’ Chests, and list a hyperlink to it on its online page. As Awan (2014) argued:
The media and terrorists are in what we might call a symbiotic relationship. Terrorists naturally benefit from media that inspires fear in a much larger target audience; they use it to turn a local event that affects a limited number of immediate victims into a global issue. And, unsavoury as it sounds, the media benefits from terrorist outrages too, most obviously by selling papers and winning audiences.

Engel (2014) argued that one of the main reasons that ISIS flourished and consolidated its power was because of Western media. The relationship between terrorist media and mainstream media is oxymoronic; while mainstream media employed its capabilities to counter ISIS’ messages, it also promoted its propaganda, which facilitated the success of ISIS’ many video productions because they were given a worldwide audience.

As Rose (2014) noted, “Amateur videos and images are also being uploaded daily by its foot soldiers, which are then globally disseminated, both by ordinary users and mainstream news organisations hungry for images of a conflict their own cameras cannot access”. The ultimate success of ISIS’ networks—including their employment of new information logistics infrastructure and the maintenance of their information flows—is evidenced in the fact that their produced content is wanted. As Sandkuhl (2007) observed:

The main objective of Information Logistics is optimized information provision and information flow. This is based on demands with respect to the content, the time of delivery, the location, the presentation and the quality of information. The scope can be a single person, a target group, a machine/facility or any kind of networked organisation. (p. 46)
Within this context, ISIS’ video productions focused on the presentation of content. The versatile quality content of propaganda videos forced news-mainstream media to disseminate ISIS’ messages, instead of countering them. Anti-ISIS powers have agreed on waging information warfare to counter ISIS’ online messages. However, ISIS survives in this competitive environment, wherein information dissemination is crucial for the maintenance of network structure. This is because connectivity and flows of information are the backbone of networks. Although the content and production quality of ISIS’ videos are similar, their productions are appealing to mainstream media networks because of their varied ways of killing of their victims. From the beheadings in *Flames of War* to the burning alive in *Healing of the Believers’ Chests*, ISIS uses varied methods to kill their victims (e.g., drowning in cages and executions of spies and militias). As such ISIS maintains its flows of information and network relationships through a simple supply and demand marketing strategy. Sandkuhl (2007) argued:

If information logistics is regarded as the planning of information flows, this consequently implies the planning of an information-logistical infrastructure. In doing so, two essential areas need to be distinguished. Whereas on the one hand network relations and/or supplier-requestors relations need to be defined and structured, on the other hand the resulting information-logistical basic infrastructure must be designed and optimized. (p. 46)

ISIS’ media propagators achieved their core objectives by optimising content online by borrowing from Western movies, reality shows and hip-hop culture. The symbiotic relationship between the media and terror is evident in the media’s coverage of terrorism, which incites more terrorism, which in turn produces more media coverage.

4.16 Conclusion
In this chapter, I explored the digital media logistics of ISIS’ networks with a focus on Twitter as the prime medium of communication used by ISIS and its international affiliates. Examining the IO of digital media is the first step to understanding how terror networks promote their terror narrative and how these messages are distributed so quickly. This chapter examined the information logistics of ISIS’ networks from two perspectives: information as a paradigm and ANT. Both perspectives explained how ISIS leveraged its network and established decentralised distribution networks by enlisting more actors. This served to sustain the network through ISIS’ affiliate engagement. By exploring the information logistics of ISIS, researchers can understand how terror networks manoeuvre in information environments for the purpose of strengthening its message and loop of information.
5 Chapter 5: Degrading Operation—Attacking the Digital Logistics of ISIS’ Networks

5.1 Introduction

As explained in Chapter 4, ISIS runs complex media logistics operations, which are dependent on broad digital media networks that enable them to establish decentralised distribution networks. These networks exploit the functionality of social media platforms, encrypted digital communication applications and anonymous sharing portals. That is, the mobilisation of many heterogeneous elements has enabled ISIS to leverage their networks and created complex associations between the information environments and human actors. These associations will explain how ISIS built decentralised communication networks and became an agent of stigmergic operations.

The decentralised structure of ISIS’ networks has enabled a new phase of information warfare dependent on decentralised C2 operations. Therefore, approaches to disrupt ISIS flows of information are less successful, as ISIS has weaponised multiple digital media environments. Moreover, the resilience and fluidity of ISIS’ distributed networks leads to the pervasiveness of their terror narrative, which has accelerated their processes of recruitment and radicalisation. To hinder ISIS’ flows of information and disrupt its digital media activities, an international collaboration has been required between collective hacker groups (e.g., Anonymous and CTRLsec), government agencies (e.g., Sawab Centre and United States Department of State’s [USDOS] team), security agencies (e.g., CSCC) and social media platform administrators (e.g., Twitter and YouTube). Swarmcast operations, carried out by these agencies, managed to disrupt ISIS’ flows of information to some extent, by suspending its accounts on Twitter, Facebook and YouTube. Further, a new wave of
swarming operations targeted ISIS’ digital media logistics and aimed to degrade its activities on anonymous sharing portals and encrypted communication channels.

In this chapter, I outline the degrading operation conducted on ISIS’ digital media logistics. The operation was carried out by the US government and collective hacker groups, such as Anonymous and individual hackers (i.e., catallaxies⁹²), who targeted both message logistics and content.

This chapter aims to answer the thesis’s secondary question: how has the suspension of Twitter and YouTube accounts impacted on ISIS’ networking performance? To answer this question, I identify the phases of the degrading operation: degrading and destroying; countering ISIS’ propaganda; and hacking and information warfare. Second, I examine the role of hacktivists from both sides (such as ISIS’ Cyber United Caliphate⁹³) and how ISIS protected its digital legacy. Third, I analyse the effect of network governance on ISIS’ network performance.

In Section 5.5, I discuss to what extent should TOS be applied in the context of terror organisation, and how effective TOS can be in tracing and suspending ISIS’ digital activity on the network. Finally, this chapter includes an overall assessment of the information warfare that occurred between ISIS and its adversaries in the information environment.

---

⁹² The term catallaxy “describes the process by which order emerges from the seeming chaos of countless individual interactions between participants in a complex system. This spontaneous human coordination is the result of the individual action of the system’s participants, but the resulting order is not shaped consciously by human design” (Pouliot, 2017).

⁹³ Pro-ISIS collective hacker group.
5.2 Attack ISIS’ Digital Logistics

The pervasiveness, influence and reach of ISIS’ messages have helped the group to establish networks of affiliates, sympathisers and members outside its controlled territories. The influx of mujahedin from Arab and foreign countries, who migrated to the Islamic caliphate, has significantly improved ISIS’ networking performance. This is reflected by the number of triumphs, territories subdued, and military operations conducted outside their territories. Additionally, during the 2012–2013 Anbar uprisings, there were no more than 2,000 ISIS fighters. However, by 2014, there were over 30,000 mujahedin operating inside Syria and Iraq, with an unknown number of sympathisers and affiliates operating outside its territory. Further, the number of digital jihadists (e.g., Slacktivists and catallaxies) who stigmergically contributed to aggregate, generate and spread content in the name of the Islamic caliphate is unknown. Collective digital jihadi (or e-jihadists) swarmed popular social media platforms—especially Twitter—with propaganda to infuriate the US government, who launched the Global War on Terrorism, and combat them in the information environments. Recently, the Chairman of the Joint Chiefs of Staff connected the “information’ aspect of conflict with the other major elements of power. He argued that the defeat of ISIS ‘requires the application of all the tools of national power, diplomatic, economic, information, military” (Waller, 2015, p. 29).

The use of modern technologies by terror organisations has caused controversy among policymakers in the US, as they seek strategies for dealing with the issue. For instance, during the rise of Al-Qaeda in the 1990s, the fax machine played a role in the spread of Al-Qaeda’s propaganda (akin to ISIS’ use of Twitter today). Osama bin Laden used fax machines to send messages to his affiliates in the UK and US (Hughes, 1998)94. In one of the

---

94 Some researchers read the fax machine radicalisation article as satire (not factual).
messages sent by bin Laden (as cited in Hughes, 1998) through a fax machine, bin Laden stated that “the ruling to kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it”.

At that time, the real-time messaging tools opened a new paradigm of terror communication. The use of fax machine created panic among security agencies, due to fear that such messages would increase and accelerate the process of radicalisation and recruitment. There was an urgent need to devise a way to counter the new threat. Three countermeasure practices were implemented to tackle the fax machine radicalisation and dissemination of Al-Qaeda’s messages. These countermeasures included: fax machine versus fax machine; humans versus fax machine; and attacking the logistics of fax machines.

The first countermeasure, fax machine versus fax machine, was labelled by the DOD as Project Bain.95 The US government allocated US$10,000,000 to buy two million fax machines to counter Al-Qaeda’s messages. According to a senior Pentagon official (as cited in Hughes, 1998), Project Bain was “simple. Terrorists have fax machines and we should too. We can’t cede the ideological battlefield on data transmission”. Further, according to the official (as cited in Hughes, 1998), this project had a straightforward mission: “every time Bin Laden releases a declaration of war on one fax machine, there’s got to be another Fax machine right next to the bad one that transmits our positive message”. However, the use of fax machines to counter Al-Qaeda’s fax machines was a controversial move among government officials. One senior government official (as cited in Hughes, 1998) said, “We

95 Named “after the Scottish inventor of the first fax machine, Alexander Bain” (Hughes, 1998).
shouldn’t be providing counter-faxes. We need to empower other voices to counter-fax themselves”.

Countering fax machine communication with more fax machines created confusion among security agencies and community activists, because no specific fax numbers were provided with which to focus their efforts. Therefore, a community-based organisation was nominated to debate the value of the fax machine countermeasure. This was known as a Countering Violent Extremism program. Within the debate concerning countering radicalisation via fax machine, Senator John Smith of Maine and Congressman William Mahanty (as cited in Hughes, 1998) suggested that attacking fax machines logistics would solve the problem, such as blocking the phone numbers linked to faxes received from Afghanistan and ceasing fax machine ink suppliers’ access to Afghanistan. Mahanty (as cited in Hughes, 1998) argued that if the US government “stop[s] the ink, [they] stop the problem”.

Countering Al-Qaeda’s fax machine radicalisation practices are similar to the countermeasures undertaken by policymakers in dealing with ISIS’ use of sophisticated digital media techniques for radicalisation, mobilisation, recruitment, and the generation and dissemination of content. The significant amount of media content produced by ISIS—which is only increasing—has required many operations to be conducted by a range of established powers in order for the countermeasures against ISIS’ logistics to be effective. Further, Milton (2016) noted that ISIS:

has not just created a media organisation but a media network that relies on a geographically diverse group of individuals around the world to push out its messages. Defeating it is not the job of any one organisation or country, and it will likely require a multilateral effort. (p. 49)
I observed that efforts to deploy countermeasures against ISIS’ online offensive—conducted by the US and other adversaries of ISIS—have emerged in three distinct phases. Phase one has been concerned with degrading and destroying; phase two has focused on countering ISIS’ propaganda; and phase three has taken the form of hacking and information warfare.

5.3 Phase One—Degrading and Destroying

The notion of degrading and destroying ISIS’ networks on social media platforms emerged in response to ISIS’ images of the beheading of US photojournalist, James Foley. These were uploaded to Twitter and distributed through ISIS’ networks. According to Joseph Cox (2014), “The hashtag #ISISMediaBlackout quickly gained traction, with users protesting that sharing such graphic images of Foley was, in essence, spreading the terrorist group’s propaganda for them” (see Figure 65). As ISIS’ propaganda on Twitter gained momentum, policymakers and platform administrators were compelled to take action.

![Figure 65. A tweet by Hend Amry, showcasing the first use of #ISISMediaBlackout hashtag.](image)

This action was affirmed by then president Barack Obama during his speech at the General Assembly of the United Nations on 25 September 2014. Obama (as cited in McCarthy, 2015) stated that “the US will work with a broad coalition to dismantle this network of death”.
Obama presented strategic objectives for this mission, including cutting ISIS’ cash flows, paralysing the movements of foreign fighters and rooting out jihadi networks from online spaces (McCarthy, 2015).

To understand the US’s strategy in degrading and destroying the digital media logistics of ISIS’ networks, it is important to define the extent of the operation. ‘Degrading’ means:

> to lower the character or quality of an adversary C2 or communications systems, and information collection efforts or means; or to degrade the morale of a unit, reduce the target’s worth or value, or reduce the quality of adversary decisions and actions.

(Nissen, 2015, p. 67)

While ‘destroy’ refers to “put[ting] an end to the existence of (something) by damaging or attacking it (e.g., to damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt)” (Nissen, 2015, p. 67). In this chapter, I focused on the impact of degrading and destroying the digital capabilities of ISIS’ operation in regard to ISIS’ information flows, dynamics of dissemination, C2 operations, number of produced messages, recruits and on-ground operations. That is, from ANT context, the degrading operation aims at cutting off the logistical support of ISIS networks through thwart of enrolment processes of digital actors that sustain ISIS’ information flows and communication networks.

Overall, the aim of this chapter is to highlight the strategy of the US and social media administrators in destroying and disrupting the information flows of ISIS’ networks on information environments. This phase was twofold. First, it required the direct involvement of the US in tracing the digital activity of ISIS and destroying it. Second, the US applied
pressure to the administrators of social media platforms to control ISIS’ use of their platforms. In Sections 5.3.1 and 5.3.2, I examine the processes of the degrading operation at tactical level (i.e., the Whack-a-Mole operation and the Interaction and Isolation operation).

### 5.3.1 The Whack-a-Mole Operation

Operation Whack-a-Mole is counterinsurgency war strategy initiated by the US in the 1990s, after the rise of Al-Qaeda. The name of the operation is based on the arcade game of the same name (see Figure 66). This strategy was described by the former president, Barack Obama (as cited in Faux, 2014), who told CBS News on 22 June 2014, “What we can’t do is think that we’re just going to play whack-a-mole and send U.S. troops occupying various countries wherever these organisations pop up”.

![Figure 66](image.png)

*Figure 66. Cartoon depicting the Whack-a-Mole operation.*

“Whack-a-mole’ is defined by the Oxford Dictionary as “an arcade game in which players use a mallet to hit toy moles, which appear at random, back into their holes”.

---

96 ‘Whack A-Mole’ is a metaphor used by the critics to describe the US strategy against terrorism for lacking strategic clarity and being unable to reach its strategic objectives.
Within the context of the US’s Whack-a-Mole strategy against ISIS’ digital activity on Twitter, the question emerged: who was mastering the game? There was a concern that the US was being outmanoeuvred, despite its aim to outmanoeuvre ISIS. According to ISIS member Abul Muthanna (see Figure 67), trying to stop ISIS on Twitter is like whack-a-mole, because ISIS will keep coming back.

![Abul Muthanna’s reply to the United States Whack-a-Mole operation.](image)

**Figure 67. Abul Muthanna’s reply to the United States Whack-a-Mole operation.**

In reacting to the Whack-a-Mole strategy, waged by the US and other anti-ISIS powers, ISIS maintained that for every account suspended, another account should be established. For ISIS, Twitter is the digital domain wherein it enacts its IO and maintains its flows of information. If ISIS lost Twitter, they would lose a significant asset in the media war. Thus, the resurgence of ISIS’ Twitter accounts was essential to maintain their flows of information. Fisher (2015) observed that “this dispersed structure, which functions as a swarm on Twitter, has continued to develop with multiple backup accounts allowing users to maintain contact after a specific account is suspended” (p. 9). The speed of re-emerging in Twitter after an account suspension is central to ISIS’ IO strategy. Fisher (2015) noted that “resilience against takedowns and account suspensions has become an important element of the Jihadist Swarm-cast” (p. 8).
Examining the success of the mission to degrade ISIS’ digital capability operation is a
difficult task. Further, it may be too soon to determine whether ISIS’ networks are prolific or
scarce. However, in their report, *The ISIS Twitter Census*, Berger and Morgan (2015, p. 9)
claimed that the mass account suspension strategy—known as Whack-a-Mole—was a highly
successful network degrading too. They claim that ISIS found it challenging to deal with the
suspended accounts without suffering any negative consequences. It was estimated that there
were between 46,000 and 90,000 pro-ISIS Twitter accounts active in the period from
September to December 2014 (Berger and Morgan, 2015). Twitter claimed it suspended over
300,000 active Twitter accounts in the period between 2014 and 2016.

The effect of account suspensions on ISIS’ activity on Twitter has diminished significantly.
However, this does not necessarily mean that ISIS lost the battle in the Twitter sphere, that
their account suspension equated with the paralysation of their flows of information, or that
their C2 operations were thwarted. To understand the impact of the degrading mission on
ISIS’ networks, it is important to understand the dissemination dynamics and tactics used by
ISIS members and sympathisers to maintain their information flows on Twitter.

5.3.2 Interaction and Isolation

As part of their degrading strategy, the US used Interaction and Isolation processes to
reduce ISIS’ activities on Facebook, YouTube and anonymous sharing portals. Interaction
with ISIS’ digital content requires an understanding of the dynamics and mechanisms of
SMNs, the nature of engagement with disseminated content, the tools for searching and
monitoring terror entities, the strategies for identifying disseminated content and the profile
of potential people who could engage with disseminated content. According to Nissen (2015),
interaction with digital content “provides possibilities for mapping who the disseminators,
influencers or key opinion-makers are and how they drive the conversation around topics of interest, and people’s conversations and actions online that can be mined for insights and understanding” (p. 64). The Interaction and Isolation operation was launched before SMNs established policies and approaches to combat ISIS’ exploitation of their networks. In this operation, the US CSCC physically identified ISIS’ accounts on social media platforms, websites, mobile phone applications to reported them to network administrators or launched cyber attacked them using DoS.

For the ‘Interaction and Isolation’ strategy to be successful, a significant amount of resources and effective collaborations between security agencies and other ISIS adversaries were required. This process required the mobilisation of collective individuals, hackers and government agencies to identify, map and analyse the strategic tactics of ISIS’ information flows. The US government established a counternarrative strategy while collaborating with social media platform administrators (which is discussed in Section 5.7). This operation represented a significant amount of work: identify and map ISIS’ content, engage with their narrative, and identify potential content generators and disseminators. This workload became the responsibility of social media administrators, individual hackers and other international security agencies (see Section 5.4). This approach will be analysed from an information manoeuvre warfare perspective (see Section 7.4).

5.4 Collective Collaboration—Social Media Platforms Approach to ISIS’ Content

To combat the surge of ISIS on their SMNs, the US government requested Twitter and Google to delete ISIS’ active accounts on their platforms. This measure resulted in the deletion or suspension of thousands of accounts and messages. In effect, this measure led to a global cyberwar against ISIS’ affiliates. Moreover, in December 2016, Twitter, Facebook,
Microsoft and YouTube collaborated to develop innovative tools to identify terrorist imagery and videos. Their statement declared:

> We commit to the creation of a shared industry database of ‘hashes’—unique digital ‘fingerprints’—for violent imagery or terrorist recruitment videos or images that we have removed from our services … By sharing this information with each other, we may use the shared hashes to help identify potential terrorist content on our respective hosted consumer platforms. (Facebook, 2016)

However, this important agenda was already reflected in the ISIS’ distribution strategies (Lakomy, 2017, p. 48). Administrators of social media platforms have established alert systems to warn each other when ISIS uses platforms. This process was described by Fisherman (as cited in Kranish, 2017) as a “dynamic loop of information sharing known in the industry as Hash database. Social media companies use of “hashes” or “digital fingerprints” … alert other platforms of troublesome users or content”.

To understand the extent of ISIS’ exploitation of Twitter, I revisit the most important work in relation to the degrading operation, *The ISIS Twitter Census*. In this study, Berger and Morgan (2015) collected Twitter data to map ISIS’ activities on that platform. The study was based on a sample of 20,000 of ISIS’ supporter accounts. The study established that between October and November 2014 “at least 46,000 Twitter accounts were used by ISIS supporters”. The study also revealed that 20,000 confirmed ISIS supporters are residing in the territories controlled by ISIS. Saudi Arabia was the second most common location for ISIS’ supporters. In addition, one-fifth of ISIS’ supporters used English and almost three-quarters selected Arabic as their primary language. The study also revealed that the broad
countermeasures aimed at degrading ISIS’ propaganda were successful, partially because of wide Twitter account suspensions (Berger & Morgan, 2015).

Twitter has applied a strong strategy to remove ISIS accounts. This strategy is divided into three processes. First, Twitter identify ISIS content and accounts by using the Interaction and Isolation strategy. Second, Twitter relied on the reports from ISIS’ adversaries and hackers (see Section 5.8), who contacted Twitter using #targets and #OpISIS. A short loop (i.e., the decide and act aspects of the OODA perspective) of dynamic processes between Twitter staff and anti-ISIS collectives has accelerated suspensions. According to Milton (2016), this strategy “relies not only on [the] reporting of suspicious accounts from users and government officials, but also on the proactive efforts of Twitter employees and technology to identify and remove offensive content” (p. 41).

Third, Twitter identified potential ISIS accounts and affiliates through machine learning or AI. In this process, Twitter algorithms mapped the social networks of ISIS members to identify networks of followers and affiliates. AI has therefore maximised the number of suspended accounts. Gladstone (2015) reported, “Twitter says it suspended 10,000 ISIS-linked accounts in one day”. In the period between June 2015 and February 2016, Twitter claimed to suspend 125,000 jihadi accounts; between January 2016 and August 2016, Twitter claimed to suspect 235,000 accounts (as cited in Lakomy, 2017, p. 47).

Facebook’s priority was to ensure that terror-related content was removed before its provoked attackers to act (Kranish, 2017). To map, trace and remove ISIS’ digital activity on its platform, Facebook employed a network of 150 employees and utilised AI technologies. Regarding the processes involved in removing ISIS’ terror-related content on Facebook,
Fisherman explained that “before posts gets to [Facebook’s team], they’re filtered through Facebook’s computers, which have been programmed to scan content for buzzwords associated with terrorism. Only then are the posts passed onto the team”. This strategy was described by Fisherman (as cited in Kranish, 2017) as “using humans to do what humans do best, and computers for what computers do best.”

Frenett (2016) and his MoonShot group, after working with Google’s Jigsaw recently, reported their findings of a study on Facebook’s intervention with ISIS followers. Their findings led them to conclude that those who wish to fight against terror groups can reach the same digital audiences that terrorists do to intervene in various ways, including to pitch them counter narrative materials. However, the determination regarding which counter narrative materials will work in particular situations has not been identified (Frenett, as cited in McDowell-Smith et al., 2017, p. 54). The question remains: to what extent do social media platforms apply their TOS to remove terror content and suspend associated accounts?

5.5 Terms of Service Violations

Popular social media platforms, such as Twitter, Facebook and YouTube, are using their TOS to exercise control over the type of information produced and disseminated over their networks. For example, YouTube’s TOS states in relation to hateful, violent and graphic content that “it’s not okay to post violent or gory content that’s primarily intended to be shocking, sensational or disrespectful. If a video is particularly graphic or disturbing, it should be balanced with additional context and information”. Silverman (2014) observed that YouTube acts robustly when dealing with terror content. YouTube can quickly delete

content and suspend associated accounts. Under YouTube’s TOS, the platform reserves the right to remove content and, in some instances, suspend accounts. According to a YouTube spokesperson:

YouTube has clear policies prohibiting content intended to incite violence, and we remove videos violating these policies when flagged by our users. We also terminate any account registered by a member of a designated Foreign Terrorist Organisation and used in an official capacity to further its interests.

Berger and Strathearn (2013, p. 14) indicated that when it comes to freedom of speech, social media platforms are biased. They suggest that these platforms should make it clear that freedom of speech is limited when it comes to using their service.

Similarly, Twitter applies its TOS policies to content that breeches their terms. With rising international pressure on these social network platforms, particularly from the US government over ISIS’ online materials, Twitter, Facebook and YouTube have acted swiftly and imposed harsh policies by targeting gruesome content generated by ISIS.

The global coalition against ISIS should work in close cooperation with corporations and media owners to counter and eliminate the terrorist communication network, which is highly efficient and resistant to account suspensions or deletions. Removing individual accounts is not enough, because that will not disturb the flow of information within ISIS’ holistic information strategy. For effective action, a community-based approach is needed to disrupt the networking ISIS does through various social media platforms. All organisations using social media are responsible for maintaining their sites; this includes monitoring and blocking networks that can be used for terrorist attacks (StratCom, 2015, p. 48).
5.6 Phase Two—Countering ISIS’ Narrative

The principle objective that underpins the degrading of ISIS’ digital logistics is to minimise ISIS’ visibility and influence in information environments. Knowing that ISIS’ IO is based on the strategic narrative inherited from its predecessor (Al-Qaeda), anti-ISIS collectives fought ISIS in the information environments to paralyse ISIS’ tools of dissemination, attack its C2 operations and disrupt its flows of information. However, the US realised that attacking ISIS’ digital media logistics alone was ineffective in reducing the number of recruits and the influence of jihadi around the world. Thus, to counter ISIS’ narrative, the US and other ISIS adversaries established a narrative versus narrative strategy. Casebeer and Russell (2005) suggested that the most effective way to counter terrorism is by developing a ‘better story’ to replace the extremists [sic]’ one.

Braddock and Horgan (2015) outlined that an effective counter narrative must address the four criteria; the counter narrative must be effective in “revealing incongruities and contradictions in the terrorist narratives and how terrorists act, disrupting analogies between the target narrative and real-world events, disrupting binary themes of the group’s ideology, and advocating an alternative view of the terrorist narrative’s target” (p. 397). Through their study, they were able to conclude that narratives can significantly impact the “beliefs, attitudes, intentions, and behaviours” of their audiences (Braddock & Dillard, 2016, p. 18). This study identifies the need to address ISIS’ narratives through counternarratives (as cited in McDowell-Smith et al., 2017, p. 58).
When ISIS seized control of Mosul and declared the Caliphate in June 2014, the US CSCC\textsuperscript{98} intensified its operational measures by working on strategies to counter ISIS’ narrative (Fernandez, 2015, p. 15). The CSCC had followed three main strategies in countering ISIS’ narratives. First, they established a video versus video strategy (akin to fax machine versus fax machine, see Section 5.2). Second, the CSCC traced digital activity on social media platforms and notified administrators (as part of the Interaction and Isolation strategy discussed in Section 5.3.2). Third, the CSCC worked intensively to educate Muslim youth living in the West about the menace depicted in ISIS’ propaganda based on a narrative versus narrative strategy.

For example, to compete with ISIS’ propaganda online, the CSCC debuted a video production, titled \textit{Welcome to ISIS Land}. According to Higham, “The video became a viral phenomenon—viewed more than 844,000 times on YouTube—and a cause of significant irritation to its target”. The narrowing of the CSCC’s focus to ISIS’ propaganda allowed for a boost in the CSCC’s overall production. In 2014, the CSCC released at least 93 Arabic videos. In the time between the fall of Mosul (10 June 2014) and the end of the year (specifically, 5 December 2014), the CSCC’s videos were viewed on YouTube 959,187 times, with additional views occurring on Vimeo and via bootleg versions posted on Iraqi and Syrian Facebook pages. Fernandez (2015) observed that “the single most successful Arabic video, “DAESH Threatens Sunnis,” was viewed 115,050 times in two postings since ISIS supporters briefly knocked it from YouTube by manipulating YouTube community

\textsuperscript{98} Established in 2011 to bring security agencies in one hub for coordinating efforts in countering Al-Qaeda’s communication activities.
standards” (p. 15). Like the work of the Saudis, the work of the CSCC has received considerable media attention; however, it has had limited impact (Fernandez, 2015, p. 15).

In addition, the CSCC launched the ‘Think Again Turn Away’\(^99\) page on Twitter to stop foreign fighters joining ISIS and document the atrocities committed by ISIS’ jihadi. Since the rise of ISIS, the CSCC “targeted counter-messaging against ISIS in Arabic and in English” (Fernandez, 2015, pp. 14–15). In return, ISIS launched the ‘Run Do Not Walk to U.S. Terrorist State’ page on Twitter to recruit potential members from the West.

Worried European countries have also joined in the countermeasure efforts to stop ISIS’ propaganda. For instance, the British Army are creating a special digital force called Facebook Warriors, who are skilled in PSYOP. Similarly, the French Ministry of the Interior have produced a new website to counter jihad, which is aimed at discouraging young people from joining ISIS by using graphic images and messages that state, “They say: sacrifice yourself with us, you will defend a just cause. In reality: you will discover hell on earth and die alone, away from home” (Liang, 2015, p. 11).

Satirical productions have also been popular on social media platforms. The video entitled *What It’s Really Like to Fight for the Islamic State*, which was published on YouTube by Vice News in April 2016, is an example of a satirical production. According to Lakomy (2017):

\(^{99}\) Now called the USDOS team, operating in both Arabic and English, it produces videos showing the brutality of ISIS and raising awareness among the Arab and Muslim youth.
This piece was recorded by the headcam of a fallen member of the IS [ISIS] and depicted an extraordinarily clumsy fighter called Abu Hajaar during a firefight. The film instantly went viral (above 7 million views by the end of 2016). (p. 47)

5.7 Counternarrative Actors

As stated earlier, security agencies and collective groups of ISIS’ adversaries established counter narrative strategies. In Sections 5.7.1–5.7.4, I outline the role of the counter narrative strategies carried out by security agencies other than the CSCC. These are Sawab Centre, USDOS team, #AllAboutISIS and UK against Daesh. As this thesis examines the online activities of ISIS’ counter narrative actors, it is important to examine their online activity, not just the physical activities inside the centres they established in UAE and the USA. It is beyond the scope of this thesis to do so. Those actors were chosen simply because they are the most important counter narrative actors. ANT suggests following the actors wherever they are. In my opinion, the later mentioned actors were the most important as they have the capacity to carry out a strategic counter narrative of ISIS’ online activities.

5.7.1 Sawab Centre

Sawab Centre is an Arabic-based centre, established by the United Arab Emirates (UAE) to raise awareness about the atrocities committed by ISIS, counter youth recruitment, combat ISIS’ online propaganda and promote positive alternatives to extremism. Sawab Centre operates on Twitter only and focused on building a narrative to counter ISIS’ recruitment narrative (see Figure 68). Their production includes short videos of youth who have survived

100 Is an Arabic phrase meaning correction or rehabilitation.
ISIS, and depictions of the miserable life under the Islamic caliphate and the subsequent refugee crisis.

Figure 68. Screenshot of Sawab Centre. Source: Twitter.

Under the motto ‘united against extremism’, Sawab Centre’s mission is to:

- Warn youth against ISIS’ youth recruitment (see Figure 69).
- Highlight ISIS’ bankrupt ideology online.
- Focuses on families to counter extremism (see figure 70).
The centre highlights the role of the internet in radicalising and recruiting children through the hashtag, #ISISStealsYourChildhood. The Sawab Centre also runs the #DeludedFollowers campaign to expose the lies and falsehoods promoted by ISIS’ recruiters; and address the
underlying complexes and issues of vulnerable youth, including loneliness, social isolation, bullying and boredom. As stated on the UAE government’s website:\textsuperscript{101}

Sawab’s messaging will humanize the victims of ISIS attacks through highlighting the stories of parents, siblings, children, and other loved ones killed by Daesh [ISIS]. The campaign will also offer inspirational and motivational messages directed to at-risk youth to help them resist the deceptions and false promises of Daesh agents.

5.7.2 United States Department of State’s Team

The USDOS team, also known as Global Engagement Centre, was initiated by the US’s Department of State to counter extremism messages. This centre was established to replace the CSCC. Its mission, as stated on USDOS’s website,\textsuperscript{102} is to “lead the coordination, integration, and synchronisation of government-wide communications activities directed at foreign audiences abroad to counter the messaging and diminish the influence of international terrorist organisations, such as ISIS”. The activity of the USDOS team is only available on Twitter and messages are presented in Arabic (see Figure 71). Its clear messaging strategy aims to decrease the allure of ISIS and prevent the recruitment of new extremists.

\textsuperscript{101} http://www.uaeinteract.com/docs/Sawab_Center_warns_against_Daesh_youth_recruitment/79241.htm.

\textsuperscript{102} https://www.state.gov/r/gec/.
According to the Department of State website, the work of the USDOS team is focused on four core areas:\(^{103}\):

- **Partnerships**—The aim is to build partnerships with NGOs, schools, governments, civil society groups and religious leaders. The USDOS team aims to build a strong global network of positive messages to counter violent extremism. The USDOS team is committed to supporting its partners with essential funding, technical assistance and capacity building.

- **Data analytics**—The USDOS team uses data analytics systems from both the public and private sectors to better understand radicalisation dynamics online, which guides and informs their messaging efforts and measures their effectiveness. In addition to data analytics systems, the USDOS team has drawn from polling operations, target audience studies and academic research.

- **Content**—The USDOS team is pursuing collaborative, thematic campaigns in coordination with a coalition of nations and global partners to counter ISIS. The

---

\(^{103}\) These core missions were copied and paraphrased from DOS team website www.state.gov/r/gec.
USDOS team also developed and procured unbranded content and make it available to their global network of partners.

- Interagency engagement—The USDOS team liaise daily with the interagency to coordinate day-to-day operations and campaign efforts among the many US national security agencies that operate in the information space. The USDOS team is staffed by detailers from several US agencies, allowing it to effectively coordinate, integrate and synchronise efforts across the interagency.

5.7.3 #TruthAboutISIS Hashtag

![Screenshot of #TruthAboutISIS hashtag Twitter account.](image)

While ISIS’ propaganda and its online messages focused on daily on-ground triumphs, #TruthAboutISIS presented messages to counter ISIS’ narrative. All news broadcasted on its website and on its Twitter feed exposed the failure of ISIS’ propaganda (see Figure 72).

---

104 https://www.truthaboutisis.com/
When this Twitter feed emerged, The Guardian reporter, Wright (2015), observed that #TruthAboutISIS “has for the past few months been turning fire on ISIS using the same sophisticated video and social media techniques used by the group itself”. Wright (2015) also noted that “the site has no email contact, phone number or address, and is registered anonymously using a proxy server based in Dayton, Ohio”. The man behind the #TruthAboutISIS was interviewed by Wright (2015) who declared that “he was deliberately trying to mimic ISIS’ use of slick video production and social media tactics to engage an audience who might be tempted to join the group”.

This demonstrates the success of the strategy of fighting narrative with narrative. Arguably, this countermeasure was so effective because the man behind #TruthAboutISIS had studied sophisticated production and analysed the thematic narrative of ISIS. As Casebeer and Russell (2005) argued, “In practice, effective counter-narrative strategy will require understanding the components and content of the story being told so we can predict how they will influence the action of a target audience”.

236
5.7.4 UK Against Daesh

Similarly, the same counter narrative policy was introduced by many security agencies. The UK government have initiated a counternarrative operation, aimed to expose the brutality of ISIS. The British Foreign Office created a Twitter account, ‘UK Against Daesh’ (see Figure 7), which was aimed to restrain ISIS’ recruitment and radicalisation efforts (see Figure 74). Initiated in 2014, it was composed of multilingual videos and social media messages (Lakomy, 2017, p. 48).

Figure 73. Screenshot of ‘UK Against Daesh’ Twitter account.

Figure 74. The type of messages used by ‘UK Against Daesh’, posted to Twitter.
5.8 Phase Three—Hacking and Information Warfare

In this chapter, I discussed the US’s strategies for countering the narrative and digital logistics of ISIS’ networks. Despite these approaches, ISIS remains active and its flows of information seem less interrupted. This is because ISIS has learned how to manoeuvre in the information environment and always finds an alternative route to maintain their networking structure.

In this section, I analyse the role of hacker activisms (i.e., ‘hacktivism’) and digital catallaxies as part of the information warfare against ISIS. This includes the role of Anonymous and CTRLSec as collectives, as well as other individual catallaxies, such as Nun believer, Daesh eliminator and Noon. However, before examining the role of hacktivism within the degrading operation, it is important to define its terminology, understand the nature of its existence and analyse the role of hacktivism in similar events in the Arab region.

Hacktivist was a term coined in 1996 by Omega, a member of a group of internet hackers who called themselves The Cult of the Dead Cow. Mills (2012) defined hacktivism as “the use of legal and/or illegal digital tools in pursuit of political ends”. Hacktivist groups, which are leaderless, aim to protect the free flow of information on the internet. Their mission was clearly stated on the Anonymous website, “We want transparency and we counter censorship … this is why we intend to utilise our resources to raise awareness, attack those against and support those who are helping lead our world to freedom and democracy” (Anon’s.org, 2013). According to Frediani (2013), “Anonymous is a galaxy of individuals who find themselves attracted by the same forces […] that are created and undone according to their interests or personal interactions” (p. 112). Anonymous themselves have specified that they
“are not hackers, or terrorists but ordinary citizens who decide to take the virtual streets to demonstrate” (Frediani, 2013, p. 386).

Jordan and Taylor (2004), in their book *Hacktivism and Cyberwars: Rebels With a Cause?* have documented the hackers activity and its effect on the 21st century’s movements. They suggested, “These hacktivists seek to radicalise hacking’s original obsessions with information freedom and access by creating tools that ensure cyberspace remains a place where information is freely and securely available” (Jordan & Taylor, 2004, p. 4). Examining hacktivism and its involvement in social movements is significant and important. Jordan and Taylor (2004) noted, “As a movement it deserves attention because it is situated where it is; drawing in powerful alternative visions of society, arming these visions with informational tools and injecting itself as a radical virus into twenty-first-century societies” (p. 165).

The digital roots of the Arab Spring uprisings attracted the attention of hacktivist groups. As such, they sought to support Arab civil society actors in the information warfare against their governments. The significance of hacktivists direct involvement in the events of the Arab Spring uprisings was twofold. First, hacktivism dismantled the barrier of information production and dissemination by creating more options. Second, hacktivism empowered social actors, by shifting the balance of power from governments to activists by enhancing the latter’s communication technology usage and by trying to paralyse governmental communication facilities (Shehabat, 2015, p. 73).

Digital hacktivists bring together technical experts, and increasingly, activists with the common aim of uniting in non-violent—but often illegal—action. As Jordan and Taylor noted, hacktivism is the emergence of popular political action—of the self-activity of groups
of people—in cyberspace. It is a combination of grassroots political protest, with computer hacking. Hacktivists operate within the fabric of cyberspace, assessing what is technologically possible in virtual lives; they reach out of cyberspace, utilising their virtual powers to shape offline life. Social movements and popular protests are integral parts of 21st century societies. Hacktivism is activism, influenced by the digital and electronic age (Jordan & Taylor, 2004, p. 1).

To this end, to recruit members to join their cause, hacktivist groups created what they call ‘operations’. The word operation reinforced the idea that they were not engaging in a mere protest or anarchy, they are embarking on a mission (Olson, 2013, p. 135). Any Anonymous member could create and name operations, simply by accessing the Internet Relay Chat (IRC) Anonymous channel. For example, long before the development of the Arab Spring, Anonymous waged Operation USA and Operation Payback. When the events of the Arab Spring started to unfold, Anonymous commenced one of its largest operations called Operation Egypt (#OpEgypt). Soon after the emergence of ISIS, Anonymous declared #OpIceISIS. This operation aimed to destroy ISIS’ propaganda and influence on the internet (see Figure 75).

5.9 Operation Ice ISIS
Part of the efforts to suppress jihadist propaganda online, the hacktivist group Anonymous declared operation ISIS. Griffin (2015) suggested that this operation concentrated its efforts on searching and neutralising ISIS’ online content on both social media platforms and websites using DDoS attacks. Known as #OpIceISIS, this operation succeeded in paralysing hundreds of ISIS-related channels of information dissemination, such as the ‘The Dawn of Glad Tidings’ application (#opISIS, 2015). This application, according to Berger and Morgan (2015), was the official mobile phone application, responsible for disseminating the latest news about ISIS’ operations.

To examine the role of hacktivists in attacking digital logistics of ISIS’ networks, I discuss the most prominent hacking collectives (e.g., GhostSec and CtrlSec) and individuals (e.g., Nun believer, Noon and Daesh eliminator), who voluntarily participated in #OpIceISIS. For the purpose of this discussion, primary data was obtained from the hackers themselves, through my personal contact with them via Twitter and through #OpISIS.
GhostSec claimed that they attacked 233 websites, destroyed 85 websites and had 25,000 Twitter accounts terminated. Jonny Appleweed, an anonymous hacker, devoted his time to attack ISIS on Twitter and on other digital platforms. He reported that:

> GhostSec operates like a military unit with members responsible for intelligence gathering, organising, logistics and of course, those operating the weapons, digital weapons that is. The group uses its skills and advanced tools to remove ISIS sites from the web either temporarily or in some cases permanently. (Appleweed, 2015)

Appleweed also explained the hacking techniques used by GhostSec to remove ISIS’ sites, including DoS attacks, Domain Name System (DNS) amplification, Structured Query Language (SQL) injection, cross-site scripting and brute forcing techniques (Appleweed, 2015).

### 5.10 CtrlSec

CtrlSec is a collective of hackers, who started to fight terrorist groups from their computers. They initiated #OpIceISIS after the Nice attack in August 2014, and subsequently aimed to identify and report as many ISIS-affiliated Twitter accounts as possible (see Figure 75). In other words, they are acting as the hammer in the ongoing game of whack-a-mole (see Section 5.3.1). According to Cottee (2015), the founder of CtrlSec is called Mikro. Cottee (2015) claimed that CtrlSec is closely related to GhostSec; both groups originated from Anonymous and thus, they share personnel and resources.

Mikro (as cited in Cottee, 2015) explained the techniques used to trace ISIS’ accounts on Twitter. He insisted that “every suspect tweet and Twitter account is tracked down manually
by one of the group’s 28 operatives, many of whom can read Arabic” (Mikro, as cited in Cottee, 2015).

Mikro (as cited in Cottee, 2015) claimed that CtrlSec identifies 200 to 600 pro-ISIS Twitter accounts per day. I have monitored the activity of CtrlSec on Twitter; it is obvious that the group reported hundreds of suspected ISIS accounts as #targets. However, many of these accounts appear to be false flags. That is, several reported accounts are owned by either anti-ISIS individuals, belong to Arab Twitter activists, or (in some cases) are news agencies, such as Al Jazeera. Through personal contact with the group administration on Twitter, I have suggested that CtrlSec are targeting random people, especially those who tweet mostly in Arabic (see Figure 76). To fight ISIS on Twitter, CtrlSec established a step-by-step tutorial to report ISIS’ accounts to Twitter support (see Figure 77). Also, on their webpage they encouraged people to take part in war on terrorism (see Figure 78).

![Figure 76. Screenshot shows false flags of suspected ISIS accounts.](image-url)
CtrlSec’s operation is more advanced than just searching for hashtags and filing reports. (Collier, 2015) reported that CtrlSec leader said, “that part of their operation includes enlisting native Arabic speakers, who pretend to be ISIS sympathisers, in order for CtrlSec operatives to be introduced to more reclusive ISIS members”. When targeting mass identification of ISIS’ affiliates, CtrlSec uses the very openness of Twitter—the same openness that helped ISIS spread its propaganda—against ISIS To examine the significance of reporting ISIS’ Twitter accounts and activity, I will discuss the data produced by CtrlSec in the following section.
5.11 Data Analysis of Reported Accounts

Primary data were obtained from CtrlSec regarding the number of ISIS’ accounts on Twitter that were targeted between February 2014 and September 2016. As shown in Figure 79, the total number of accounts reported to Twitter was over 25,000. As of March 2015, Twitter had suspended approximately 13,700 accounts. However, almost 11,600 reported accounts were not suspended.

Figure 79. Screenshot of ISIS-affiliated Twitter accounts, as reported by CtrlSec in 2015.

<table>
<thead>
<tr>
<th>Year</th>
<th>Suspended</th>
<th>Inactive</th>
<th>Targets</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/09/25</td>
<td>144,453</td>
<td>3,028</td>
<td>10,171</td>
<td>157,652</td>
</tr>
<tr>
<td>Previous month</td>
<td>138,457</td>
<td>3,045</td>
<td>10,027</td>
<td>151,529</td>
</tr>
<tr>
<td>Difference</td>
<td>+5,996</td>
<td>-17</td>
<td>+144</td>
<td>+6,123</td>
</tr>
</tbody>
</table>

Figure 80. Screenshot of ISIS-affiliated Twitter accounts, as reported by CtrlSec in 2016.

In September 2016 alone, CtrlSec’s total number of reported accounts exceeded 157,000, with almost 144,000 accounts suspended. In the previous month (August 2016), there were 151,000 reported accounts and 138,000 of these accounts were suspended (see Figure 80). The findings from this data suggest:
• ISIS’ resurgence on Twitter is dynamic.
• ISIS is an agile and resilient network, which maintains its presence on Twitter.
• The number of ISIS’ accounts appears to be beyond the imagination of platform owners, scholars and counterterrorism organisations.

Moreover, CtrlSec traces ISIS’ digital activity on JustPaste.it sharing portal. The data indicate (see Figure 81) that from January 2017 until September 2017, there were 7,223 accounts targeted. JustPaste.it suspended 4,045 accounts, while 3,176 remained active.

![Image of JustPaste.it statistics]

Figure 81. Screenshot of number of ISIS-affiliated content on JustPaste.it, reported by CtrlSec in 2017.

Milton (2016) also observed the effect of the degrading operation on Justpaste.it portals between January 2015 and April 2016 (see Figure 82). As shown in Figures 81 and 82, the 2016 degrading operation accelerated the suspension of ISIS’ accounts.
Overall, to measure the far-reaching impact of account suspensions on ISIS’ network performance is beyond the scope of this thesis. However, I have several observations regarding ISIS’ digital activity on Twitter, since the degrading operation started in August 2014:

- Despite its attempts to maintain its strong presence on Twitter, ISIS’ accounts have less followers compared to when ISIS started its Twitter activity in early 2014.
- ISIS’ communication strategy has changed; their focus has shifted towards disseminating propaganda videos.
- ISIS’ followers appeared to not follow other ISIS members, perhaps to evade suspension or identification as a target.
- ISIS continues to link its information on Twitter to other digital platforms.
- ISIS minimised use of #IslamicState, #Khilafah and #baqyia to evade suspensions.
- Suspensions sparked an influence warfare between ISI hackers and ISIS adversaries’ hackers.

5.12 Conclusion
This chapter examined the degrading operation on ISIS’ digital activity across digital media platforms. This chapter explored three countermeasures initiated by ISIS’ adversaries to paralyse ISIS’ IO over digital media platforms. These countermeasures involved degrading and destroying, countering ISIS’ propaganda, and hacking and information warfare.

According to data obtained from the hackers running #OpIceISIS, it appears that decentralised networks have performed robustly, compared to the countermeasures taken by government security agencies. This chapter has shown that Twitter—ISIS’ main hub—remains unable to cope with the resurgence of ISIS’ accounts. Further, Twitter is unable to control ISIS’ propaganda, because of the group’s use of trending hashtags. As Winter (2015a) argued:

No group does this more effectively than Islamic State [ISIS], the supporters of which have proved to be both resilient and quick to adapt to all counter-measures to date. Indeed, over the past year, despite the formidable obstacles that Twitter’s administrators now present them with, Islamic State’s propaganda productivity and rate of dissemination has continued to accelerate. (pp. 10–11)

While anti-ISIS powers worked hard to degrade its digital capabilities, ISIS managed to evade and minimise the effect account suspensions by harnessing anonymous sharing portals and encryption communication applications. In Chapter 6, I will examine the role of anonymous sharing portals and encryption applications within the digital logistics of ISIS’ networks.
6 Chapter 6: ISIS’ Information Feedback Loop

6.1 Introduction

In chapter 5, I discussed the strategy of ISIS adversaries to thwart information loop of ISIS networks by attacking its digital media logistics. The purpose of this chapter is to map of the media strategy of ISIS and to understand how they manoeuvred in information environments to maintain their networking structure and sustain flows of information. This manoeuvring sustained ISIS’ information flows and led to the accomplishment of its IO, by using micro platforms as the basis for auxiliary media logistics. This strategy was employed intensively after ISIS’ activity diminished on Twitter.

The aim of this chapter is to propose an examination of ISIS’ use of these portals as a response to the countermeasures against its online propaganda operations. This chapter suggests that anonymous sharing portals (e.g., sendvid.com, JustPaste.it and dump.to) and encryption communication channels (e.g., Telegram) have been instrumental in allowing jihadi groups to generate content, disseminate propaganda and communicate freely. These networks diminished the effects of the broad jihadi propaganda filtering efforts of popular SMNs. Crucially, while much of the literature’s attention has been concentrated on analysing the role of encrypted communication channels (such as Telegram), little attention has been paid to anonymous sharing portals that acted as black boxes for ISIS-related propaganda. Telegram played a critical role in recruitment and maintained a secure medium of communication. As such, the focus of this case study is on Telegram’s role in recruitment and as a catalyst for jihadis to initiate attacks in the West.

That said, the rise of distributed communication networks has offered new possibilities for the emergence and expansion of terror networks. Since its emergence in 2013, ISIS managed
to utilise digital media communication technologies to disseminate globally its propaganda content and foster communication between its members. In particular, images and video footage aimed to generate fear have been successfully broadcasted globally by the ISIS propaganda network. Noticing a correlation between the growing spread of ISIS’ propaganda videos on social media platforms, anonymous sharing portals, encrypted applications and the rise of terrorist activity in the Middle East and Europe, the US government established countermeasures in 2015, which were aimed to degrade and hinder the spread of ISIS’ propaganda online. These efforts included the deletion of ISIS’ online content and suspension of social media accounts, as well as hacker attacks against the websites used by ISIS affiliates. These countermeasures were largely successful in suppressing ISIS’ propaganda across popular social media platforms (see Sections 5.4 and 5.5).

In a clear effort to adapt to these countermeasures and sustain its information flows, ISIS moved the core of its propaganda network to other online platforms, substituting anonymous sharing portals for the popular sites they had previously dominated, such as Twitter and YouTube. These new online platforms were primarily encrypted communication channels such as Telegram, Signal, and WhatsApp, as well as anonymous sharing portals, such as JustPaste.it, sendvid.com and dump.to. Shehabat and Mitew (2018) referred to them as ‘anonymous’, because they protected the anonymity of their users and were, at the time, little known to the wider internet audience. It is important to emphasise that ISIS used these channels even before the network degrading countermeasures began. However, prior to the degrading countermeasures, these online platforms arguably played an auxiliary role in the overall communication strategy of the organisation.
These digital platforms have helped ISIS in building of an actor-networks. In other words, these digital platforms enable associations, connections and links between as many as heterogeneous elements as possible regardless they are human or non-human, individuals or collectives’ subjects or objects (Krieger & Belliger, 2014, p. 114).

This chapter is divided into two case studies. The first examines the role of anonymous sharing portals and their role in maintaining ISIS’ networking structure and sustaining its flows of information during the degrading operation. These portals will be analysed through an ANT concept of black box. ANT recognises the complexity of ISIS’ network assemblage and provides a means with which to conceptualise the role of anonymous sharing platforms in ISIS’ propaganda networks. The second case study explores the role of the encrypted application, Telegram, in its significance in catalysing lone wolf attacks in the West. This case study was derived from socio-sphere perspective, which Shehabat, Mitew, and Alzoubi (2017) called the ‘emergence of terror socio-sphere. These case studies acknowledge the paradigm shift that occurred in ISIS’ communication strategy. Early versions of these two case studies were published as journal articles.\footnote{Shehabat, A., & Mitew, T. (2018). Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. \textit{Terrorism Research Initiative,} 12(1); Shehabat, A., Mitew, T., & Alzoubi, Y. (2017). Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West. \textit{Journal of strategic security,} 10(3), 3.}

\subsection*{6.2 Case Study One: Black-Boxing the Black Flag—Anonymous Sharing Platforms and ISIS’ Content Distribution Tactics}

Due to their unique characteristics, anonymous sharing platforms play an important role in ISIS’ online strategy and thus, demand a specific framework of analysis. The ease of sharing
content and the anonymity of the users create a dynamic whereby platforms act as automated message amplifiers, playing the role of black boxes in the wider information network. Virtually all users on these platforms fall in one of three—often overlapping—roles: they either dynamically produce and aggregate content, act as intermediaries retranslating and curating content across multiple platforms, or passively consume the information flowing across the network. In other words, the content flowing through these platforms is highly dynamic and visual, lending itself to visual data gathering and ethnographic observation. As Moore (2014) argued, screenshots are a useful research method in this context because:

as digital tools, they diminish permanence in exchange for malleability and performativity. As media objects, they can be dynamically traced across the networks of their dissemination and require a re-evaluation of the axioms of cultural production that considers texts independently of experience. (Moore, 2014, p. 141)

In this case study, I first examine the broad online effects of the countermeasures aimed at the ISIS propaganda network. Second, using the notion of a black box drawn from ANT, I examine the relationship between ISIS jihadi and the emergence of anonymous sharing platforms. Finally, I examine three anonymous sharing portals to understand how they could have contributed to ISIS’ IO.

6.3 The Rise of ISIS on Information Environments

Since its emergence in 2013, ISIS quickly gained notoriety as a terror network, arguably due to the savagery it demonstrated against its enemies and people under its control. Concurrently, ISIS appeared to quickly recognise the importance of digital communication tools in its self-proclaimed goal to establish a global caliphate. Images of savagery were broadcasted virally through SMNs and global media and were clearly intended to frighten
enemies and lead to further gains on the ground in both Syria and Iraq. Twitter, YouTube and JustPaste.it were extensively utilised by ISIS to conduct its IOs: producing and disseminating propaganda videos for potential recruits and spreading its radical views among Muslim youth globally (see section 4.2).

The role of social media platforms in aiding terror organisations has been examined extensively by scholars, journalists and think tanks. For example, in *Populism, Extremism and Media: Mapping an Uncertain Terrain*, Alvares and Dahlgren (2016) highlighted the role played by web 2.0 platforms in the pervasiveness of the terror narrative, as these platforms created space for uncensored violent content. Alvares and Dahlgren (2016) argued that file sharing portals, videos and personal spaces, targeted different audiences namely, supporters, public opinion and enemies.

Before Alvares and Dahlgren (2016), in *Tweeting the Jihad*, Jytte Klausen (2015) claimed that the “jihadist insurgents in Syria and Iraq use all manner of social media apps and file-sharing platforms, most prominently Ask.fm, Facebook, Instagram, WhatsApp, Pal Talk, kik, viper, JustPaste.it, and Tumblr” (p. 1), while Twitter was the preferred domain of communication. Klausen’s (2015) article aims to address to what extent access and content to SMNs was controlled, and how the web 2.0 media environment altered not only the theatricality of violent incidents but also, more broadly, how media usage has affected terror organisations. To do so, Klausen (2015) collected information retrieved from 59 Western-origin fighters from the most notorious ISIS Twitter accounts known in Syria. She found out that “stream of self-publication using social media is, in fact, controlled communications” (Klausen, 2015). Terrorist-controlled social media now drives the ‘slow media’ coverage, because mainstream media have become captives of social media streams and thus,
vulnerable to misinformation campaigns and tactics of deception and misinformation. This is because social media easily amplifies false images of strength (Klausen, 2015, p. 20).

However, the social media activities of ISIS were monitored closely by the US and proprietors of social media platforms (Kimery, 2015), and were met by a series of countermeasures intended to degrade ISIS’ online presence (Higham, 2015). As stated in Chapter 5, the efforts—by the US and other anti-ISIS powers—to deploy countermeasures against ISIS’ online offensive have taken the form of three distinct phases of development.

Phase one involved degrading and destroying (see section 5.3). The US government requested Twitter and Google to delete ISIS’ active accounts on their platforms (Arthur, 2014). This measure resulted in deleting thousands of accounts and messages, in effect leading to global cyberwar against ISIS’ affiliates.

Phase two involved countering ISIS’ propaganda (see section 5.6). To compete with ISIS propaganda online, the US government and ISIS’ adversaries directed the efforts of the CSCC, USDOS team, Sawab Centre and UK Against Daesh (see Section 5.8).

Phase three involved hacking and information warfare (see section 5.8). Part of the less overt efforts at suppressing jihadist propaganda online, the hacktivist group Anonymous declared #Operation ISIS. Anonymous and other hacktivist groups claimed to take down and deface hundreds of ISIS’ Facebook pages and websites (see Section 5.10).

The online war against ISIS has reached a point whereby the US coalition forces, Anonymous hackers and other anti-ISIS actors have managed to seriously degrade ISIS’
information dissemination capabilities across popular SMNs. The countermeasures against
ISIS’ propaganda on popular social media platforms encouraged ISIS to shift the emphasis of
its IO to anonymous digital portals and encrypted communication channels, such as
JustPaste.it, sendvid.com, dump.to, SHAREit, Wood Vid and archive.org, as well as
Telegram, WordPress, Pinterest and Tumblr.

That being said, it is important to note that anonymous sharing portals (such as Telegram,
JustPaste.it, sendvid.com and dump.to) were already used by ISIS as auxiliary
communication channels prior to the degrading operation. However, for the purpose of this
case study, I aim to demonstrate that coordinated filtering across popular social media forced
ISIS to switch its primary IOs to these platforms and leverage them as communication black
boxes, which allowed ISIS to circumvent the primary vector of the campaign against its
operations.

This case study focuses on the lesser known anonymous sharing platforms (i.e., JustPaste.it,
sendvid.com and dump.to), which were used by ISIS to further its IOs and communication
objectives.

6.4 Degrading ISIS’ Online Activities

Popular social media platforms such as Twitter, Facebook and YouTube are using their
TOS to exercise control over the type of information produced and disseminated through
their networks. For example, YouTube’s TOS state in relation to hateful, violent and graphic
content that, “it’s not okay to post violent or gory content that’s primarily intended to be
shocking, sensational or disrespectful. If a video is particularly graphic or disturbing, it
should be balanced with additional context and information".\textsuperscript{106} Silverman (2014) observed that YouTube acts robustly when dealing with terror content. Under YouTube's TOS, the platform reserves the right to remove content and, in some instances, suspend accounts. According to a YouTube spokesperson:

\begin{quote}
YouTube has clear policies prohibiting content intended to incite violence, and we remove videos violating these policies when flagged by our users. We also terminate any account registered by a member of a designated Foreign Terrorist Organisation and used in an official capacity to further its interests.
\end{quote}

Berger and Strathearn (2013) indicated that when it comes to freedom of speech, social media platforms are biased. They suggested that these platforms should make it clear that freedom of speech is limited when it comes to using their service (p.41). In a similar vein, Twitter governs what is posted against its TOS policies (see section 5.5). With rising international pressure on these social network platforms, particularly from the US government over ISIS’ online materials, Twitter, Facebook and YouTube have acted swiftly and imposed harsh policies in which the gruesome content generated by ISIS is targeted. Twitter, for instance, waged a Twitter war against pro-ISIS accounts and managed to suspend many thousands of accounts, which resulted in a significant degradation of ISIS’ Twitter presence.

It also appeared that the broad countermeasures aimed at degrading ISIS’ propaganda was successful, at least in part because of wide Twitter account suspensions. Berger and Morgan (2015) argued that the mass account suspension strategy—known as Whack-a-Mole (see Section 5.3.1)—was highly successful as a network degrading tool (see Figure 83). ISIS

\textsuperscript{106} YouTube TOS can be accessed at https://www.youtube.com/static?gl=AU&template=terms.
found it challenging to keep up with replacing suspended accounts without suffering any negative consequences.

Figure 83. A tweet posted by Jim Berger on 20 September 2014.

In other words, Berger and Morgan’s (2015) study offered conclusive evidence that when account suspensions are carried out on a consistent basis across a range of platforms, they have an adverse effect on the targeted network. While Twitter has been largely successful in suppressing ISIS propaganda, Silverman (2014) suggested that hosting extreme content posed long-term challenges for all social media platforms, and that YouTube and Facebook in particular must keep updating their tools to dynamically trace and report graphic materials disseminated by potential terrorists. In this respect, proactive monitoring of platforms and targeted account removals have noticeably harmed ISIS’ content distribution and propaganda tactics on social media.

Interestingly, and in an apparent effort to resist such persistent network degrading operations, ISIS has tried to recruit personnel tasked with mitigating the effects of network attacks and sustaining their IO. As Atwan (2015) observed:

Most of Islamic state [ISIS] commanders and recruits are tech-savvy; coding (writing software programs putting information in html) is as familiar to them as their mother
tongue. Most of the digital caliphate business is conducted online, from recruitment to propaganda to battlefield strategy and instructions.

ISIS members and sympathisers have specifically targeted unpoliced, anonymous and safe sharing platforms, which allow the anonymous dissemination of uncensored content. Often, such platforms are also relatively obscure and unknown to the wider public—a factor contributing to their anonymity.

Ironically, and in a development reminiscent of the NCW theories of John Boyd, the overall success of the strategy of degrading any overt social media presence by ISIS appears to have led to the rapid changing of media dissemination tactics by ISIS, and the fast adoption of anonymous alternatives. Specifically, it appears that the ISIS switch to anonymous and obscure alternatives to popular social media platforms was made possible through the adoption of storage and sharing portals, such as JustPaste.it, dump.to, sendvid.com, archive.org, dailymotion.com and liveleak.com. As Boyd (as cited in Brehmer, 2005) famously argued:

> Generating a rapidly changing environment—that is, engaging in an activity that is so quick it is disorienting and appears uncertain or ambiguous to the enemy—inhibits the adversary’s ability to adapt and causes confusion and disorder that, in turn, causes an adversary to overreact or underreact ... [T]he message is that whoever can handle the quickest rate of change is the one who survives. (Brehmer, 2005, p. 10)

Boyd (1976) famously suggested that to win in an environment of high information density, one has to manoeuvre at speed and therefore, operate inside the OODA loop of one’s adversary (see Section 7.4). The weaponisation of anonymous sharing platforms has arguably
enabled ISIS to mass-disseminate propaganda while avoiding suppressive actions. This is an information equivalent of manoeuvring at speed and has provided a way for ISIS to operate inside the OODA loop of its adversaries. Further, as Shehabat and Mitew (2017) have argued, ISIS has successfully trialled stigmergic swarming operations, in which they harnessed multiple anonymous platforms to maintain their network structure.

In section 6.1.3, I focus on three case studies of anonymous online portals to illustrate their use by ISIS in establishing new channels of content dissemination and communication. Further, I examine how these portals allowed ISIS to maintain an operational network structure.

6.5 Anonymous Platforms as Black Boxes

As discussed in Section 4.12, to understand how ISIS has managed to route around extensive account suspension operations waged against it on popular social media platforms, it is necessary to examine the role of anonymous sharing platforms, by using a conceptual toolkit informed by ANT (Latour, 2005). From an ANT perspective, networks are populated by entities conceptualised as actants, because they simultaneously act and are acted upon. Actants, whether human or non-human, always have agency, which here stands for the ability to force change or a detour in the interactions between networks (Latour, 2005, p. 7). Agency, and action in turn, are always already the property of associations of human and non-human elements. Accordingly, one of the main strengths of ANT is that it allows the tracing of actors in a network, based on their actual role in the flow of agency (Law, 1999, p. 3).

When examining the role played by an anonymous sharing platform within the wider ISIS network, an ANT-informed perspective makes no distinction between social or technical
nodes in the network. The ANT perspective focuses on entities actively performing within a network. Therefore, anonymous sharing platforms immediately stand out, because they act as accelerators of information flows, while making it harder to trace the logistics of how these flows are performed. In effect, they black-box certain elements of the network. In this context, the black box is a conceptual metaphor developed in ANT to describe network assemblages that function so well that their internal logistics are “opaque from the outside” (Callon, 1986, p. 31). Black boxes are created through what ANT terms as “acts of translation”, in which actors are first enrolled in the network and then work to stabilise it from the inside, which creates the appearance of a monolithic assemblage (Besel, 2011).

From the perspective of these case studies, the black box concept helps to understand how ISIS maintained its networking structure by adaptively shifting operations to lesser known online sharing portals.

Opening a black box allows examination of the ways in which “a variety of social aspects and technical elements are associated and come together as a durable whole” (Cressman, 2009, p. 6). The notion of opening and examining a black box is possible, because when focusing on a black-boxed entity, which is seemingly homogenous from the outside, ANT sees “processes, performances, socio-technical rituals, and enactments […] driven by the dynamics of making connections, of binding things together, of extending associations, of “translating” and “enrolling” actors into networks” (Krieger & Belliger, 2014, p. 9). The same could be said for the role of online sharing portals, mobile phone applications and other technical assemblages enrolled in the networks of ISIS’ affiliates.

When analysing the case studies in section (6.2.4), it appears that ISIS is leveraging the stability and distributed nature of their relatively established communication networks to
enlist new actants, which in turn facilitates the emergence of new networks. Crucially, the relative opacity of lesser known cloud portals, such as JustPaste.it and sendvid.com, coupled with the migration of already established distributed networks of ISIS affiliates, who are drawn to these anonymous platforms by their appealing TOS, creates a black-boxing dynamic. Ironically, the operations degrading ISIS’ overt digital capabilities on popular social media sites have resulted in the migration and development of this dynamic. That is, ISIS’ networks seem to have reacted to the degradation of their capabilities on popular SMNs and rapidly migrated to new anonymous portals. As Stern and Modi (2010) pointed out, “Terrorists respond to changes in their environments by changing their mission and changing their shape. What is important in such events is that information logistics is essential in disseminating messages of terror” (Stern & Modi, 2010, p. 282).

6.6  ISIS’ Black Boxes

6.6.1  JustPaste.it

JustPaste.it is a free content sharing portal, which provides document storage and file sharing services under the motto of “sharing text and images the easy way”. The site is hosted by Cloudflare and owned by Polish entrepreneur Mariusz Zurawek (as cited in Fishwick, 2015), who described JustPaste.it as a platform in which ‘you are able to do what you want with almost two clicks. It doesn’t require registration, it isn’t searchable and access to specific content is only available via a link or if it makes the “most popular” page’. However, early in 2014, ISIS harnessed this service to disseminate its online videos, brutal images of beheadings, texts that aimed to spread its radical ideology and most importantly, the controversial digital edition of ISIS’ online magazine, Dabiq. Since its emergence in July 2014, Dabiq was hosted by JustPaste.it and archive.org. The English language magazine ostensibly targets Western audiences to garner new recruits (see Figures 84–86).
Figure 84. Cover of Dabiq magazine, issue hosted by JustPaste.it. Note: Full URL is obfuscated.

Figure 85. Tweet with extreme content posted by ISIS members on JustPaste.it. Note: Full URL is obfuscated.

Figure 86. Tweet with material advertising migration to ISIS-held territory posted on JustPaste.it. Note: Full URL is obfuscated.
JustPaste.it not only allows ISIS to host the magazine, but also offers a free folder share option, through which ISIS’ networked affiliates can share, store and disseminate information to global audiences. The platform offers advanced features, such as pasting text directly from a word processor or a web page, formatting and exporting to PDF, automatic importing of images, secure content publishing, Secure Sockets Layer (SSL) connection and password-protected access. To protect the contents of text notes from web crawlers, the site allows the use of encrypted tags. Indeed, one of the most valuable options JustPaste.it offers is password protection for disseminated content, which makes it a uniquely secure environment for exchanging messages or files.

Describing the site’s appeal to users, Fishwick (2015) also pointed out the easy-to-use template that functions effectively even on slow internet connections. JustPaste.it also has a mobile phone application, with no interruptions from pop-ups or other advertising materials. Leveraging these features, ISIS’ members and affiliates have utilised JustPaste.it to send encrypted messages, upload videos and files (such as jihadi materials, books and instructions), share information and upload online magazines. Links to the content uploaded on the site have been shared via Twitter, Facebook, Telegram and other social media platforms to increase participation for potential recruits, propaganda and other logistical support. Overall, JustPaste.it appears to have proved helpful to ISIS affiliates, as folders and files can be widely shared by only copying a hybrid link, allowing the file to be printed or read online.

107 Writing and formatting tools are also available for right-to-left languages (e.g., Arabic). Additionally, no login credentials are needed, and the platform works on mobile phone devices (JustPaste.it, 2014).
Arguably, the pervasiveness of ISIS’ *Dabiq* and *Rumiyah* magazines is indebted to the existence of this sharing portal. Interestingly, files uploaded to JustPaste.it can be deleted under the TOS agreement, according to JustPaste.it TOS:

- Any material posted anonymously will be deleted after five days.
- Any content that may spread hate or cause harm will be removed instantly.

Fishwick (2015) emphasised how the anonymity of JustPaste.it served ISIS, noting that “it’s role in Islamic state’s [ISIS’] propaganda machine has largely gone unnoticed”. All the images uploaded to the service by ISIS members have details of a related Twitter account stamped on them. The user’s Twitter handle is also printed at the bottom of each image, so reporters have been crediting the images to Twitter. The use of JustPaste.it by ISIS’ members has brought international attention to the site, with the site’s traffic approaching 10,000,000-page views per month (see Figure 87).

![Figure 87. JustPaste.it traffic in November 2015. Source: http://www.alexa.com/siteinfo/justpaste.it.](image)
According to Google Analytics (2015) “The platform has about 2.5 million unique users a month, which works out at about 10 million views every month”. Zurawek, the site’s founder, started seeing what he called “a large growth” of traffic to his website from Saudi Arabia, Egypt and Syria. The site makes it easy to publish text, photos or PDFs. At the beginning of 2014, rebels and civilians in Syria discovered JustPaste.it and began using it to post news. However, at some point over the summer of 2014, Silverman (2014) noted that “jihadists discovered it as well, and the site soon became one of the favoured tools of the Islamic State [ISIS] for sharing news, official communiques, and graphic propaganda”. As stated by its founder (cited in Fishwick, 2015), the site: “does not compete with advanced online text editors, such as Google Docs or Microsoft Office 365, but rather creates a place that is extremely easy and simple to use. It’s similar to Pastebin, the service popular with hackers, but with image files too”.

As the activity of ISIS on JustPaste.it drew the attention of authorities in the UK, the police requested that the site delete ISIS’ content, including all videos showing graphic executions at the hands of ISIS, as well as all pro-ISIS propaganda. In combating ISIS’ use of his service, Zurawek (cited in Fishwick, 2015) commented: “It’s not my choice that ISIS has selected my site … As long as I’m cooperating with the police, removing content, and not allowing ISIS to make propaganda, I think it’s good for the site that many people will know about it”.

The architecture of JustPaste.it, coupled with the possibility of using Virtual Private Networks (VPNs) and The Onion Routers (TOR) to obfuscate IP addresses, makes it hard to ban specific users. Nevertheless, the site appears to have made an effort to police the content uploaded by users and actively remove extremist materials. In response, an ISIS affiliate—
Abu Talout Al-Khurasani—messaged Zurawek to condemn the site’s efforts to police uploaded content. This demonstrates how significant the platform is to ISIS in maintaining its communication and dissemination structure. In the letter (see Figure 88), the author claims that 70 per cent of justpase.it traffic is ISIS content.

![Figure 88. A copy of the letter sent by Abu Talout Al-Khurasani to Zurawek. Source: JustPaste.it.](image)

### 6.6.2 Sendvid.com

Sendvid is an instant video upload portal, used by ISIS to route around wide account suspension and content deletion on YouTube and DailyMotion. Specifically, ISIS media production outlets such as Al-Hayat, Al-Furqan, and Al-Itisam extensively used the video uploading portal in their propaganda dissemination. HD quality videos, such as *Flames of War*, *Message Covered With Blood*, and *Healing of the Believers’ Chests* were first uploaded to Sendvid and then popularised virally through Twitter networks. A simple search for Sendvid on Twitter returns mostly links to ISIS propaganda videos. Sendvid is a crucial element of ISIS’ information logistics, as videos linked to Sendvid can also be shared via
other social networks such as Facebook, Twitter, archive.org, Tumblr, Telegram, dump.to and email, or can be stored in users Google Drive or Dropbox for future retrieval.

Sendvid has been used by ISIS affiliates from early 2015 to widely copy and aggregate propaganda materials and thus, build publicly available collections of terrorist-related content. As Mahzam (2015) pointed out:

The electronic digitisation of the extremist identity of ISIS has been made effective through its frequent injection of videos, incessant release of periodicals and downloading of visual reports in multiple languages, eventually building up a digital compendium that will remain accessible for future generations for reference.

Further, unlike YouTube, Facebook, and Twitter, wherein administrators are alerted to remove both jihadi content and the associated accounts, Sendvid is a safely unpolicied archiving platform, in which data can be uploaded anonymously, even under false Facebook, Twitter or Google accounts.

The following appears to be the standard reply to enquiries regarding jihadi content by the Sendvid support team:

Thank you for contacting us regarding this matter. As a service provider, we try to promote freedom of speech and remain as neutral as possible to all groups regardless of their views. With that being said, we do work with several foreign and domestic agencies in removing videos that we deem to be in violation of our Terms of Service. If you encounter any videos that violate our TOS, we encourage you to report them to our abuse department at: abuse@sendvid.com.
In theory, all online sharing portals have the same TOS in regard to removing videos or documents promoting violence. Sendvid’s TOS are quite clear that the service does not allow “adult, obscene, illegal or objectionable content” and that ‘accounts and content that violate this will be removed without warning”. However, in practice, Sendvid host these videos unless explicitly notified of breach of the TOS. Most of the gruesome videos uploaded by ISIS are in fact still available on the Sendvid service and are freely shared on Twitter (see Figures 89 and 90). Interestingly, Sendvid recently has become a preferred site for pornographic materials, which appears to have caused ISIS affiliates to reduce their presence, as this contradicts with Islamic sharia values.

Figure 89. Screenshot of video titled The Happiness of Almojahideen, posted to Sendvid.
6.6.3 Dump.to

Dump.to is an online sharing platform with no requirements for login credentials,\textsuperscript{108} using archive.is as a web carrier. The sharing portal also has no clear TOS policies that govern the dissemination of its content. The importance of this service in the context of ISIS is that it allows users to share, upload and converge links from similar sharing sites such as JustPaste.it and sendvid.com; all types of data can be stored and shared via link to ISIS’ affiliate networks. Dump.to allows documents, video, voice messages and music to be stored and shared, which in turn allows ISIS’ affiliates to aggregate, edit, curate, reclassify and republish jihadi propaganda content. In addition, content shared on the site can be protected by password, commented on and edited anonymously or by using a pseudonym. Most importantly, the lack of policing and governance makes dump.to a vital medium for information sharing among jihadi, who can communicate in the open through encrypted messages posted directly through the site’s interface.

\textsuperscript{108} Dump.to is registered to a German company operating behind the kasserver.com domain.
The site hosts most of ISIS’ online video propaganda content, as well as jihadi music (e.g., *Nasheeds*), *Dabiq* magazine links, and extremist jihadi books. For example, most of ISIS’ controversial books such as *Hijra to the Islamic State* (which translates as ‘migrating to ISIS land’) and *How to Survive in the West* were available to download for free, arguably helping ISIS recruit Western affiliates and encouraging migration to ISIS-controlled territories (see Figures 91–96).

**Figure 91.** Screenshot of iBRABO Twitter account, highlighting the use of dump.to by ISIS.

**Figure 92.** Jihadi training materials, books and propaganda available on dump.to.
Figure 93. Links to Dabiq propaganda magazine on dump.to.

Figure 94: Some significant dumps by Al-Hayat Media Centre (e.g., news reports, breaking news).

Dump.to considers itself a free and anonymous publishing platform that never takes responsibility for content being published. Typical of similar sharing portals, Dump.to’s TOS claim to prevent content or material containing child pornography, phishing and malware,
violent threats, spam campaigns, private and confidential information, or invasion of privacy.\textsuperscript{109}

6.7 Discussion

As their presence started to fade on Twitter and YouTube—as a result of the globally coordinated filtering campaign—ISIS decided to move the primary hub of their IOs to anonymous sharing portals such as Telegram, JustPaste.it, sendvid.com and dump.to. This was a strategic decision, to transition these sites from being used as auxiliary platforms to ISIS’ primary communication and dissemination channels within ISIS’ strategy. The characteristics and typology of these anonymous sharing portals—including ready templates, easy video uploads and mobile phone supported applications—created ‘participatory media’ (Jenkins, 2006) environments wherein information could be accessed across multiple SMNs. In other words, these digital platforms worked as information feedback loop to sustain information flows across multiple digital media environments include SMN’s. the dynamic of anonymous digital media portals that include aggregation and dissemination of videos, images, hyperlinks, documents and connectivity across other information environments created actor network that leveraged ISIS networks. That is, for ANT Anonymous sharing portals are actor networks that make a difference in the behaviour of human users.

\textsuperscript{109} An enquiry about ISIS’ use of dump.to services leads to the following standard reply from the company:

Dear visitor,

We are sorry that you have found improper content in our network. Please note that in order to process your abuse report and protect our users’ privacy and integrity, we request that you provide a photo ID (ID/Driving License/Passport/…) within 24 hours by replying to this email.

NOTE: Your report will automatically be rejected if you do not submit the requested documents

Dump.To team.
However, to understand dissemination dynamics and its connectivity across other information environments, it is estimated that JustPaste.it, sendvid.com and dump.to portals have contributed approximately 20 percent of the information disseminated by ISIS to Twitter alone (see Figure 97).


To an extent, these new sharing portals empowered ISIS’ message, by enhancing connectivity in the network and by adding more actors to its structure. From an ANT perspective, these new sharing portals served as information intermediaries, allowing for fluid and anonymous information aggregation, curation and dispersal. Publicly available, with the anonymity of no login required, allowed links and content to be aggregated and mass-distributed continuously and with variable dynamic intensity based on ad hoc requirements.

These platforms allowed ISIS to maintain its flow of information, enlist new actors and leverage its distributed affiliate and sympathiser networks to reach and mobilise potential
jihadi around the world. Further, as suggested in section 6.2, anonymous sharing platforms had a key role in the ongoing information warfare waged by ISIS. By using anonymous sharing platforms as black boxes in its information network, ISIS routed around social media account suspensions and leveraged new platforms as strategic information weapons to serve its IO objectives.

Importantly, as Krieger and Belliger (2014) pointed out, enhancing connectivity across the network generates information flows that are “increasingly difficult to control and steer” (p.143). It can be argued that anonymous sharing portals such as sendvid.com, JustPaste.it and dump.to “consist[ed] neither of objects nor subjects, but actors and mediators” (Krieger & Belliger, 2014, p. 187), which enabled the black-boxing of media hubs in ISIS’ IO strategy.

By examining the TOS policies of SMNs and anonymous sharing portals in relation to ISIS’ use of their services, it was identified that the financial capabilities and reputation of Twitter, Facebook and Google motivated them to take immediate actions against jihadi content. Meanwhile, the three anonymous sharing portals examined have the overriding aim of expanding their user base and seem to have extremely limited resources to track content disseminated by ISIS or other extremist networks who seek an easy, secure and fast medium of communication. The lack of resources makes the policing and active removal of ISIS’ content prohibitively expensive to the proprietors of these platforms.

Moreover, as already mentioned, the coordinated campaign to police Twitter and YouTube for jihadist content has forced ISIS to shift its focus towards using anonymous sharing portals as its primary tools for aggregation and dissemination of propaganda content. The
anonymous functionality of these portals acts as a black box, obfuscating the logistics of ISIS’ global propaganda network. When coupled with the ability to create hybrid web links and PDF files, which then can be disseminated across most social media, these platforms enable the rapid redistribution of content, even under conditions of severe policing and filtering. Even though anonymous sharing portals seem to have intensified their efforts to remove ISIS-related content, this does not solve the underlying problem. ISIS’ affiliates can still use these services for the aggregation of content advertised on other anonymous social media platforms, such as Telegram.

6.8 Conclusion

This chapter examined the role of anonymous sharing portals in relation to the dissemination of ISIS’ propaganda and network communication in the aftermath of the global degrading operation, orchestrated by the most popular social media platforms. The aim was to highlight the significance of anonymous sharing portals in terms of ISIS’ propaganda campaign. The main argument in this chapter is that anonymous sharing portals acted as black boxes for ISIS-related propaganda content, helping terror networks to sustain high-intensity information flows and maintain global communication channels. The emergence of these portals has fundamentally changed the way ISIS distributes its propaganda globally; these platforms allow terror networks safe aggregation and the ability to disseminate content links rapidly across popular social media without suffering from efforts to degrade the network. This in turn has enabled terror networks to maintain global IOs, even in the face of coordinated efforts at policing and filtering.\textsuperscript{110}

\textsuperscript{110} Internal challenges and dilemmas that social media platforms experienced is internal issues of policies on how to police their platforms. Facebook, Twitter, and YouTube update their terms of service on a
6.9 Case Study Two: Encrypted Jihad—Investigating the Role of Telegram Application in Lone Wolf Attacks in the West

6.10 Introduction

Between February 2015 and August 2016, Europe was subjected to a series of attacks by individual lone wolf terrorists\(^{111}\), pledging their allegiance to ISIS. Nice, Brussels and Cologne suffered over 400 casualties caused by lone wolf attacks. According to the Global Terrorism Index (GTI, 2016), the phenomenon of lone wolf attacks in Europe and North America intensified after the rise of ISIS. Calls for individuals to carry out lone wolf attacks were spread online through a sophisticated IOs strategy adopted by ISIS, with the self-professed goal of striking back at coalition forces. Communication technologies—such as social media platforms (e.g., Facebook), anonymous sharing portals (e.g., JustPaste.it), cloud computing (e.g., Google Drive) and encrypted communication applications (e.g., Telegram)—were the backbone of ISIS’ modus operandi. Importantly, the use of mobile end-to-end encrypted applications such as WhatsApp, Signal and Telegram contributed to the emergence of a new paradigm of terror communication—an online terror-sphere. As Hughes and Meleagrou-Hitchens (2017) argued:

\(^{111}\) The term lone-wolf is widely used by ISIS propaganda outlets to encourage attacks against western targets. For that purpose, I have used the same term used by ISIS not lone actors. Lone-actors is more convincingly within this context, but other scholars and academic, such as Wiemann (2015, 2013), have used the term ‘lone-wolf” when discussing terrorism in the west.
The emergence of applications such as Telegram, SureSpot, Kik, and—since its recent offering of end-to-end encryption—WhatsApp has been a particular game changer for the Islamic State [ISIS] and its efforts in the West. The wide adoption of newly introduced ‘end-end’ encryption communication technologies have allowed ISIS, as well as other groups, to establish and successfully leverage a secure medium of communication (p.1).

In particular, Telegram—largely due to its native support of encrypted one-to-one and one-to-many communication—has been widely adopted by ISIS and its affiliates globally. This case study aims to examine the role played by Telegram in ISIS’ strategy of encouraging lone wolf attacks to target Western countries. Launched in 2013 by the Durov brothers, the developers behind the Russian social network VKontakte, Telegram has arguably popularised the use of end-to-end encryption in social media messengers. In 2015, the Telegram platform introduced public channels, which enabled one-to-many communication alongside its core one-to-one functionality. Telegram channels enabled ISIS members and affiliates to establish their own media platforms with numerous followers. They were able to receive one-to-many messages, while also communicating individually across encrypted connections. ISIS members and affiliates created hundreds of channels, using the Telegram service to generate content, personalise encrypted one-to-one communications and therefore, control the logistics of dissemination of sensitive information and propaganda. Information broadcasted over Telegram channels can be instantly shared across multiple digital platforms and vice versa.

The significance of ISIS’ use of the platform lies in the ability to establish multipurpose channels, which strengthen ISIS’ propaganda machine. Crucially, this allows for ISIS affiliates, only latently connected to the central hub of the organisation, to receive and share a coherent centralised propaganda message as well as establish encrypted communication
channels with each other. Such channels act as systems of coordination, message reinforcement and activity planning.

The objective of this case study is to conceptualise the relationship between the emergence of Telegram as an information logistics tool of ISIS and identify its role in the surge of lone wolf attacks in the West. The case study focuses on the dynamics of ISIS’ IO to recognise different themes that characterise its use of the platform for terrorist mobilisation. Following a brief discussion of the methodology of the argument, the paper discusses the notion of a terror socio-sphere and concludes with preliminary findings.

6.11 Methodology

The study is based on an approach—informed by digital ethnography. This approach as ANT suggested requiring the tracing and mapping of network of actants. For that purpose, this approach required the researcher to join, as an observer, the public Telegram channels operated by ISIS members and affiliates. Identifying publicly available ISIS channels on Telegram was not difficult, because ISIS maintains a designated public channel called Nashir (which means ‘disseminator’ in Arabic). The broadcasting role of the channel is demonstrated by the number of ISIS affiliates on Twitter, who share and rebroadcast links to content originating from Nashir. In line with its broadcasting function, this channel operates in several languages, including Arabic, English, Turkish, and Spanish, and recommends trusted ISIS channels for its members to follow.

One of the important considerations when encountering such channels is their authenticity as legitimate ISIS-operated content distribution nodes. The author adopted a practical rule-of-thumb approach in establishing the authenticity of channels, by focusing on the themes
prevalent in the content and messages shared. For example, it is highly probable that any channel spreading hate towards the West, sharing authentic ISIS propaganda and encouraging attacks against Western targets is a trusted ISIS channel. In addition, another important metric that can be used as a filter of authenticity is the peer-to-peer filtering performed by ISIS channels themselves. Such channels will vet and share information from other trusted channels that are operated by ISIS affiliates and therefore, leverage a distributed crowd-filtered network to achieve a snowballing effect in terms of information dissemination.

The study mirrored this snowballing approach and involved the researcher joining 70 ISIS-affiliated Telegram channels. To collect the data from these channels, the researcher established a channel on Telegram, named ‘Data Collection’. The collected data includes all shared content, such as images and graphics, as well as videos encouraging individuals to attack Western interests (e.g., attacks against potential infrastructure networks, such as airports, water supplies and electricity grids) and the killing of military or police personnel. The information shared across these channels also includes instructional content aimed at potential lone wolf attackers, digital logistics advice aimed at channel members (e.g., opening a Twitter account using a hacked phone number), instructions for making small bombs and explosives and—most importantly—instructions for lone wolves on leaving media traces, such as videos or notes pledging allegiance to ISIS.

For the purposes of this case study, Shebabat et al. (2017) focused on three types of content:

- Information aimed at lone wolves, encouraging attacks and including instructions and methods of attacks.
- Information aimed to inspire other potential lone wolves to carry attacks.
- Information that celebrated acts of terror and claiming responsibility.
All gathered information is being presented as screenshots captured directly from Telegram channels. Screenshots are:

Excellent examples: as digital tools, they diminish permanence in exchange for malleability and performativity. As media objects, they can be dynamically traced across the networks of their dissemination and require a re-evaluation of the axioms of cultural production that considers texts independently of experience. (Moore, 2014)

Further, screenshots play an important role in making sense of data visualisation and provide the ability to map and graph the research method. For this study, the analysis sought to answer two important ontological and epistemological questions:

1. What do these data represent?
2. What claims can be made from them?

6.12 Terror Socio-Sphere

Since its emergence, ISIS rapidly adapted cutting-edge communication technologies to attain its IO objectives (see section 3.4). In many ways, this process resembles the way popular social movements across the Arab world leveraged social media platforms as a catalyst for political mobilisation during the ‘Arab Spring’.

Arguably, the important role of SMNs during the events of the Arab Spring uprisings precipitated the shift to a new communication paradigm in the Arab world, a phenomenon which has been termed the emergence of “new Arab public sphere” (see Section 3.5; (Lynch, 2006). According to Marc Lynch, the new Arab public sphere emerged as a result of “a
generation that has gained the platforms and the mechanisms to engage in sustained arguments, debate and discussions about their common concerns”. By contrast, as most Arab countries are ruled by either military personnel or coercive secular or theocratic regimes, freedom of speech, personal liberty and political debate are highly restricted. Most Arab regimes are non-democratic, and any call for grassroots political mobilisation condemning political power is persecuted. During the Arab Spring events, grassroots movements across the region were using social media to broadcast content calling for freedom, democracy and social justice. In effect, the emergence of social media facilitated the participation of Arab publics in political debate and acted as a powerful catalyst for political mobilisation.

The debate over the role of digital platforms in the emergence of this new public sphere is connected to the work of Jürgen Habermas, who developed the concept of the public sphere to account for “a realm of our social life in which something approaching public opinion can be formed” (Habermas, 1989, p. 85). According to Habermas, the most important feature of the public sphere is its engagement of the public in a “rational-critical debate”, involving such fundamental liberal rights as freedom of opinion and speech, freedom of the press, and freedom of assembly and association. Interpreting Habermas’s argument, David Krieger, and Andréa Belliger coined the term “socio-sphere”, suggesting an abstract space that is “neither private nor public, but it is based upon the new form of communication made possible by digital media, namely ‘many to many’ communication” (Krieger & Belliger, 2014, p.157). They argued that the new socio-sphere enables and encourages participation in different ways regardless of traditional boundaries.

The notion of a socio-sphere provides a useful framework within the context of this study, as it allows us to approach the role of Telegram in ISIS propaganda operations from a systemic
network-focused perspective. In supporting one-to-many as well as one-to-one communications, Telegram has in effect transformed ISIS sympathisers and affiliates into distributed information aggregators and disseminators, able to act stigmergically without direct coordination and control. As Krieger and Belliger point out, socio-spheres allow participants to be network actors despite geographic boundaries. Arguably, the rise of encrypted social media applications has produced a new triadic paradigm shift in communication, enabling the simultaneous performing of private-to-private, private-to-public, and public-to-public communication. To situate Telegram in the emergence of a digital terror socio-sphere, it is important to understand how terror organisations have harnessed the platform and how Telegram has served their agendas. Also, it is important to assess the topology and architecture of the platform, as well as the ways in which it has changed the dynamics of communication. Within this context, Shehabat et al (2017) argued that the encrypted communication affordances provided by Telegram have contributed to the emergence of a public terror socio-sphere. In particular, ISIS’ IO on Telegram is centred on one-to-many, many-to-many, and one-to-one communication with far-reaching ramifications.

Zizi Papacharissi has argued that individuals can engage socially in a private media sphere situated within their personal and private spaces (Papacharissi, 2010). This private social interaction sphere is rhetorically established by utilising existing and imagined geographical places (Papacharissi, 2010). Encrypted communication applications such as Telegram, WhatsApp, and Signal act as such geographic spaces, in effect enabling a participatory terror socio-sphere of information flows. This is in distinct contrast to other public communication channels such as Twitter and Facebook. The private/public socio-spheres of terror are enacted as spaces for potential terrorists to share common grievances in and thus, have become unifying rhetoric loci for ISIS-related propaganda aimed at affiliates and sympathisers. For
example, messages showing the brutality of coalition forces destroying homes and killing innocent people are constantly diffused across Telegram channels. This type of content serves as a force multiplier, in that it acts to unify affiliates around a cause perceived as just, as well as inspire potential lone wolves to carry on attacks. Importantly, the significant increase of the number of attacks against Western interests during the years 2015–2016 can be mapped to the rapid adoption of Telegram by ISIS in 2015. It has been established that the perpetrators of a number of lone wolf attacks in this time period used Telegram as their main communication channel (GTI, 2016). Consequently, Telegram has been perceived as a threat to the security of the European continent and the USA, insofar as it enables secure end-to-end communications across the new terror socio-sphere. Within this context, it is important to consider why ISIS shifted its IO strategy away from popular SMNs and migrated to Telegram.

6.13 ISIS’ Digital Migration to Telegram

Telegram promotes itself as an ultra-secure instant messaging system because all data is encrypted from start to finish, a process known in the industry as end-to-end encryption. Headquartered in Berlin, Telegram has more than 100 million active subscribers and is widely used in the Middle East, Central and Southeast Asia, and Latin America (Torbati, 2016). Telegram is considered the main hub for ISIS’ communication (Russon & Murdock, 2016).

While in this case study an attempt is made to examine the role of Telegram in lone wolf attacks, we set to examine the extent to which ISIS members and their affiliates are using Telegram to inspire potential lone wolves to carry attacks. The collected data obtained from ISIS’ Telegram channels suggested four main reasons behind ISIS’ digital migration to
Telegram: (1) seeking encryption, (2) seeking a channel-supporting platform, (3) enhancing ISIS’ digital infrastructure against cyber-attacks, and (4) decreasing exposure to hacktivism and other information warfare countermeasures.

6.14 Seeking Encryption

Prior to the emergence of ISIS, terror organisations such as Al-Qaeda were keen to encrypt and secure their communications. In the past, Al-Qaeda coordinated terrorist activities in Europe using draft messages on shared email accounts or by sending encrypted files (Nesser, Stenersen, & Oftedal, 2016). Personal anonymity and secure chat are important capabilities driving ISIS to adopt the platform. Using Telegram has made obfuscating and protecting attacker identities from Western intelligence agencies much easier, since only few electronic clues are left in intercepted datasets (Schechner & Faucon, 2016). While Telegram has been helpful to establish a socio-sphere and hide the identity of potential lone wolves, Nico Prucha has argued that anonymity and encryption have not benefited the strategic level of ISIS IOs (Prucha, 2016). He argues that the “secrecy and encryption of Telegram is harmful for IS’ swarming operations as the networks which are sustained on Telegram lack the outreach as well as the opportunities for projecting influence, which Twitter in particular allowed”. In addition, unlike encrypted applications such as Signal, which has been endorsed by Edward Snowden, some encryption specialists question the quality of Telegram encryption, suggesting that the platform may have a backdoor. That being said, Pavel Durov, the developer of Telegram, has consistently argued that the core of strength of Telegram is user anonymity, and has challenged encryption specialists to test Telegram’s protocols for exploits with a $100,000 USD reward (Kavanaugh & Shiloach, 2015).
Interestingly, WhatsApp, which is another popular encrypted communication app, was not adopted by ISIS because Facebook purchased it in 2013. Despite WhatsApp’s recent adoption of the same end-to-end encryption protocol as Signal, ISIS supporters are convinced it is not safe and is the easiest application to be hacked. Kavanaugh and Shiloach noticed that ISIS supporters who have long used other mainstream social media platforms, such as Twitter, have been increasingly joining Telegram. As stated in section 6.2.5, this is because Telegram allows its users to send encrypted messages, providing an advantage to jihadi while making it more difficult for law enforcement to identify ISIS affiliates online.

6.15 Seeking a Channel-Supporting Platform

As mentioned in section 6.2.1, one of the most important Telegram features, unveiled in September 2015, is the creation of public and private channels on the platform. This new feature enables users to establish their own channels to share information with an unlimited number of anonymous subscribers. ISIS strategically harnesses this feature by swarming Telegram with a large number of private and public channels in multiple languages and therefore, generates ad hoc networks ensuring its IO objectives. For instance, in the aftermath of the Paris attacks, for which ISIS claimed responsibility, Telegram suspended 78 pro-ISIS Telegram channels. Despite that, the Nashir political channel was relaunched in English, Russian, French, Turkish and Somali to maintain network presence and target potential international subscribers. In November 2015, ISIS swarmed Telegram with hundreds of channels, each specialised in a specific type of content. The most popular ISIS channels on Telegram are Dabiq, Nashir, Amaq and Gazwa. According to Berger and Perez (2016), these channels “have been used as the initial point of distribution for propaganda releases. Once released on Telegram, links to the propaganda content are subsequently distributed on Twitter”.

285
6.16 Enhancing ISIS’ Digital Infrastructure Against Cyber Attacks

In an effort to disrupt ISIS communications and other core functions, the US military’s Cyber Command announced the launch of its first attack against the organisation’s digital infrastructure in August 2015, during president Barack Obama’s visit in Hanover (Wie, 2016). Google, Twitter, and Facebook responded to calls from US Cyber Command to help shutting down accounts affiliated with ISIS, with Twitter suspending over 300,000 accounts related to the organisation. The degrading of ISIS’ Twitter affiliates network led many Western analysts to believe that ISIS in general was in decline (see section 5.2) (Prucha, 2016). These coordinated network degrading attacks pressured ISIS to shift some of its digital activities away from popular social media such as Twitter to other platforms such as Telegram, even though initially, as Berger and Perez argue, “these other platforms are used primarily as backups for Twitter” (Berger & Perez, 2016). While efforts have been made to severely degrade ISIS presence on Twitter and Facebook, governments have been finding it increasingly difficult to track and monitor communications on Telegram (Russon & Murdock, 2016).

Telegram’s functionality enables users to have one-to-one and group conversations that are end-to-end encrypted, and ISIS has taken full advantage of the platform’s privacy benefits to establish a community of channels, bots, and secret chat rooms. As Kavanaugh and Shiloach point out, “even anonymous, which claims to have hacked or crippled thousands of ISIS Twitter accounts and online forums, has been ineffective on Telegram” (Kavanaugh & Shiloach, 2015). An ISIS member called Abu-Osama Sinan Algazi has claimed that the network degrading operation has been largely unsuccessful, as “in this electronic war between the supporters and the Crusaders, lots of our brothers prefer Telegram over anything else” (Prucha, 2016).
Unlike Facebook or Twitter, which are capable of regularly suspending accounts in a centralised manner, Telegram’s more distributed nature, coupled with end-to-end encryption, demands a collective user-led effort to report ISIS-affiliated channels to the Telegram administrators.

6.17 Decreasing Exposure to Hacktivism and Other Information Warfare Countermeasures

In the context of US Cyber Command operations against the organisation in 2015, hacktivist groups such as “Anonymous” and “CtrlSec” declared #OpIceISIS (see Figure 98), aimed at hacking and disrupting ISIS’ online presence across a variety of blog hosting platforms, Twitter accounts, and mobile phone applications. Under the motto “ISIS we are going to kick you out of the Internet”, anonymous attacked affiliated ISIS websites such as “ummetislam.net” and took down the ‘glade of tiding’ mobile app, as well as thousands of ISIS-affiliated Twitter accounts (see sections 5.8 and 5.9). These swarm-like attacks were successful, to the extent that they forced ISIS to migrate its network to Telegram, perceived as a safer platform of operations.
6.18 ISIS on Telegram

The strategic rationale behind ISIS’ use of Telegram was outlined clearly by its Nashir channel in the following three objectives: (1) declaring electronic jihad, (2) waging media manoeuvre warfare, and (3) providing an online platform for the recruitment of lone wolves.

6.18.1 Declaring Electronic Jihad

The concept of electronic jihad was widely used by Al-Qaeda leaders such as Al-Zawahiri and Al-Awlaki to inspire and recruit potential members to Al-Qaeda. Al-Awlaki, for instance, used the concept “WWW Jihad for mobilizing prospective adherents and inciting terrorist actions” (Rudner, 2016). In a similar vein, ISIS used the concept of e-jihad to encourage followers and affiliates to establish Telegram channels and Twitter accounts. Throughout our observation of ISIS’ Telegram channels, we noticed a widespread conviction among the organisation’s affiliates that opening channels on Telegram is considered partaking in Jihad.
The concept of electronic jihad has been leveraged by ISIS to enrol numerous affiliates into a distributed network used to disseminate propaganda videos, organise financial support, issue warfare activity updates, reach out globally to potential recruits, and paint a propagandised utopian picture of daily life in the territories controlled by ISIS. Activities as simple as the dissemination of the ISIS weekly multilingual magazines *Dabiq* and *Rumiyah*, or the sharing of instructional materials focused on setting up encrypted communications and evading surveillance, or sharing updated safe channel lists, all count as electronic jihad.

### 6.18.2 Waging Media Manoeuvre Warfare

Periodically ISIS’ Telegram channels declare media manoeuvre warfare, or what they call “Gazwa e’lamyah” in Arabic. In practice, media manoeuvre warfare involves the mass re-opening of suspended social media accounts across multiple platforms, in conjunction with the creation of new accounts. This is viewed as manoeuvre warfare insofar as it is understood that the re-established accounts will exist only temporarily, soon to be shut down by the host platforms, though long enough to achieve a pulse-like broadcasting of messages aimed at a broader global audience. The pulse messages could like the following: “dear brother, don’t imprison yourself in Telegram channels only as most of your channel members are ISIS supporters, but break the chain and join channels of infidels and other social networks to upset your enemies. Strive to be among them in the networks they have created and be steadfast therein, patiently awaiting your reward”. In general, ISIS’ media manoeuvre warfare aims to:

- Identify and report anti-ISIS channels to be suspended.
- Post and upload videos and materials on Facebook and YouTube.
- Use currently trending hashtags to reach numerous audiences.
○ Tweet daily at peak times propagandising purported atrocities committed by coalition forces.

These messages are usually coordinated by ISIS affiliates calling themselves ‘The Media Mujahedeen’. Figure 99 shows an example of these messages, explaining the importance of media in winning the war against coalition forces. As stated clearly in Figure 99, the ISIS propaganda arm considers the media battle to be worth at least 75% of the overall victory. Framed in this way, ISIS supporters are considered to have direct responsibility to use media as a weapon. In addition, the message encourages followers to keep re-engaging with Twitter, considering it as the most important media field. In other words, ISIS believes winning the media war means winning the war against coalition forces.

Figure 99. Message forwarded from the Nashir Telegram channel.
6.18.3 Online Platform for the Recruitment of Lone Wolves

Part of ISIS’ stated IO objectives are to spread a message of fear among the native populations of coalition forces, and to inspire Muslims to engage in lone wolf attacks striking at Western targets (see sections 3.4 & 3.5). According to Ramon Spaaij, lone wolf attacks are characterised by a person working individually, not belonging to an organised terrorist group, and not directed by an outside command or hierarchy (Spaaij, 2010). However, direct online ties between individuals carrying out attacks in the West and ISIS networks are hard to prove and often uncertain, even though ISIS has claimed responsibility for most attacks occurring in the period between 2015 and 2016. Data gathered by Nesser, Stenersen and Oftedal shows that “only 6 out of 23 single actors […] acted solely based on online inspiration” (Nesser et al., 2016).

6.19 ISIS’ Telegram Channels

On November 26, 2016, the ISIS media channel Al-Furat released a video in French with Arabic subtitles, titled “Sur leur pas”, meaning ‘on their way’ in Arabic. According to Nico Purcha, “the video is in the 16:9 format, full HD, and features praise for the spate of ‘lone wolf’ attackers in 2016. The film demonstrates vividly how ISIS uses Telegram to instigate attacks” (Prucha, 2016). Reviewing the role of encrypted communication platforms such as Telegram in catalysing lone wolf attacks; our observations over the type of messages generated and disseminated via ISIS’ Telegram channels involve two main themes: (1) inspiring lone wolf attacks, and (2) claiming responsibility for, and celebrating acts of terror.
6.19.1 Inspiring Lone Wolf Attacks

The term “lone wolf” was initially coined in the late 1990s by two white supremacists, Tom Metzger and Alex Curtis, as part of an effort to encourage other supremacists to act alone in committing violent crimes. Other terms that have been used to describe similar or comparable forms of political violence include “leaderless resistance” and “freelance terrorism” (Weimann, 2012). According to the US Homeland Security Committee report (2016), ISIS “has successfully crowd-sourced its terrorism agenda by inspiring independent followers to conduct most of its attacks. Two-thirds of ISIS plots against the West appear to have been inspired by the terror outfit, rather than directed by it or carried out by trained jihadists” (HLSC, 2016). This skill to franchise terror has decreased the cost of the group’s operations and increased the impact of its violence.

As shown in Figure 100, the frequency of individual attacks occurring in the West increased markedly between July and August 2015, after ISIS called for lone wolves to carry on attacks. Significantly, two-thirds of these attacks were carried out by inspired individuals acting as lone wolves.
According to the Homeland Security Committee report, ISIS has been tied to at least 75 terrorist attacks against Western interests since early 2014 (HLSC, 2016). A list of ‘do it yourself jihad’ attacks against Western interests, compiled from ISIS’ Telegram channels, wherein ISIS claimed responsibility, and/or the perpetrators pledged allegiance is shown in Table 2.
<table>
<thead>
<tr>
<th>Date</th>
<th>Country</th>
<th>City</th>
<th>Weapon</th>
<th>Causalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 July 2015</td>
<td>France</td>
<td>Nice</td>
<td>Truck</td>
<td>80 killed</td>
</tr>
<tr>
<td></td>
<td>Germany</td>
<td>Wurzburg</td>
<td>Axe/knife</td>
<td>4 wounded</td>
</tr>
<tr>
<td>24 July 2015</td>
<td>Germany</td>
<td>Ansbach</td>
<td>Suicide bombing</td>
<td>15 wounded</td>
</tr>
<tr>
<td>24 July 2015</td>
<td>France</td>
<td>Rouen</td>
<td>Knife</td>
<td>1 killed (84 years priest)</td>
</tr>
<tr>
<td>22 March 2016</td>
<td>Brussels</td>
<td>Brussels</td>
<td>Suicide bombings</td>
<td>32 killed; 300 wounded</td>
</tr>
<tr>
<td>2 December 2015</td>
<td>USA</td>
<td>San</td>
<td>Shooting</td>
<td>14 killed; 21 wounded</td>
</tr>
<tr>
<td>1 January 2017</td>
<td>Turkey</td>
<td>Istanbul</td>
<td>Shooting</td>
<td>39 killed; 71 wounded</td>
</tr>
</tbody>
</table>

Table 2: Number of Lone Wolf Attacks Against Western Countries, Weapons Used and Number of Casualties. Illustrated by the author.

As an illustration of the method of catalysing lone wolf attacks, Figure 101 shows a message broadcast by the Nashir channel, encouraging individuals to carry out what they call ‘do it yourself jihad’. The message provides ideas to encourage lone wolf attacks, including examples of easy to obtain weapons as well as methods of perpetrating terror attacks.
In a significant example of escalating targeting capabilities, the UCC Telegram channel broadcast a link to a ‘kill list’ file posted on JustPaste.it and addressed at lone wolves, containing the alleged names, addresses, and telephone numbers of a hundred US soldiers (see Figure 102). The message uses two main hashtags, “#kill Dogs” and “#Individual wolves” and reads: “we know all your citizens INFO, and we have all your personal data. And your systems have failed to protect the most of your data [sic]. We are watching you. And we will kill you”.

Figure 101. Screenshot from ISIS Telegram channel, Nashir Political Services.
The UCC channel has also previously broadcasted links to manuals and instructions on terror tactics and methods aimed at lone. Such messages are usually identified with the “lone wolves #get ready” hashtag in Arabic (Figure 103), and suggest terror tools for ‘do it yourself jihad’ including guns, cars, trucks, knives, etc.

Additionally, prior to the 2016 Olympics in Rio de Janeiro, ISIS-related Telegram channels encouraged individuals to adopt Munich-style\textsuperscript{112} attacks targeting Western athletes. The use of the #RioLW hashtag (LW refers to lone wolves) on ISIS-related Telegram channels (see Figure 104) were considered serious enough to force Brazilian authorities to mobilise extra 200,000 military personnel to secure the Olympics.

\textsuperscript{112} Referring to the 1972 PLO terrorist attack on Israeli athletes during the Munich Olympics.
At any one point, a number of visual messages aimed at potential lone wolves circulate across ISIS-related Telegram channels, with the clear purpose of inspiring further terrorist attacks (see Figures 105 and 106).

Figure 103. Screenshot obtained from UCC Telegram Channel, titled ‘Lone Wolves #getready’.

Figure 104. Screenshot obtained from SITE intelligence group discussing the #RioLW hashtag.
Figure 105. Screenshot from the Sham State Media Organisation Telegram Channel, encouraging more attacks.

Figure 106. Screenshots from a propaganda video encouraging attacks, posted on the Barood Telegram Channel.
Overall, the number of people that have been killed by jihadi violence in Western Europe from 2014 to 2016 (273 people) is greater than the number in all previous years combined (267 people; (Nesser et al., 2016). This is due to a small number of highly deadly incidents, as shown in Table 2. In the period of 2014 to 2016 alone, 42 well-documented plots were registered (of the 42 plots, 38 were reported to be linked to ISIS), with nine plots registered in 2014, 17 in 2015, and 16 in 2016.

### 6.19.2 Claiming Responsibility for and Celebrating Acts of Terror

In the aftermath of each individual attack on a Western target, pro-ISIS channels on Telegram are flooded with images and posts mass-produced by online collectives of e-jihadists celebrating these attacks by hijacking popular hashtags such as #NiceAttack, #Nice, #Brussels (see Figure 107).

![Figure 107. Screenshot from ISIS Telegram channels celebrating lone wolf attacks.](image-url)
The process of establishing responsibility for and celebrating in the aftermath of lone wolf acts of terror works fluidly, whereby Amaq News Agency (the main media wing of ISIS) would usually claim responsibility for an attack in its immediate aftermath, and simultaneously encourage affiliates to celebrate the lone wolf across related Telegram channels and propagandise his pledge of allegiance, if there is one, across wider social media (Harris, 2015) see Figure 108 and 109).

Ironically, it appears that content disseminated by Amaq News Agency is considered authentic and trustworthy both by international media outlets and ISIS sympathisers. Even so, Western-led efforts to degrade and suppress its social media presence have pushed Amaq into adopting Telegram as its primary platform. To date, it appears that despite Telegram’s continuous attempts to take down the Amaq News Agency channel it keeps resurfacing with a large number of followers. The channel is important enough in the ISIS information warfare operations to feature lone wolf pledges of allegiance, filmed before or after major attacks (Figure 109).
There appears to be substantial evidence that Telegram is used by ISIS as a propaganda platform inspiring individual jihadist to act against Western targets. To ascertain its role in context, it is important to analyse lone wolf attacks in the West before and after the emergence of ISIS.

6.20 Analysis of Lone Wolf Attacks

To date, there is little evidence proving that ISIS is directly coordinating terror plots against the West, even though the organisation celebrates these attacks when they occur and claiming responsibility post factum. On a more conceptual level, Gartenstein-Ross has argued that the failure to identify direct ties between lone wolf attacks and ISIS is part of a broader and long-lasting pattern of underestimating the goals of jihadist networks in Western countries (Gartenstein-Ross, 2016). In France, ISIS member Rachid Kassim has been linked to at least two plots that were initially believed to have been carried out by lone wolves with
no oversight or direction from ISIS. He is also thought to have been the orchestrator of over half of the 17 total plots foiled by French authorities in 2016. Most of the planning was done through his Telegram channel ‘Sabre de Lumière’ (i.e., Sword of Light). In an analysis of 38 ISIS-linked plots and attacks in Europe between 2014 and October 2016, 19 (50%) were found to have involved online instruction from members of ISIS’ networks. By contrast, prior to the emergence of ISIS on Telegram, GTI indicates that in 2014 lone wolf attacks motivated by political extremism accounted for most deaths, compared to Islamic fundamentalism which accounted for only 19% of total deaths (see Figure 110).
Figure 110. Screenshot shows Islamic fundamentalism is not a major catalyst for lone wolf attacks in the West. Source: GTI.

After the emergence of ISIS and its subsequent calls for individual attacks against Western interest, Islamic fundamentalism became the primary motivation for terror attacks in Western countries. The strategy was outlined by Abu Mohammed Al-Adnani, the spokesperson of ISIS, who is on record saying that “lone wolf attacks in the US and Europe were dearer to us than the biggest action by us in Iraq and Syria” (Withnall, 2016). ISIS propaganda aimed at potential Muslim lone wolf attackers in the West have been systematically broadcast via social media available globally. As Weimann noted, “In nature, wolves do not hunt alone:
they hunt in packs. So, with the lone-wolf terrorists: there is a virtual pack, a social network, behind them. They may operate alone, but they are recruited, radicalized, taught, trained, and directed by others” (Weimann, 2012). Even though so far, the number of attacks that can be credited to lone wolves is less than 2% of overall terrorist activity in most countries, the problem is in the rapidly growing number of attacks and the tremendous difficulty in predicting and disrupting them (Spaaïj, 2010).

Crucially, as argued in sections 6.2.7 and 6.2.8, this process maps onto the ongoing efforts aimed at degrading ISIS’ digital capabilities, as the primary achievement of these efforts has been to push ISIS IOs to Telegram. Consecutively, security agencies and terrorism researchers have started highlighting the role of Telegram as a catalyst for terrorist mobilisation. In popular media this is typically framed as a new a sinister discovery:

The two men who are accused of killing a French priest on July 26 met on the service (Telegram), and the BBC reported that one of the attackers discussed his murder plan in a closed group there. So, it makes sense that French law enforcement would want to be seen as cracking down on possible terrorism plans on the app (Morrison, 2016).

In the aftermath of ISIS’ shift to Telegram there has been growing awareness in media and policy circles of the role played by encrypted communication technologies and the rise of lone wolf attacks in the West. In an October 2015 testimony before the House Homeland Security Committee, the then FBI director James Comey stated that:

ISIS has used ubiquitous social media to push into the United States, into the pockets, onto the mobile devices of troubled souls throughout our country in all 50 states with a twin message: come or kill, come or kill. Come to the so-called caliphate, live a life
of glory, participate in the final battle between good and evil on God’s side. Come to
the caliphate, and if you can’t come, kill where you are (HLSC, 2016).

Telegram is often considered the primary driver behind the emergence of a new style of
digital jihad because of its facilitation of encrypted communication between ISIS members
and affiliates (Russon & Murdock, 2016). There has been increasing awareness of the role of
private Telegram channels in the facilitation of radicalisation and coordination between ISIS
members and potential lone wolf recruits (Garcia, 2016). These types of channels act not only
as one-to-many propaganda outlets, but also as one-to-one and many-to-many coordination
platforms. Importantly, the secure format of these communications makes it much harder
for security agencies to ascertain the coordination logistics of terror acts and disrupt potential
attacks (Khalaf, 2015) see Figure 111). For example, even though there is no evidence that
Telegram was used to coordinate the Paris terrorist attacks, the attackers managed to
coordinate and execute their plans while evading detection by counterterrorism officials
(Kavanaugh & Shiloach, 2015). ISIS propaganda has been quick to claim responsibility for
lone wolf attacks while maintaining a propaganda image of overwhelming success (see
Figure 112).
6.21 Discussion

Most messages posted on Telegram by ISIS members and affiliates highlight the role of lone wolves in perpetrating terrorist attacks across Western countries. These posts work to both reinforce ISIS propaganda of success and positive momentum against the West, as well
as catalyse and recruit new lone wolf attackers from among a multitude of ISIS sympathisers. ISIS members and affiliates acting as e-jihadists are using Telegram channels as logistical tools to support outreach to and communication with potential lone wolves. Logistical support extends from facilitating secure one-to-many and many-to-many communication channels, to producing and rapidly sharing visual propaganda in support of attacks, free distribution of hacked or sock-puppet Twitter accounts, and instructions to evade surveillance through TOR and VPN. For ANT, this mechanism that connects network actors and integrate them in a social form. This new social form brings stability and determines the flexibility of the network (Krieger & Belliger, 2014, p. 186). Specific logistics information for perpetrating lone wolf attacks includes tools, potential locations, tactics for target identification, and methods of concealment. Weimann has argued that “in fact, almost all of the lone-wolf cases in recent years have involved the use of electronic social media. For lone wolves, online communication provides the needed social bonding, a (virtual) community and a source of guidance, support and moral backing” (Weimann, 2012).

In addition, Telegram channels have provided ISIS with a safe media environment allowing it to communicate propaganda to a global multilingual audience. Key propaganda messages are disseminated in Arabic, English, French, Portuguese, German, Turkish, and Spanish making it much harder to disrupt ISIS’ IOs. In effect, Telegram acts as an open-source marketplace of communication between leading figures of the terror organisation and a multitude of globally distributed affiliates and sympathisers. This is consistent with Gartenstein-Ross’s conclusion that encrypted social media applications such as Telegram have allowed ISIS to build cohesive and intimate online communities facilitating rapid radicalisation (Gartenstein-Ross, 2016).
It is important to note that, while Telegram has been leveraged effectively by ISIS and its affiliates, the terror organisation has failed to establish and maintain a wide media presence across popular social media platforms. ISIS-affiliated Telegram channels constantly encourage followers to reopen suspended Twitter accounts, demonstrating that the organisation still sees Telegram as a poor substitute for the global public platform of Twitter. The specific architecture of Telegram has forced ISIS to use it as a semi-closed coordination and initial media generation network involving: 1) ISIS fighters uploading information and receiving updates from battles in real time, 2) ISIS affiliates or sympathisers sharing news and updates, 3) anti-ISIS actors (Intelligence agencies, hackers…etc.), and 4) researchers and journalists.

Although direct links between ISIS and individual lone wolves are hard to substantiate, studies have found a link between lone wolf attacks in the West and specific calls from ISIS preceding them (Spaaij, 2010). That being said, the nature of lone wolf attacks necessitates a case-by-case study of each incident. Lone wolf attacks may be motivated by a combination of beliefs, personal vendettas, religious, or political objections. Moreover, the emergence of ISIS-related “virtual entrepreneurs” has injected additional network complexity into what were traditionally considered radicalised lone wolves attacking Western targets (Hughes & Meleagrou-Hitchens, 2017). For example, ISIS-related virtual entrepreneurs have been involved in assisting with travel logistics and therefore, act as connecting hubs between fully distributed lone wolves operating in target countries. This development has made it much easier to motivate and inspire individuals who are ready to perpetrate terrorist attacks.

6.22 Conclusion
This study represents an understanding of the role of encrypted social media in enabling lone wolf attacks. This case study illustrated how ISIS affiliates utilise Telegram, and the reasons behind the organisation’s digital migration. Although ISIS has effectively leveraged the affordances of Telegram, the organisation always asks its followers to harness other platforms such as Twitter and Facebook. Throughout this study, ISIS’ Telegram channels were persistently vulnerable to suspension by Telegram administrators. Popular channels such as Dabiq, Amaq and Nashir have been suspended hundreds of times, dramatically reducing their audience. Further, anti-ISIS actors have also migrated to Telegram, countering its propaganda and reporting channels for suspension. Nevertheless, it can be concluded that ISIS has harnessed Telegram’s affordances to encourage, coordinate where possible, and propagandise lone wolf attacks against Western countries, as well as maintain its global network of terrorist IOs.

However, to understand the role of micro-platforms and encryption communication applications in maintaining networking structure of ISIS networks, I argue that these new information environments are also enabled ISIS to launch swarming attacks as part of the information-centric warfare against its adversaries. In Chapter 7, I will explain how ISIS survived degrading operation using OODA loop manoeuvre warfare model.
Chapter 7: Distributed Swarming and Stigmergic Effects on ISIS’ Networks—Observe, Orient, Decide and Act Loop Model

7.1 Introduction

Up to this point this thesis has examined ISIS’ IO and digital media logistics that attempted to gain information superiority to maintain its networking structure and sustain flows of information. The aim of this chapter is to understand information warfare that has occurred between ISIS and its adversaries from a manoeuvre warfare perspective (see section 6.18.2).

The emergence of digital communication technologies has enrolled actors (humans and non-humans) through processes of translation and enrolment as suggested by ANT (Latour, 1987, 2005; Callon, 1986), which fundamentally changed the structure and communication dynamics and assisted the formation of new actor-networks, such as networks of terror. Previously hierarchical, centralized organisations have been reorganised as interconnected, decentralised and distributed networks. This shift has affected ISIS’ IOs, personnel communication and dissemination tactics (see section 6.1). To hinder ISIS’ communication and disrupt its IOs, the US government declared operation ‘degrading ISIS’ digital capabilities’ (see section 5.1). This operation leads to the intensity of information-centric warfare, as ISIS’ networks adapted stigmergic swarming operations to survive the interruption of its information infrastructure. In this chapter, I argue a paradigm shift in terror communication has emerged from adapting decentralised information logistical tools. The advent of anonymous sharing portals (e.g., JustPaste.it, sendvid.com), cloud computing (e.g., Google Drive, Dropbox) and encrypted applications (e.g., Telegram, WhatsApp, Signal) have supplemented terror organisations with logistical tools that helped the organisation to

---

An early version of this chapter has been published in the Journal of Media and Information Warfare, cited as Shehabat and Mitew (2017).
maintain its networking structure, evade interceptions and survive attempts targeting its IO capabilities. However, this analysis has a time period associated with it between 2014 and 2016 – that as part of the shift to distributed networks, the flexibility and movement to and away from platforms is common and that this chapter is not suggesting the use of these platforms in particular is static.

Ultimately, these new digital media environments enabled ISIS to launch swarming activities and play a pivotal role in information-centric warfare against its adversaries and vice versa. To analyse information-centric and manoeuvre warfare in the context of this study, I expand on Boyd’s (1974) model of manoeuvre warfare theory ‘Observe-Orient- Decide-Act’, commonly known as the OODA loop. In this chapter, first, I shed light on the OODA loop model and its role in the information manoeuvre warfare perspective. Second, I use the OODA loop framework as lenses through which to examine the change in ISIS and the IO of its adversaries as a result of new digital media environments. Finally, I highlight swarming and stigmergic practices ISIS opted to use to strategically engage in battles in the digital media environment.

7.2 Network-Centric Warfare: ISIS Versus the World

As observed in section (3.5) the declaration of Islamic Caliphate in August 2014 has fundamentally changed the network architecture of ISIS’ organisation. The shift from non-state actors to state actors and naming Mosul as the capital city of Caliph Abu Bakr Al-Baghdadi—required ISIS to use digital media technologies for C2 operations. This includes: networking, communication, information dissemination and propaganda. As Nissen (2015) argued, non-state actors such as rebel groups in Syria that do not have a formal structure need distributed information systems to coordinate, synchronising actions and for C2 operations (p.71).
The US, Shia militants, individual hackers and hacker collectives, attempted to disable ISIS’ communication capabilities by suspending accounts on popular social media platforms, hacking web pages and disseminating misinformation (see Section 5.2). To maintain its network structure, and organisation of C2 operations, ISIS managed to adapt its activities in multiple digital media environments to manoeuvre and survive the degrading operation strategy initiated by its adversaries. One way to understand this change is to employ the Network Centric Warfare (NCW) approach to the study of the networking by terror organisations. Cebrowski & Garstka (1998) argued that “the occurrence of structural and logical of NCW depended on information hosted by a high-quality information backplane” (p.5).

The logical model of NCW suggests that in the study of ISIS networks we should focus on the emergence of new tendencies of communication processes that transformed confrontation between ISIS and its adversaries into ‘open-source warfare’ depending on a complex processes of communication strategies. That is, as Robb (2015) argued that ISIS are using open-source warfare “to radically improve the quality and the security of its global insurgency and using the unmonitored one to one communication of the PlayStation Network (PSN) to coordinate attacks across the world”.

In other words, NCW is about taking advantage of digital networks by manoeuvring and exploiting IOs over digital media networks. It is important to acknowledge that

---

114 This includes controlling information flows, keeping channels of dissemination intact, opening channels of communication, and preserving their digital legacy for propaganda purposes.

115 A term coined by John Robb to describe how insurgent leverage on open source software and other communication technologies to organise themselves and share information (Robb, 2007).
geographically isolated forces depended on strong networking which considered the backbone for NCW (Smith, 2003, p.3). The distributed networking structure of ISIS depended on decentralised C2 operations and to some extent decentralised information logistics. This was revealed in ISIS’ on-ground advances and the reach of their message beyond the capacity of its adversaries. In the period between 2014-2016 ISIS clearly showed its ability to be a powerful organisation, capable of surviving sustained information-centric warfare.

C2 “is about employing the organisation’s logistics and capabilities (people, systems, material and the relationships between them) towards a specific objective or task” (NATO, 2006, pp. 5–7). From an ANT perspective, it is the enrolment of network actors that help to form network assemblages and maintain flows of information (see 4.11). To sustain flows of information and maintain networking structure ISIS managed to enrol many digital actors, including those offered by open-source digital media communications. Cebrowski & Garstka (1998, p.3) predicted that terror organisations would take advantage of the emergence of new cloud computing, sharing portals and encrypted applications. They observed: “access to all necessary information sources, weapons reach and manoeuvre with accuracy and speed of response are the facilitating elements to achieve to achieve high performance information grid which advanced C2 practices” (Cebrowski & Garstka, 1998, p. 6). This suggests that the high speed and accessibility of internet technologies enables the creation and distribution of content to flow across various information environments in the world at large (p.3). Cebrowski & Garstka prediction became reality as ISIS accessed these digital media technologies that became part of its C2 operation which enabled them to enrol actors to their network. For example, the architecture of sharing portals (e.g., JustPaste.it, share.it), platforms (e.g., Twitter, YouTube) and mobile phone applications (e.g., Telegram,
WhatsApp) enabled ISIS’ IO to enrol more actors in the formation of their information environment. This occurred as collaboration between networked digital environments shifted to network-centric operations, which “[…] are characterized by information-intensive interactions between computational nodes on the network” (Cebrowski & Garstka, 1998, p. 3). Moreover, Edward Smith argued that the militants’ capability to collaborate, aggregate, disseminate (see Section 7.8.3), create, analyse and access information gives them an advantage over their opponents and superiority in digital media environments (Smith, 2003). For example, information shared on anonymous digital platforms can be uploaded and shared on almost every digital technology including mobile phone applications. Hybrid links of shared information (see 7.6) can be downloaded, adjusted and shared.

To understand the need for ISIS to establish communication networks in the information environments we must examine the geographical space they operate in; the battle fronts they wage; the need for logistics; and the political structure of their organisation. On the one hand, the massive geographical space ISIS controlled in Syria and Iraq between 2014- end of 2016 (23 welayats or provinces) made it the largest terror organisation in the world.

Communication technology was essential to coordinate communication between divided forces across Welayats. Therefore, to keep their territory under control, ISIS established a communication hub in every Welayat (effectively establishing nodes in the network) to coordinate military action and maintain IO. The former Dutch General Fran Osinga asserts that this embrace of information revolution enabled the growth of ISIS networks. Dispersed forces were able to join, communicate, consult and coordinate efforts in more effective ways. It also assisted militants in adapting to new networking structures. To counter these newly formed networks, other networks must be created to defeat them (Osinga, 2007 as cited in
Safranski, 2008). In other words, this counter strategy worked in Iraq and Syria as the
government forces were unable to defeat ISIS militants (centralised versus decentralised).
The involvement of other networked militant groups such as Shia militant groups has
declared many victories in fighting against ISIS (decentralised vs decentralised).

In the context of ISIS networks, it was crucial for ISIS to adopt a distributed networking
structure rather than depend on the centralised operational network of its previously hieratical
C2 operations. IO of ISIS networks therefore, is empowered by what Edward Smith (2003)
calls ‘self-synchronized’ operations that accelerate the speed of command of ISIS networks.
Smith suggested that,

the network would permit us (the military) to decentralize or flatten the command
structure, taking the control function down to the lowest practicable level of
command and shortening the response cycle by removing unneeded levels of
command and control. (Smith, 2003)

The effectiveness of this decentralisation was observed in November 2016 while ISIS was
under pressure from coalition forces in the battle of Raqqa (Syria). Despite coordinated
opposition ISIS managed to take control of Palmyra city\textsuperscript{116}. This move demonstrated that the
speed of command by the decentralised networking structure of ISIS was more effective in
urban warfare compared to its adversaries centralised organisation. The battle of Al-Bab
(October 2017- Feb 2017) is another example of how the decentralised networking structure
of ISIS defeated Turkish forces during the first weeks of the attack. Turkey suffered severe
casualties and losses of military equipment as a result of the ISIS’ C2 operations which

\textsuperscript{116} I invite the reader to consult the timeline of the ISIS operation provided in this thesis on page xvii.
depended on information shared between units operating on the ground without an official hierarchy of command.

To understand speed of command of decentralised networks, in the context of information-centric warfare, Cebrowski & Garstka (1998) suggested that speed of command, has three parts: First, information superiority is a decisive factor to understand battlespaces. This can be achieved by adapting fast and powerful networks that depend on technology, simulation capabilities and excellent sensors. Second, speed and precision of effect-based swarming operations (to be discussed in section 7.5). Third, blocking of enemy’s operation before they start, this is referred to as operating inside the OODA loop of adversaries (which will be considered in section see 7.2). The aspects of speed of command, as suggested by Cebrowski & Garstka, were successfully employed by ISIS in the information warfare which was part of NCW. Applying speed of command aspects Cebrowski & Garstka regarded the technology used by unequal forces, number of military personnel and position they hold is a strength of NCW (Cebrowski & Garstka, 1998, p. 4).

Understanding Cebrowski & Garstka’s analysis of the speed of command from NCW perspective in relation to correlation between OODA loop and information network-centric warfare, Mark Safranski recognised three significant Boydian ideas have found their place in NCW: (1) the idea of manoeuvre warfare; 2) Swarming operations depended on unites acting in synch. Which Boyd refer to as auftragstaktik decentralised-based C2. These operations depended on complex information systems; and 3) Information superiority is decisive advantage in completing OODA loop cycle accurately and rapidly (Safranski, 2008). To emphasise on how network structure of ISIS networks deepened its roots in digital communication platforms and type of centric information warfare occurred. OODA loop
would help identify the dynamic of information-centric warfare arose in the networked digital media environment.

### 7.3 The Observe, Orient, Decide and Act Loop

The OODA loop is a theory for manoeuvre warfare developed by US fighter pilot Colonel John Boyd in 1974. Boyd established his strategy theory during the Korean war where he succeeded in taking down enemy fighter jets using the increased speed of decision-making, a process based on his OODA loop. The outcome of this approach is that “the side that can make the quickest decisions is most likely to win” (Osinga, 2005). The acronym OODA stands for Observe, Orient, Decide, Act which Osinga (2007) defined OODA loop as:

A circular arrangement of causally connected elements, in which an initial cause propagates around the links of the loop, so that each element has an effect on the next, until the last ‘feeds back’ into the first element of the cycle. The consequence is that the first link (‘input’) is affected by the last (‘output’), which results in self-regulation for the entire system (P.72).

Major Jeffrey L. Cowan, from U.S. Air Force described Boyd’s theory of manoeuvre warfare as the following: during air combat, a fighter pilot first observes his enemy using onboard sensors or his own vision. Then the pilot applies manoeuvring tactics based on his assessment to energy rate, tactics, type of aircraft and how to move into an advantageous position. Then, the overall assessment of type of manoeuvre needed to get advantage to be in offensive rather defensive position. Finally, unpredictable and asymmetrical manoeuvre to be accomplished with great speed. Then the pilot to repeat the cycle (Cowan, N. D). To understand manoeuvre warfare from military perspective, Colonel William Lind outlined the goal behind manoeuvre

317
warfare from an operational level “as the destruction of the enemy’s vital cohesion—disruption—not by piece-by-piece physical destruction. The objective of manoeuvre warfare is to disrupt the enemy’s mind. The principal tool is moving forces into unexpected places at surprisingly high speeds” (Lind, 2004, p. 56). However, manoeuvre warfare, according to Marine Corps doctrine “is a warfighting philosophy that seeks to shatter the enemy’s cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope” (Corps, 1997, p. 73).

To win the war, suggested Boyd, it is important to understand the OODA loop of your opponent more rapidly than they understand yours and to continue to do so. (Cited in F. Osinga, 2005, p. 6). Carol Kopp explained that the functions of the OODA loop are all about making the right decision and acting upon information gathered, distributed, analysed and understood. The faster we gather, analyse distribute and understand information the faster our decision is able to be made. The faster we act upon provided information the greater the superiority during combat (Kopp, 2005, p. 2).

Defeating the OODA loop of one’s opponent is achieved by going through the four stages in a faster loop than the opponent. This means that in the context of the overall dynamics of a complex theatre-wide engagement, the organisation able to operate in a more decentralised manner, in a pattern consistent with auftragstaktik, would likely be able to close its OODA loops faster and therefore is more likely to be victorious. For example, the faster a combatant gathers data from the field (observe), and analyses it into meaningful information (orient), the faster their decision-making (decide), which in turn gives them the opportunity to act beyond an opponent’s cognitive envelope (act).
However, Boyd’s manoeuvre warfare strategy theory was never officially published. According to James Scaminaci, Boyd “spread his thinking throughout the Pentagon via constantly evolving marathon briefings, each of which could last between 14 and 18 hours” (Scaminaci, 2016). Nonetheless, Boyd’s theory *A Discourse on Winning and Losing* has been reproduced thousands of times as journal articles, essays, and dissertations. As Grant T. Hammond, Boyd’s biographer, said, “He wanted to give things away—especially ideas” (cited in Cowan, N. D). Colonel Osinga, was the first to interpret and unveil the idea behind Boyd’s OODA loop model and suggested that the “significant operational advantage will accrue to the side that can complete the decision cycle—Observation-Orientation-Decision-Action—in the shortest time span” (F. P. Osinga, 2007). In his PhD thesis, *Science, Strategy and War*, Osinga (2005) described the usual interpretation of the OODA loop as a tool for strategy (a strategy for winning wars). Additionally, In *Patterns of Conflict* Boyd (1986) explained his “adapt and survive” strategy to win battles. As he puts it ‘operating inside an adversary’s OODA loop involves “Observe, orient, decide and act more inconspicuously, more quickly, and with more irregularity […]” (as cited in Richards, 2012, p. 9). Moreover, in *Essence of Winning and Losing* Boyd claims that our decided actions in combat cannot be achieve accurately without OODA loops. Applying the function of the OODA loop model enhances our senses and observations and helps in collecting necessary information, so we can carry out our actions accordingly (Boyd, 1996, p. 1).

In the illustration of the OODA loop (see Figure 113) Boyd documented the dynamic process of the OODA cycle and its relationship between components of his loop cycle operating inside enemy’s OODA. Boyd (1996) explains, “how orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window” (P.3). That is, OODA is a rapid process of
observations followed by orientation, decision-making, and acting. The faster a fighter loops using the four components the more likely they are to win. Edward Smith emphasised the OODA effects during crisis, war and peace times suggesting: observe phase depended on new information technologies that require greater time compression and precision. Sensor-based awareness is basic element of effect-based warfare that require vulnerability of opponents to act against and to achieve wanted outcomes. (vulnerability of the West is targeting and bombing publics or potential targets such as train stations, airports…etc (Smith, 2003).

Within the context of this study, Boyd’s OODA theory is useful for considering C2 operations dictated by centralised hieratical networks without reference to distributed versus centralised networks. While the notion of OODA and NCW is about manoeuvrer warfare occur between hierarchical centralised networks (states) in the physical world. Therefore, in the following, this chapter first applies OODA theory to distributed networks competing against centralised networks in battle, which occurred in the information environment (with some further reflections of physical warfare occurring between ISIS and its adversaries).

![Diagram of the OODA loop](image)

**Figure 113.** A diagram of the observe, orient, decide, act (OODA) loop, showing the OODA loop functions during combat.
The OODA loop model helps to understand patterns and effects of speed of command for both networks from NCW perspective. Boyd used the phrase “operating inside opponents’ OODA loops” which according to Osinga (2005) he “seemed careful never to define”. To operate inside the OODA loop of ISIS adversaries, Osinga’s suggested that this can be achieved through destabilising their adversary’s capacity to adapt and orient to various situations, while improving their own capacity to respond (F. Osinga, 2005). To better understand the pattern of conflict between ISIS and its adversaries in information environments from OODA loop perspective, the following shall examine information processes of OODA loop elements of both sides of the conflict.

7.4 Inside ISIS’ Observe, Orient, Decide and Act Loop

Examining ISIS’ OODA feedback loop helps to understand the function of distributed networks of ISIS in adapting and migrating to new digital environments and arrays of information-centric warfare. That is, ISIS can’t achieve its IO without having access to digital media technologies. These communication technologies enable ISIS to establish their actor networks and therefore it enabled them to sustain information flows and connectivity. In what follows, this chapter examines Boyd’s influence on NCW and the strategy of ISIS adapting to various digital media environments and includes analysis of the OODA loops of both ISIS and its adversaries, with attention to the dynamics of stigmergy and swarm operations. The argument put forward here is that, the speed of the decision-making process of ISIS networks is increased by harnessing anonymous sharing portals, cloud computing sites and end-end encryption applications. Speed of command helped in maintaining ISIS’ IO and created new trajectories for information dissemination tactics. Also, the topography of new digital environments enabled ISIS to launch distributed swarming operations based on a large-scale content distribution, efficiency, security and privacy to achieve its IO objectives.
The OODA loop cycle of ISIS (as noted in section 7.2) depended on a large number of smaller operations in the digital media environments, replicating what Edward Smith calls “semi-independent operations” (Smith, 2003, p. 61). For instance, hijacking Twitter hashtags using swarming strategies strengthened the spread of terror narrative (see Figure 114).

Figure 114. ISIS used #shahz al-hemam—that is, ‘glad tiding’—to assert their continued use of popular social media networks for electronic jihad.

These operations were masterminded by dispersed individual media jihadi or affiliates, who repeatedly disseminated information on a large scale and kept doing it. The can be considered as the Act phase in OODA cycle. These operations were facilitated by utilising multiple digital media environments in hope of disrupting opponents’ decision-making cycle by degrading their operation across popular social networking platforms. Based on the above knowledge, and through tracing of digital logistics of ISIS’ actor network, the OODA loop of ISIS networks can be described as the following:
7.4.1 Observe

Between 2013 and 2015, ISIS adapted digital media technologies to achieve its global ambitions by copycatting Al-Qaeda’s IO tactics in utilising internet technologies, including Twitter, YouTube, Facebook, which were the prime hubs for ISIS communication and dissemination strategies. Other digital media portals (e.g., Sendvid, dump.to) and end-end encrypted applications (e.g., Telegram, WhatsApp) were presented, but played a subservient role in ISIS’ IO strategy. Pro-ISIS digital jihadi observed interruption occurred to its IO caused by its opponents. Also, ISIS observed the emergence of new digital dissemination tools (share.it, Daily Motion, JustPaste.it), which enabled them to preserve and resume their IO through these online environments.

7.4.2 Orient

ISIS were oriented about the existence of new digital media environments such as JustPaste.it, sendvid.com, woodvid.com, dump.to, Telegram, Signal, Top4top, Tumblr and Pinterest that maintain connectivity and enable information dissemination. Also, understanding of SMNs vulnerability in terms of hacking, disinformation and media warfare was vital to ISIS— that sped up loop cycle of ISIS (decision phase) by disseminating misinformation and obtain sensitive information which required a costly security response from its adversaries. The function of new online environments where ISIS operated, enabled information movement from one medium of communication to another (e.g. Justpaste to Telegram). It also meant the use of many environments at the same time without losing the IO objectives of the dynamics of anonymous and encrypted communication platforms (see Chapter 6 for details). Hence, the adaption of new digital environments sped up decision-making cycle by creating multi-inputs evolved within multilayered digital portals.
7.4.3 Decide

To maintain connectivity and dissemination while ‘degrading operation’ underway (see sections 5.3.1 and 5.3.2), ISIS decided to launch its IO through the new digital media environments mentioned in the ‘Orient’ loop. Therefore, the existence of anonymous sharing platforms, encrypted applications and cloud computing site gives ISIS speed in adapting new information dissemination tactics.

7.4.4 Act

To maintain flows of information and carry out successful IO strategy, ISIS acted so quickly to degrading operation by adapting of new digital media environments. Speed in shifting its IO to new digital media environments have greater impact on ISIS’ IO and in maintaining of its networking structure (speed in command). Nevertheless, new processes of producing information dissemination cycle have increased dissemination mechanisms.
To this end, in examining speed of command and superiority in the battle of information environment, it is important to assess the OODA loop cycle of ISIS adversaries.

7.5 Inside the Observe, Orient, Decide and Act Loop of ISIS’ Adversaries

The function of OODA model is to assist in winning battles. So, to defeat ISIS in the information environment, it is essential for its adversaries to operate inside the loop of ISIS networks and paralyse its IOs. To do that, Boyd suggested, [...] we change the situation more rapidly than the opponent can comprehend and keep doing it (Boyd, 1986, p. 5, as cited in Richards, 2012, p. 9). In interpreting Boyd’s thoughts of OODA functions, Osinga argued that, as an enemy relies on information and communication systems, disrupting and destroying their information and communication systems is essential. Attacking the communication systems of enemies can lead to superiority during conflict (Osinga, 2007 as cited in Safranski, 2008). That is, trace activity of ISIS by its adversaries in new digital environment and block it before content reached wider audience. For example, recently ISIS adversaries succeeded in collaboration with Mr Mariusz Zurawek, the developer of anonymous sharing portal JustPaste.it, to blackout content linked to ISIS accounts (see 6.1.4). Therefore, to achieve dominance over information disseminated by ISIS affiliates, Osinga asserted, it is important to get advantage over information flows of adversaries. This will lead to destroying the enemy’s C2 operations and to operating inside their OODA decision more rapidly (Safranski, 2008 as cited Osinga 2007).

To achieve the objectives of degrading operations, Osinga suggests adapting to a game of Interaction and Isolation (see section 5.3.2). This can be achieved through complete isolation of opponents from the information environments they operate on. This process will lead to losing internal and external cohesion of opponents’ networks by disruption of information flows. Isolating ISIS from Twitter, for instance, has created chaos in ISIS’ IO (as discussed in
5.2.2). As a result, ISIS called on affiliates to initiate operation #elzamthagrak, which means ‘stay in your domain’, to maintain their processes of communication. The aim behind the strategy of Interaction and Isolation, as Osinga (as cited in Safranski, 2008) pointed out, “is to change the opponent from an open into a closed system which slowly suffers the fate of all closed systems”. Within the latter context, to understand how OODA loop feedback of ISIS adversaries operate is illustrated in Figure 116.

Figure 116. Inside the observe, orient, decide and act loop of ISIS’ adversaries. Illustrated by the author.

7.5.1 Observe

In this phase ISIS opponents seek to observe ISIS’ IO objectives and processes of information diffusion. This includes collecting data to identify strengths and weakness of terror narratives and motivations to help establish and direct counter narrative agendas. ISIS adversaries observed that the terror narrative moved across popular social media platforms particularly on Twitter and YouTube in 2014. For example, Berger and Morgan (2015) monitored activity of ISIS on Twitter suggesting ISIS has almost 90 thousand Twitter accounts in 2015.
7.5.2 Orient

Identification of the many new digital environments aiding ISIS’ message to spread, which included: identify the disseminators and type of message; ontology of messages, generators and dissemination processes; Aggregating and analysing of disseminated content. which in this phase ISIS adversaries managed to identify the main nodes of communication and message generators. For example, targeting messages generated by Asawrity media and Shami Witness have impacted on the number of propaganda produced to serve ISIS’ IO. Also, the contentious attacks on the main channels of dissemination on Telegram such as Dabiq, Nashir political and Amaq have helped to control the spread of ISIS channels on Telegram.

7.5.3 Decide

In this phase ISIS opponents moved in fast to counter ISIS’ messages by tracing and identifying dissemination processes and creating chaos in ISIS’ information environments. Disrupting ISIS dissemination tactics was critical and hindering its message of terror was a step towards adapting the ‘Interaction and Isolation’ strategy as suggested by Osinga. ISIS opponents managed to create noise in the communication networks of ISIS (mostly in Telegram and Twitter) by waging information warfare, which included; inserting disinformation through network participation; suspension of ISIS accounts; hacking operations and creating counternarratives on digital networks. In Telegram channels, for example, ISIS opponents were able to join ISIS’ Telegram channels and report it to Telegram as channels spread hate and terrorism. As a result, Telegram opted to suspend these channels more often (see section 6.2).
In identifying the dissemination processes of ISIS networks, ISIS opponents’ response was twofold. First, they degraded ISIS’ digital capabilities by hacking, introducing misinformation and tracing locations of disseminators. The ‘whack a mole’ operation, for instance, was successful in paralysing ISIS’ social media accounts on Twitter and YouTube (see section 5.3.1). The most powerful pro-ISIS affiliates, Shami Witness and Turjuman Asawrty networks, were paralysed permanently after police traced their location and leads to the arrest of Shami Witness (see Figure 117). Also, it has been reported than more than 300,000 accounts associated with ISIS have been suspended by Twitter Inc.

![Shami Witness Twitter Feed](image)

*Figure 117. Screenshot of Twitter feed of ISIS propagandist, Shami Witness.*

In examining the OODA loops of both, ISIS and its adversaries, it can be observed that speed of command of ISIS was faster in adaptation and survival game compared to its adversaries. The more attacks on ISIS information infrastructure the more it moved to new digital environments. This argument was echoed by Michael Waller (2015) US military strategist and Secretary of Defence Advisor who argued that jihadi movements including ISIS and Al-Qaeda have “penetrated our own OODA loop and have affected our ability to orient, decide
and act” (Waller, 2015, p. 30). However, the resilience of ISIS networks and survival of degrading operation is because of ISIS’ adaption of distributed swarming operation in the information environment, to be discussed in the following section.

7.6 Swarming and ISIS’ Information Operations

This aim of this section is to examine the information-centric warfare of swarm operations of both ISIS and its adversaries. Since the rise of Calipha in 2014 the success of on-ground operations and the expansion of territories fall under ISIS control, ISIS called collectives of e-jihadists and fighting groups to swarm digital media environments to achieve speed of command and carry out IO objectives. Meanwhile, ISIS adversaries, employed swarming operation to degrade ISIS’ digital capabilities and destroy information networking infrastructure. The US government established the United Counter-terrorism Centre (UCC) to counter the narrative of Al-Qaeda and then directed its activity to fight ISIS in the information environments (see section 5.7.2). Also, the collective hacker groups such as Anonymous established #OpIceISIS in 2014 to help in degrading operation (see 5.10).

Swarming is a military tactic derived from animals and insect behaviour when attacking its enemies. A swarming attack occurs from multiple directions in order to control and paralyse an enemy. Swarming attacks rely on what Libicki (1994 as cited in Arquilla & Ronfeldt, 2000) calls “the many and the small” (p.22). Arquilla & Ronfeldt argued that “swarming is also likely to prove valuable to terrorist and transnational criminal organisations” (Arquilla & Ronfeldt, 2000, p. 43). Furthermore, John Robb, in Brave New War, identified two types of swarming operation, the “massed” and the “dispersed” (Robb, 2007, p. 122). According to Robb (2007), massed swarming is based on distributed operations, such as those that occur in a hive of bees. Massed operations start as a single unit and then divide to swarm the target.
Dispersed swarming, on the other hand, is based on small operations by decentralised groups that have special tasks; one example of dispersed swarming is the Minutemen, who inflicted heavy casualties on the British army during the American revolution in the battle of Concord during the American civil war. Robb gave another account of dispersed swarming, which occurred in Iraq in 2007, where small groups or individuals of anti-US actors/guerrillas attacked identified targets such as a sniper (Robb, 2007, p. 122).

The swarm activity of ISIS affiliates can be described as spontaneous coordination between ISIS members/affiliates in diffusing, sharing and generating information across the spectrum of digital media environments. In ISIS Telegram channels, for example, ISIS’ propaganda videos, publications and personnel communication is shared across the platform via hybrid links codes that lead to the anonymous sharing portals. Purcha (2016) observed that ISIS Telegram channels maximised the global reach of its propaganda during the Brussels attack in March 2016. ISIS Telegram channel operatives encouraged affiliates to hijack trending Twitter hashtags and disseminate information in French language. Also, ISIS harnessed other media environments to conduct what they call “social media raids” to maximise flow of information and reach of this information (Prucha, 2016, p. 52).

The decentralisation of ISIS networks empowered the swarming operations as collectives of e-jihadists carried out ISIS IO strategy without coordination and even an identifiable leader. Prucha observed that jihadist media strategies have been demonstrated to be resilient and intelligibly implemented during online swarming operations: “The disbelievers ... are confronted in their media war by an army of [IS] supporters who dedicate their time for the defence of the people of jihad” (Al-Ghazzi as cited in Prucha, 2016, p. 54). These jihadist strategies reconfigure constantly, like a flock of birds or a bee-swarm.
As digital media became the backbone of ISIS networks, the study of media manoeuvre warfare in context of swarming operations part of NCW is required. Cebrowski and Garstka (1998) noted “Information technology is undergoing a fundamental shift from platform-centric computing to network-centric computing” (p.3). Which means that NCW occurs when outnumbered ISIS agents storm multiple digital media environments with information to fill them with terror narrative and propaganda. According to Leonard Doob “Propaganda was considered an arm of warfare” (Doob, 1950, p. 424). For instance, ISIS appeal to affiliates to launch swarm attacks on Twitter, which includes: the re-opening of suspended accounts; the hijacking of trending hashtags; the hacking of opponents’ accounts; and the mass and diffuse spread of information and misinformation across multiple digital media environments, because (as discussed 4.10.2/3) ISIS believes that Twitter is the most important medium for information dissemination. These swarm operations were coordinated and directed by e-jihadists through digital media environments. Arquilla & Ronfeldt argued that “swarming depending completely on robust, rapid communications” (Arquilla & Ronfeldt, 2000, p. vii).

To understand the role of digital media technologies in ISIS’ swarming operations and speed of command, Arquilla and Ronfeldt (2004) suggested that, new information technologies “render an ability to connect and coordinate the actions of widely distributed “nodes” in almost unprecedented ways” (P.4).

Successful swarming can happen when participants “engage adversaries from all directions simultaneously” (Arquilla & Ronfeldt, 2000, p. vii), which ISIS performed and coordinated utilising different digital media environments simultaneously. These swarming actions occurred, consequently to its opponents’ degrading operations. Arquilla and Ronfeldt (2000) argued that swarming is enabled by information transformation and IOs circulated across much of the spectrum of battle (P.43) and the swarming of networked actors will lead to
defeat adversaries in detail (Arquilla & Ronfeldt, 2000, p. 5). An example of coordinated distributed swarming of networks in the information environment is the reopening of suspended Twitter accounts and it has been estimated that ISIS managed to open almost 900,000 accounts using fake names, generic emails and hacked phone numbers. This swarming operation were a major blow to degrading operations.

Digital communications enable the rise of swarm networks and to hinder the swarming activity of networked actors, Arquilla & Ronfeldt suggested, a high level of information security is needed. Poor information security would rise the cost of decoding and intercepting adversary’s communication (Arquilla & Ronfeldt, 2000, p. 67).

7.7 Stigmergy Operations of ISIS Networks

The coordinated efforts of ISIS actors to swarm digital media environments of IOs is what military and network analyst John Robb (2007) in his book *Brave New War* and in *Global Guerrillas* blog analyse from a stigmergy perspective. According to Robb (2004) “stigmergy can be used as a mechanism to understand underlying patterns in swarming activity. As such, it can be applied to the understanding of swarming attacks by diverse bands of global guerrilla”. The indirect coordination between ISIS e-jihadists using digital media environments is an example of the practice of stigmergy. That is “Creating baths for information distribution through Self-organised cluster of individuals who have knowledge in access to digital networks” (Robb, 2004). The study of stigmergy in context of ISIS networks enables ISIS adversaries to understand mechanisms of ISIS digital networks for the purpose of disrupting its IO. However, stigmergy “is a term used in biology, from the work of French biologist Pierre-Paul Grasse, to describe environmental mechanisms for coordinating the work of independent actors” (Robb, 2007, p. 124). Take for example, ants that use
pheromones to create chemical trails for other ants to follow. In a similar way people use weblog links to establish information paths, for others to follow (see Figure 118).

Figure 118. Hybrid web log links to ISIS content disseminated via Telegram.

The term stigmergy is derived from the Greek words’ *stigma* ("sign") and *ergon" ("to act"; Robb, 2007, p. 124). In the context of this study, I examine the indirect communication between ISIS affiliates and e-jihadists in digital media environments that have affected the speed of command for ISIS IO.

Robb (2007) described the mechanisms of environmental coordination in the context of global guerrillas as marker-based, sematectonic, quantitative and qualitative, which will be discussed and analysed in the following sections.

7.7.1 Marker-Based

Markers or signs left by actors influence the actions of other actors. In the context of global guerrilla warfare, a marker or sign could be the site of an attack and the news of the attack
delivered by traditional broadcast and the newer forms of social media. The description of the
attack in the media is a stigmergic marker for others to follow. An important example of this
stigmergic marking is the idea of ‘lone wolf’ attacks. Lone wolf attacks include ISIS
perpetrators, loners who committed terror attacks, which leave distinct marks behind them.
Markers can be a short video of the perpetrator/s pledge of support to ISIS or describing their
forthcoming actions. In both cases mainstream and other media highlight such events on their
headlines.

7.7.2 Sematectonic

Environmental conditions influence the behaviour of all actors in a system. This applies to
terrorist activity, for example multiple guerrilla’s attacks on a certain type of target can
generate a global security response by nation-states, which changes the potential of attacks
against that type of target in the immediate future. An increased security presence is a
sematectonic signal to terrorist operatives to select something else. Robb (2007) notes that
“stigmergic systems use simple environmental signals to coordinate the actions of
independent agents (each with their own decision-making process)” (P.124). A key example
of this is the attacks on train and airport network systems by ISIS lone wolf or wolf pack
operations in Brussels, Turkey and USA that occurred between 2015 and 2016 (see Section
6.2 for greater detail). Similarly, part of the electronic jihad operations that ISIS encouraged
it affiliates to engage in used hacking strategies to attack energy networks. ISIS urged
followers using Telegram to secure communication by adopting anonymous sharing portals
and utilise ZeroNet Network technology to evade degrading operations. As ZeroNet system
makes it hard to remove hosted websites (C. Liang, 2016, p. 86).
Quantitative signals are scalable. This means that the size of a global guerrilla attack on a given location can meter the scale of the security response. For instance, the attack in Nice, France, on the 14th of July 2016, involved a perpetrator running over Bastille day celebrants with his truck, killing 80 people. The size of the attack carried out with a basic and easily available resource worried security agencies across Europe. Security agencies were not familiar with the vehicular method of attack and as a result, France declared a state of emergency, deploying and mobilising the military to protect the network infrastructure from future attacks. Moreover, during the 2016 New Year’s Eve celebrations, authorities in most European countries, Australia and Canada built barricades to hinder Nice-style attacks. The simple attack produced a massive scale of effect. The small size of the attack produced a large number of casualties and draw attention to at risk infrastructure and alerted security agencies across the globe to a new method of terrorism.

Quantitative stigmergic in digital media environments can be common social networking mechanisms seen on Facebook or Twitter as ‘likes’, ‘shares’, ‘retweets’ and on Telegram by the number of views. Part of ISIS’ IO objects are the effective engagement of digital content measures. The more shares, likes and retweet the more these stigmergic indicates help to create new audiences. For example, most European recruits may have affected by Mujatweets, which impacted on increase number of ISIS recruits from European countries. Some of those recruits migrated to ISIS land, and some carried out acts of terror or became ‘sleeper cell’ which may be activated at any time.
7.7.4 Qualitative

Environmental signals are varied and can change a message based on their combination. Robb (2004) suggested “Attacks on major networks such as airports or trains is qualitative as huge security response acted quickly to secure such networks from shutting down”.

Qualitative stigmeric signals of ISIS can be the planning for responding to messages disseminated through digital media to ISIS sympathisers to commit an act of terror in Western countries.

Stigmeric operations of ISIS networks can be observed through what Marsh and Onof calls the cybernetic loop of three aspects (Marsh & Onof, 2008, p. 7):

- Agents: collective of ISIS’ e-jihadists (media jihadists) and affiliates targeted digital media environments to generate, aggregate and disseminate information (will be discussed in section 7.7.5). “All that is necessary for stigmergy to occur is for the outcome of the behaviour of the relevant agent to be appropriately affected by previous environmental changes” (Holland & Melhuish, 1999, p. 174).

- Environment: the medium of communication ISIS agents utilised can be encrypted, secure or even open-source network. To understand how dynamic and rapid change of agents in adapting to new environments, Marsh and Onof (2008) suggested:

  Stigmergy distinctively relies on the cybernetic relationship of agent -- environment -- agent environment through ongoing and mutual modification or conditioning enabled by the rise of computing technologies (and the democratisation of technology), the possibilities and the scope of a stigmeric environment have exponentially increased—collaboration mediated and afforded by an environment—being the mark of stigmergy. (p. 7)
• Sign: used for communication as a collection of tails linked to ISIS content. This includes direct links to ISIS propaganda distributed across digital media environments. The rise of anonymous sharing portals has created unique sign for ISIS content as all uploaded content transformed and shared as pheromones tails that can be easily followed, duplicated and distributed across digital media environments.

Marsh and Onof argued that mutual process of modification and conditioning of the cybernetic loop of agent-environment-agent-environment are ongoing and being part of stigmergy, which dissolve tension between self-serving individual and the social corpuses through indirect interaction (Marsh & Onof, 2008, p. 14). The dynamic of stigmergic operation have helped ISIS to build robust networks of information sharing and participation.

7.8 Observe, Orient, Decide and Act Loop Effect on ISIS’ Networks

To examine what has been said, I shall summarise OODA loop, distributed swarming and stigmergic effects on ISIS networks. The following section seeks to explain how the utilisation of new digital information environments in the context of OODA loop can generate a networking centric warfare effect. This effect can be examined through observation of ISIS and its opponents’ OODA loops. Tracing of ISIS’ online activity can explain how swarming activity occurred and how the interaction between Jihadists and the online environments has shaped the organisational form of ISIS networks that enabled it to carry out IO and engage in NCW. From lenses of ANT, swarming activity of ISIS has changed the agency of the online environment. In other words, Justpaste.it, Telegram and Sendvid were created to share videos and files, the extensive use of these portals by terror organisations have changed its purpose and became hubs and tools that mediate terror
communication. Therefore, these portals became suspicious for ordinary usage and became a target for security agencies.

To understand the paradigm shift in ISIS’ IO strategy and the effect of utilising of digital information environments. This information environment according to the DOD (as cited in Prisco, 2012) “consists of three interrelated dimensions, which continuously interact with individuals, organisations, and systems. These dimensions are known as physical, informational, and cognitive” (see 4.2). The function of the physical dimension “is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organisations to create effects” (Prisco, 2012). While, the informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information (as cited in Prisco, 2012, pp. iv-iiiv).

To contextualise the role of information environments harnessed by ISIS from paradigm shift and information warfare perspectives it is important to understand the function and architecture of these environments. On the one hand, the rise of anonymous sharing platforms, cloud computing technologies and encrypted communication applications is twofold: a) ready template for immediate information upload and; b) Personal anonymity and security at the centre. In other words, new digital communication technologies enhance efficiency, security, and privacy of users (to some extent) and impact on information warfare. On the other hand, interaction, collaboration and convergence between digital entities (network actors) is critical. For example, generated content can be shared, duplicated, and retrieved across multiple digital platforms.
More bluntly, putting decision into action by transmitting from one digital environment to another is a key success of ISIS networks. The information swarm operation ISIS performed on multiple digital media environments disseminated a high volume of information and sped up the process of their OODA by shortening its cycle to Decide and Act (see Figure 119).

![Figure 119. Diagram explaining the observe, orient, decide and act loop effects on ISIS networks. Illustrated by the author.](image)

ISIS stigmergic swarming operations are helped through the creation of short information loops. These short loops assist the network to maintain itself through speed. In other words, the process of ‘Interaction and Isolation’ and ‘Whack a Mole’, adapted by ISIS adversaries based on centralised C2 operations was slower than ISIS digital operations. ISIS established distributed networks as it orients itself of what is happening in the information environment. For example, ISIS affiliates were encouraged to share propaganda videos and ISIS messages to all followers active on Telegram and Twitter.

Observing the existence of new environments fastened the decision-making process and adjusted the ISIS loop. Agility and speed of ISIS OODA advanced its operation inside opponents’ OODA. Agility and speed can be achieved through self-synchronisation of ISIS e-jihadists adapting swarming operations warfare achieved through stigmergic operations of ISIS collectives. Therefore, decentralised structure of ISIS networks sped up C2 over
multiple digital environments via distributed swarming operation. As Cebrowski & Garstka (1998) argued:

Speed of Command is the process by which a superior information position is turned into a competitive advantage. It is characterized by the decisive altering of initial conditions, the development of high rates of change, and locking in success while locking out alternative enemy strategies. It recognizes all elements of the operating situation as parts of a complex adaptive ecosystem and achieves profound effect through the impact of closely coupled events (P.6).

Within this context, ISIS have increasingly observed the continuous suspension of their accounts so that their OODA cycle have been shortened lapses between ‘Observe’ and ‘Act’. That is to say, the adaption of swarm operations helped ISIS to function effectively as swarmers shared information across multi-digital media environments with other affiliates. To analyse ISIS speed of command it is important to examine ISIS digital swarmers and how they operate. The swarming operation of ISIS networks, therefore, works as the following (see Figure 120).
As shown in Figure 120, ISIS agents conducting self-synchronized swarming operations include generators, aggregators and disseminators, each of which will be detailed in the following sections.

7.8.1 Generators

There are two types of information generators with ISIS IO, the first are active agents who are active combatants witnessing live the actions of ISIS on-the-ground operations. The second type of generators are ISIS affiliates who gather videos and photos and information shared by active combatants for propaganda purposes. An example of the second type of information generators are Asawrty and Shami witnesses on Twitter. Another example exists on the Telegram platform, where Nashir news and the Dabiq and Amaq channels were established as information generators of the second type that aggregate and disseminate digital information (see Figure 121).
7.8.2 Aggregators

The category of aggregators (see Figure 122) includes active combatants and e-jihadists who respond to calls of ISIS spokesman, such as Abu Muhammed Al-Adnani who claimed that fighting in the media is more important than fighting in physical war. The role of aggregators is focused on collecting necessary data to be included in propaganda war. Fundamentally, the aggregators role is mapping and collecting data regarding distributed content over digital media environments. The collected data is a twofold manner. First, the data is collected for future retrieval and redistribution, and second, the data is then used for propaganda purposes. Aggregators played pivotal roles in sustaining ISIS’ propaganda operations and keeping collected data safe to recycle when needed. ISIS aggregators can be observed via Telegram channels, where information collected from multiple sources to keep Telegram channels active (see Figure 122).
7.8.3 Disseminators

Digital disseminators are non-physical combatants. ISIS disseminators formed a digital army of ISIS contributors keeping ISIS propaganda moving across media networks. Disseminators are self-synchronized and operate via swarms. ISIS disseminators concentrated their activity in finding and establishing channels of information diffusion (see Figure 123). The adaption of anonymous media networks, cloud computing and encryption application is the ‘stigmergy’ of disseminators to maintain networking and communication structure of ISIS networks.

Figure 123. Example of information disseminator on Telegram channel.
The collaboration of ISIS agents through processes of information\(^{117}\) aggregation, generation and dissemination, self-synchronisation and swarming operations has formed its network-centric structure. As Arquilla & Ronfeldt (2000) argued, “swarming is crucially important because swarm forces depend upon uninterrupted flows of information to actualize their potential” (P.67). That is, synchronisation of information of ISIS e-jihadists using swarming operations have infiltrated most of media environments with information, has been decisive factor in high speed manoeuvring its adversaries.

To this end, this is “Open Source warfare” (Robb, 2007, p. 116). As John Robb (2007) asserts, “terrorism and guerrilla warfare are rapidly evolving to allow non-state networks to challenge the structure and order of nation (P.175). That is, internet technologies enabled terror organisations to network, facilitate direct/indirect coordination launch swarm operation which pose a great challenge to nation-states.

### 7.9 Conclusion

This chapter has investigated the information-centric warfare that occurred between ISIS and its adversaries in the information environment. I extensively examined the swarming operations of both sides of the conflict using the OODA feedback loop model of manoeuvre warfare to better understand the dynamic of information-centric warfare. To overcome dispersed forces and massive geographical space ISIS relied on, digital media networks,

\(^{117}\) This thesis adopts a broad definition of ‘information’. Information is defined as something that refers not only to communications media and the messages transmitted, but also to the increasingly material. ‘information content’ of all things, including weapons and other sorts of systems (Arquilla & Ronfeldt, 2000, p. 2).
which offered unique, secure and free communication to coordinate attacks and achieve IO objectives. ISIS adversaries opted to use account blocking and content suppression strategies to defeat ISIS and hinder its propaganda machines used for recruiting jihadi, fundraising and carry out lethal attacks (i.e. lone wolf). At first glance, ISIS adversaries successfully suppressed ISIS e-jihadists, removing them from popular SMNs especially on Twitter, and YouTube. Meanwhile, the rise of anonymous and cloud computing communication technologies enabled ISIS to shift its activity to newly formed applications, including Telegram, Justpaste and Sendvid. Moreover, this new digital media environment offered anonymity, and security to ISIS e-jihadists, which increased the number of digital swarmers across the globe. In other words, the OODA loop cycle of ISIS IO was faster compared to its adversaries. Therefore, maintain flows of information of ISIS through swarm operation was quite successful.

To understand information warfare occurred and how ISIS managed to maintain information loops during degrading operation from lenses of ANT is that, ISIS managed to establish heterogeneous networks that enables it to enrol and translate more network actors to its networks. The use of anonymous sharing portals, encryption applications, digital media platforms and other digital media logistics as network actors have leveraged its networks and helped it to carry out stigmergic operations without direct coordination between network agents. With that being said, the speed of information processes and disseminations enables ISIS to operate inside the OODA of its opponents.

To this end, the detailed analyses of centric information warfare occurred between ISIS and its adversaries, I conclude that ISIS managed to operate inside the OODA loop of its adversaries. That is, the decision-making cycle of ISIS e-jihadists OODA was faster
compared to its adversaries. In doing so, swarming of multiple digital media environments of ISIS e-jihadists was greater than operation degrading ISIS digital capabilities. As collectives of e-jihadist depended on secure, robust, networked, encrypted communication has prevailed in the battle of information environment. In other words, disrupting IO of ISIS by suspending accounts was inadequate to win the battle of information environment.
Conclusion

As of writing the concluding chapter of this thesis, two stigmergic operations occurred. The first was the Paris attack that occurred on the 13th of May 2018, and the second was the capture of five top ISIS leaders in Syria on the 10th of May 2018. To understand these two incidents from a stigmergic perspective is to consider that the Paris attacker left information signs. In this case, the attacker posted a video to the internet expressing his intention to carry out an attack on behalf of ISIS. On the surface, the attack appears as a ‘lone wolf’ operation, but the attacker was simultaneously operating as a node in a swarm who adapted to the digital media network norm without being part of a physical terrorist network. The case of the captured ISIS leaders was an example of the dynamic of quantitative stigmergy. That is because the architecture of the Telegram enabled networking between the digital environment and other network actors. The information feedback between the digital environment and actors has led to suppress these loose swarms which lead to their capture. In other words, understanding the signal and reacting to it as an emergent communication has led to the capture of ISIS leaders.

However, for terror networks, the message does matter; for anti-terror powers, it's essential to counter terror messages before it gets attention. The battle in the 21st century is over the control of information. Using a mixed-method approach, this thesis sets out to answer the main research question: What was the role of ISIS digital media logistics in resisting attempts to degrade its IO objectives between 2014 and 2016? In addition, secondary questions of: Did ISIS' three communication strategies of weaponisation, stigmergy, and manoeuvring create a paradigm shift enabling it to counter attempts to degrade it propaganda and recruitment
networks? And, were the counter strategies of degrading operation has been successful to obliterate ISIS' IO objectives?

To answer the main question, (see chapters 3, 4 and 6) using screenshots and ANT, the thesis traced ISIS’ digital media logistics and examined ISIS’ dynamics of message assemblages, and processes of information aggregation and dissemination to understand: the role of digital media logistics in the restructuring of ISIS networks, sustain flows of information, create dynamic loop of information, and enhance the production of propaganda content. Tracing of ISIS’ digital media logistics also explains how ISIS succeeded to mobilise jihadists (both e-jihadi and active combatants) who played a critical role in leverage of ISIS networks and help to achieve its IO objectives.

To understand the paradigm shift in ISIS' communication strategy, this thesis has explored ISIS' IO and counter-narrative responses from an information warfare perspective. This study has examined ISIS' digital media logistics as toolkits of its IO strategy (see section 4.2). It has explored the ways that ISIS generates and disseminates its messages to achieve its political agenda (see section 3.6).

In this thesis, ANT was used as theory and methodology to understand the role of network actors in establishing terror networks (see section 4.15 and 6.5). This theory suggested that the change of agency of network actors can change a network's dynamics and purpose of use. ANT is used to explain how social media was developed as a tool to facilitate communication between human actors; however, it soon became a tool for the spread of fear and recruitment. That is, the agency of these platforms changed when the purpose of their use change. Therefore, stigmergic swarming terminology defined the role of network actors—humans and
non-human—in message assemblages and flows of information. In other words, this thesis showed how decentralised messages are generated and disseminated with or without being intentionally mediated, in which this thesis refers to as stigmergic operations of ISIS networks (see section 7.7). For example, bots and applications have been designed for self-automation of information dissemination which sustains information flows. As Fisher (2015) noted that "this type of behaviour is evidenced by the ability of Jihadist groups to continue to disseminate content in the face of concerted efforts by Western governments and social media platforms to disrupt their channels of communication" (Fisher, 2015, p. 5).

This thesis identified three main challenges involved in countering the ISIS narrative, information loop and the logistics of message assemblages (see chapter 5), that are: the weaponisation of multiple information environments, stigmergic swarming, and information warfare. To examine the counter strategy operation of ISIS adversaries that aims to answer the second question, this thesis identified three phases of countering ISIS' IO objectives: disruption of information flows, countering its narrative and open hacking operations. Using screenshots methodology, this thesis comprehensively identified methods that were used to attack ISIS' digital media logistics and counter its narrative. It highlighted how ISIS' adversaries have established a holistic approach to address ISIS' leveraging of its networks via social media platforms (see section 5.2). By investigating the counter-strategies used by ISIS' adversaries, this thesis identified three ways to combat the upsurge of ISIS online content: account suspensions and hacking operations. This thesis also highlighted the important strategies used to degrade the digital capacity of ISIS, that include: whack a mole and interaction and isolation operations.
To answer the third research question, this thesis has highlighted ISIS’ IO operation strategy in the weaponisation of information media environments, stigmergic swarming operations, and manoeuvre information warfare strategies to evade degrading operation. This thesis has argued that attacking the digital media logistics of ISIS networks in the period between 2014 and 2016 was unsuccessful, as ISIS adapted stigmergic swarming operation of information environments. In other words, a paradigm shift in terror communication occurred, through which ISIS maintained its existence in information environments, the speed of message dissemination and sophistication of message assemblage. This logistical operation allowed ISIS to maintain its network structure, despite its adversaries attempts to dismantle or disrupt it. As Rose (2014) stated,

Now, in the age of YouTube, Twitter, smartphones, cheap cameras, and software, the superpowers no longer control information. Ironically, the beneficiaries of this media democratisation are a medieval theocracy hell-bent on eradicating democracy from the face of the earth.

Through this thesis has become increasingly clear that information logistics are essential for the generation and dissemination of messages of terror and that ISIS effectively harnessed this strategy, while its adversaries responded and reacted, attempting to keep pace.

To understand how information warfare occurred between ISIS and its adversaries, this thesis examined three case studies to show how ISIS weaponised social media platforms and outmanoeuvred its adversaries in the information environments (see sections 6.2, 6.9 and 7.2). ISIS’ digital activity was traced through its favourite microblogging platform (i.e., Twitter), anonymous sharing portals (i.e., JustPaste.it, sendvid.com, dump.to) and encrypted communication channel (i.e., Telegram).
To contextualise the information warfare that occurred in the digital sphere, this thesis used and expanded on Boyd's OODA loop manoeuvre warfare model (see section 7.3). This approach revealed that the speed of command, resilience and swarming operations gave ISIS superiority over its adversaries in the information environment. This study indicated that IO and information warfare are both military actions, which seek to gain information superiority over an adversary. For this purpose, this thesis referred to the concept of auftragstaktik (mission-based tactics). As used in this thesis, the OODA loop is useful in understanding asymmetrical (i.e., uneven) digital warfare, wherein the fighting entities are not equal in terms of military capacity. This thesis revealed that guerrillas strategically harnessed multiple information environments to outmanoeuvre their adversaries, by operating inside the information loop of their adversary. Further, this thesis has explored that the weaponisation of information environments helped ISIS to carry out auftragstaktik operations.

This thesis demonstrated the fluidity and agility of information sharing portals that are free, easy to access and encrypted. They have galvanised the message and communication of ISIS. These portals have also enabled ISIS to become more sophisticated and organised, which is evident by the productions that exploit the features of the horror genre. Digital media technologies have been used to shape a new genre of horror production and as such, the organisational structures of terror groups, such as ISIS, have become more sophisticated.

ISIS' intention was to threaten the security of Western nations and other coalition forces who had joined forces against ISIS in Syria and Iraq. As such, it is important to study and understand the proliferation of information, made possible by the widespread usage of anonymous sharing portals and encryption applications. These portals and applications
became domains for secure, convenient and free-access communication for terror organisations. This thesis contributes to understanding the cybersecurity threat posed by ISIS and other emergent terror networks. It demonstrated how Twitter and anonymous portals helped ISIS establish dynamic information and content loops. Encrypted communication applications facilitated secure communication between potential recruits to support the physical attacks. These messages exploited the terror genre, spreading effectively to potential jihadists and inspiring individuals to carry out attacks outside the Islamic Caliphate.

To highlight aspects of information warfare that occurred between Islamic terror organisations and their adversaries before the rise of ISIS, this thesis focused on case studies of three terror organisations and examined the ways they harnessed social media and satellite channels to gain superiority over their adversaries in the information environments (see section 1.6, 1.10 and 1.15). Hamas, al-Qaeda, and Hezbollah have depended on information as a weapon in the face of well-equipped adversaries. The asymmetrical warfare carried out against these organisations (especially Hamas and Hezbollah) affected their media production techniques, which they used to gain sympathy and support from the international community. Meanwhile, Al-Qaeda's IO aimed to spread fear through the production of sophisticated propaganda videos. However, the advancement of internet and mobile phone technologies allowed ISIS to build decentralised and distributed networks by using these technologies for their new C2 operation centres.

This thesis also demonstrated the lessons learned from the digital activism during the Arab Spring uprisings and its role in shaping new waves of terror in Syria and Iraq. Further, this thesis examined the role of social media platforms in political polarisation, the bifurcation of political powers and the impacts of these on future networks. This thesis extensively
examined the Arab Spring uprisings from a networking perspective and explained how the uprisings changed the dynamic of network tendencies (see sections 2.3 and 2.8).

Additionally, the study of the Arab Spring uprising was addressed from an information warfare perspective, such as the Egyptian Government's internet connection shutdown and the role of the Syrian Government in tracking activists, misinformation, deception, and propaganda.

Two of the most important outcomes of this research was the documentation of ISIS' IO (see sections 3.5 and 4.8) and the countermeasures that were carried out by ISIS' adversaries (see sections 5.3 and 5.4). The effective use of auxiliary sharing portals—which maintained communication, flows of information and PSYOP—by Hamas, Hezbollah, Al-Qaeda, and ISIS, through which open source information environments were used for the spreading of fear and propaganda is what Clausewitz (1832) theorised as a "continuation of a war by other means".

An interesting finding of this research was that the collaboration of networks of ISIS' adversaries have played a role in promoting ISIS' terror narratives and directing its messages. The symbiotic relationship between the media and terror is evident in the media's coverage of terrorism, which unintentionally advertises terror organisations' messages and incites more terrorism, which then produces more media coverage. Stern and Modi (2010) argued that successful terror organisations "respond to changes in their environments by changing their mission and changing their shape" (Stern & Modi, 2010, p. 282). As Farwell (Farwell, 2010) argued, "This means filling the media space, from the ground up, because every moment of attention that one's narrative attracts means less attention for that of one's adversaries".
Although this thesis addressed ISIS’ IO and its adversaries' counter-narrative strategies, it was beyond the scope of this study to address processes of recruitment and radicalisation, which are the main concerns of governments and counterterrorism agencies. This thesis highlighted the role of PSYOP as part of ISIS' IO strategy to recruit potential jihadists. However, the objectives that underpin radicalisation, such as recruitment to violent extremism, is beyond the scope of this thesis, a study of these processes need to be studied on a case-by-case basis. That is, every individual has a different motive or psychological explanation for their decision to join ISIS or other violent extremist groups.

It was beyond the scope of this thesis to address the geopolitical polarisation and influences of international and local powers in the complex warfare between guerrilla groups, such as sectarian struggles, and ideological, political or economic interests. In addition, it was beyond the scope of this study to explore the fight over hegemony and control of resources, which has also affected information warfare in digital media. Further research must investigate Russian, the US, Turkish, Iranian and Israeli direct and indirect involvement in the logistical supply of militant group who are operating inside Syria and Iraq to understand how this involvement has shaped information warfare. It is necessary to investigate the ideological struggle between the Sunni insurgent groups, such as Al-Nusra (Hayat Tahrir Al-Sham) versus ISIS and Jabhat Fateh Al-Sham versus Al-Nusra, to understand the complexity of the geopolitical spheres among clandestine organisations that share the same ideology and enemy. The role played by Israel in supporting ISIS by attacking the Syrian army needs to be studied further. Similarly, this thesis did not address the symbiotic relationship between mainstream media and widespread terror messages and how this affects radicalisation. This would be an interesting area for future research. To some extent, this thesis outlined this issue
briefly in its discussion of ISIS' message assemblages and speed with which these messages were mediated within ISIS' information warfare.

As this research extensively examined the phases of the degrading operation—particularly hacktivism—against ISIS, it briefly described the role of the UCC in hacking and spreading misinformation against its adversaries. UCC hackers did not wage large-scale operations; however, they were part of swarming activity to maintain flows by keeping information loops across multiple information environments. There is the possibility for future research to be conducted in this area.

Another important aspect of ISIS' IO, the role of women jihadi and children (Cubs of the Caliphate), was not discussed in this thesis. Although women and children were an integral part of ISIS' IO strategy, this thesis treated all human actors equally, without mentioning the gender of jihadists. However, future research could investigate the specific targeting of women and children by ISIS' IO strategy.

Although important elements were highlighted in this research, the study of the overall media logistics of ISIS' networks addressed in this thesis could be expanded upon. For example, it was beyond the scope of this thesis role of Facebook, YouTube, Daily Motion, archive.org, Pinterest, and Kik; they have only been discussed briefly. Other information logistics—such as the use of TOR, VPN, Photoshop software, memes and digital graphics—that have been widely used by ISIS were not examined in this thesis.

This thesis explained how ISIS carried out its comprehensive swarming operation of digital information environments to establish global networks of affiliates around the world,
strengthen the Islamic Caliphate with more recruits, and leverage its network and financial aid. ISIS has created a virtually leaderless organisational structure, which encouraged the recruiting of more online jihadi, who contributed to the maintenance of ISIS' network structure. It also demonstrated how the open-source information environments have globalised and leveraged ISIS networks by creating alliances with other Islamic terror networks, such as Boko Haram, Al-Shabab, the Taliban, and Lashkar-e-Taiba. With these networks in place, individuals were mobilised. Active jihadists travelled to the land of ISIS, others acted on behalf of ISIS in their countries and others chose to become digital jihadists.

When examining ISIS' or other terror organisations' use of digital media logistics, it must be considered that within the dynamic world of the internet, things are unpredictable. As such, so are the terror organisations that rely on them. Many years ago, scholars spoke of the existence of a virtual caliphate. Between 2013 and 2016, it became reality. Despite the fall of ISIS' capital cities in both Syria and Iraq in 2017, its online presence remains. ISIS' continuous online activities suggest the rebirth of a virtual caliphate is inevitable. The impact and influence of such a network will make the task of effectively countering ISIS an immense task. For this reason, research—such as the study represented in this thesis—is imperative to inform governmental and other actors in waging effective countermeasures. Some of the most effective countermeasures of ISIS, both online or on the ground, is that ISIS adversaries built a decentralised structure of command and control operations. The influx of anti-ISIS fighters, particularly from the Shia sect who arrived in Syria and Iraq from Iran, Lebanon, Afghanistan, and Pakistan, have established a new dynamic of guerrilla vs guerrilla warfare. This new form of warfare was successful to conquer ISIS and crumble the caliphate. Likewise, in the information domain, the successful operations carried out by anti-ISIS hackers established a decentralised form of information warfare in the information domains.
The collaboration between government security agencies and hacker collectives have paralysed ISIS’ communication strategy and its internet activities at the same time it helped in making of ISIS’ operation visible on social media. That is, the flagging of content or reporting of ISIS’ accounts on Twitter make the content and ISIS accounts visible. For example, I have tracked ISIS accounts and located their propaganda content simply by monitoring the activity of ‘CtrlSec’ on Twitter.

This collaboration is considered a possible countermeasure strategy in terms of understanding the trade-offs. Dealing with ISIS online activities also resulted in confusion and lack of counter strategy taken by platform administrators. Social media administrators mobilised thousands of its employees and collaborated with hacker groups such as ‘CtrlSec’ to flag content and suspending accounts of ISIS members. This strategy created confusion in the system as thousands of accounts were suspended by mistake, including mine. As an ISIS scholar, I am unable to retain my suspended YouTube account. False flagging has also affected some media channels such as ‘Al Jazeera’ and other thousands of accounts who are tweeting in the Arabic Language.

This thesis shows an important lesson that can be understood from combating ISIS, or any type of terror organisation or guerrillas on the ground or in the information domains; that the network structure is a crucial factor of winning or losing battles. In other words, in combating terrorism, an auftragstaktik operations must be carried out by governments and security agencies which is structured as a form of decentralised vs decentralised networks.

To this end, this thesis contributed to an understanding of organisational dynamics, by examining sharing portals that, despite their communication benefits, have a dark side.
Research into these sharing portals is necessary due to the rise in usage of these portals by violent groups, such as the white supremacist and alt-right. Their online activity has increased and overshadowed ISIS and Al-Qaeda to some extent.
References


Al-Rawi, A. (2014). Framing the online women’s movements in the Arab world. Information, communication & society, 17(9), 1147-1161.


Arthur, C. (23/6/2014). Taking down Isis material from Twitter or YouTube not as clear cut as it seems, *The guardian*. Retrieved from:

http://www.theguardian.com/world/2014/jun/23/taking-down-isis-youtube-twitter-google-video


BBC. (2012). Israel and Hamas wage Twitter war over Gaza conflict, *BBC*. Retrieved from:


Electronic Frontier Foundation. (2012). Report. from:
http://www.eff.org/deeplinks/2012/03/fake-youtubesite-targets-syrian-activists-malware.


Garcia, V. (2016, 08/05). At the heart of Ansar at tawhid, the "jihad channel" of Telegram and Kermiche, *Lexpress*. Retrieved from:

http://www.lexpress.fr/actualite/societe/ansar-at-tawhid-le-canal-djihad-de-telegram-et-de-kermiche_1818983.html


Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., & Maziad, M. (2011). Opening closed regimes: what was the role of social media during the Arab Spring?


January/February.

http://www.jpost.com/Middle-East/Facebooks-counterterrorism-expert-divulges-companys-anti-extremism-methods-504782


Olson, P. (2013). We are Anonymous: Random House.


376

Saber, D., & Webber, N. (2017). ‘This is our Call of Duty’: hegemony, history and resistant videogames in the Middle East. Media, Culture & Society, 39(1), 77-93.


