CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Mapping the production of knowledge of cyberterrorism and hacktivism research using an integrated bibliometric and content analysis framework
Authors	Hosford, Kevin
Publication date	2024
Original Citation	Hosford, K. 2024. Mapping the production of knowledge of cyberterrorism and hacktivism research using an integrated bibliometric and content analysis framework. PhD Thesis, University College Cork.
Type of publication	Doctoral thesis
Rights	© 2024, Kevin Hosford. - https://creativecommons.org/licenses/by-nc/4.0/
Download date	2026-11-14 16:24:57
Item downloaded from	https://hdl.handle.net/10468/16378



UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Ollscoil na hÉireann, Corcaigh
National University of Ireland, Cork



ucc
Coláiste na hOllscoile Corcaigh, Éire
University College Cork, Ireland

Mapping the Production of Knowledge of Cyberterrorism and Hacktivism Research Using an Integrated Bibliometric and Content Analysis Framework

Thesis Presented by

Kevin Hosford

ORCID: 0000-0002-5883-6906

Student Number: 114740981

For the Degree of

Doctor of Philosophy

Supervisors: Dr. James Windle and Dr. Orla Lynch

Department of Sociology and Criminology

Head of Department: Dr. Tom Boland

Submission Date: January 5th, 2024

Declaration of Originality

I hereby declare that the work in this research report titled 'Mapping the Production of Knowledge of Cyberterrorism and Hacktivism Research Using an Integrated Bibliometric and Content Analysis Framework' submitted to the Department of Sociology and Criminology at University College Cork as partial fulfilment of the requirements for the Degree of Doctor of Philosophy in Criminology is entirely my own work. Throughout this piece, work that is not my own is correctly referenced and is explicitly acknowledged.

By signing below, I confirm this originality and hereby certify that this is a true copy of my research.

Signature  Date: 05/01/2024

Acknowledgement

This thesis is dedicated to my late father, Michael, who taught me how to build homes, so that I'll always have a place to call my own. I also extend my dedication to my mother, Margaret, who instilled in me the importance of caring for others, so that the homes I build will never be without warmth and companionship.

To my sister Vanessa, thank you for being there to listen, and for keeping my spirit high during the difficult times we shared. To my cat Kib, for all the nights you've randomly woken me up from sleep, wanting to cuddle for affection. I may not have shown it then, but I appreciate the companionship.

I also wish to acknowledge my supervisors Dr James Windle, and Dr Orla Lynch who have supported me throughout periods of confusion, pain, and even a global pandemic, supporting both my PhD and me as a person with guidance, support, and their friendship. Never once have I felt excluded, and deeply appreciate the trust and opportunities you both have given me.

Lastly, I would like to thank both the Department of Sociology and Criminology for giving me the space, resources, and tea to pursue this PhD, and University College Corks IT Department who have educated me so much on technology throughout my four years working with colleagues, and even entrusting me with keys to every room on campus for a long time. If I was ever to be an Inside-hacker, then would have been the best time!

Glossary of Terms

This glossary supports the reader's understanding of certain terms used in the work. The author acknowledges that some terms are still debated academically. The glossary aims to clarify the intended meanings of these terms within the context of the thesis.

Bibliometric Analysis: The quantitative analysis of academic literature to map the scholarly output and research trends within a specific domain.

Content Analysis: A research method used for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns.

Ideologically Motivated Cyber-Events: Cyber activities driven by ideological beliefs, including but not limited to political, religious, or social motivations, aiming to achieve specific goals through digital means.

Information Communication Technologies (ICT): An umbrella term that includes communication devices such as smartphones, computer and network hardware and software, satellite systems, and so on, as well as the numerous services and applications associated with them, such as videoconferencing, messaging, and commercial/industrial services.

Knowledge Mapping: The process of creating a visual representation of knowledge within a particular domain, highlighting the relationships between different concepts, topics, or entities.

Ontological Framework: A structured representation of the concepts within a domain and the relationships between those concepts used to reason about the objects within that domain.

Paradigms: Based on the work of Thomas Kuhn, and used to describe the framework of theories, methods, and standards that define productive scientific research within a particular field for a specific period.

Scientometrics: The study of measuring and analysing science, technology, and innovation. Major research issues include the measurement of impact, reference sets of articles to investigate the impact of journals and institutions, understanding of scientific citations, mapping scientific fields, and the production of indicators for use in further research, policy and management contexts.

Taxonomy: A structured framework used to categorise and classify various elements within textual or media content, enabling a systematic analysis of its features and meanings.

Triangulation Design: Data Transformation Model: A research approach that involves the use of multiple data sources and methodologies to cross-validate and strengthen research findings.

Abstract

The proliferation of Internet Communication Technologies (ICT) has prompted scholarly interest in role of ICT in facilitating cybercrime, particularly in the domains of cyberterrorism and hacktivism. Exploration of cyberterrorism and hacktivism has faced challenges stemming from the absence of dedicated platforms, such as academic journals and conferences impeding a consistent research output and hindering collaborative research. In contrast to more established domains like terrorism studies and organised crime studies, the research on cyberterrorism and hacktivism is still in its initial stages within the academic discourse.

This doctoral thesis seeks to map the conceptual understandings and production of knowledge surrounding cyberterrorism and hacktivism research throughout a twenty-year period (2000-2020). Employing a modified version of Creswell and Clark's 'Triangulation Design: Data Transformation Model,' the research employs bibliometric analysis for a knowledge mapping of the academic domain. Additionally, a quantitative content analysis of definitions pertaining to cyberterrorism and hacktivism sheds light on key issues within the scientific domain.

The investigation reveals a dominance of male, single-author publications, primarily originating from the global north, suggesting a potential lack of collaborative trans-national research amongst a backdrop of an array of multi-disciplined parties. The absence of consistent high-impact journal contributions, lack of knowledge cohesion,

coupled with an over-reliance towards secondary sources, further hinders the rich and dynamic collection of researchers from achieving a cohesive academic discourse leading to the issue of knowledge fragmentation within academia fields. The analysis of definitions exposes cyberterrorism as predominantly hypothesised, emphasising unspecified actors and potential harms, diverging from conventional notions of terrorism as a spectacle. In contrast, hacktivism is characterised by more group-oriented definitions, rooted in specific events, their injustices, and associated hacktivist campaigns.

Recognizing the distinct ideological motivations behind both cyberterrorism and hacktivism, this thesis concludes by proposing an ontological framework in effort to decentralise the dependency towards specific research definitions. This framework aims to facilitate the collection and dissemination of event details related to these phenomena, fostering more extensive and collaborative research efforts in this evolving field.

Table of Contents

Glossary of Terms 3
Abstract 6
Chapter 1. Introduction 15
1.1 Background and Context 15
1.2 Overview of Research Project 23
1.2.1 Research Objectives and Rationale 25
1.3 Methodological Approach 28
1.3.1 Scientometrics via Bibliometric Analysis 29
1.3.2 Content Analysis 30
1.4 Contribution of Study: 32
1.5 Thesis Structure 35
1.5.1 Chapter Outline 35
Chapter 2. Understanding The Cycle of Scientific Revolutions: The Role of Bibliometrics within Criminological Research 39
2.1 Introduction 39
2.2 Scientific Development and Paradigm Shifts 40
2.2.1 Normal Science 41
2.2.2 Paradigm Shifts 42
2.2.3 Critiques of Kuhn's Structure of Scientific Revolutions 43
2.3 The Adoption of Scientometrics as an Evaluative Framework 45
2.3.1 The Role of Bibliometrics in Criminology 48
2.3.2 Network-Oriented Bibliometrics in Criminology 52
2.3.3 Conceptual 'Knowledge' Mapping within Criminology 54
2.4 Conclusion 57
Chapter 3. Introduction to Cybercrime and Ideological Hacking 59
3.1 Introduction 59
3.2 A Brief Overview of Cybercrime 61
3.3 The Emergence of Hackers and Cyber-Deviance 70
3.3.2 Hacking as Subcultures 72
3.4 Ideologically Motivated Disruptive Hacking 78
3.4.1 The Emergence and Definition of Hacktivism 82
3.4.1.1 Hacktivism as Digital Activism 91
3.4.1.2 Hacktivism as a Skilled Practice 96

3.4.2 The Emergence and Definition of Cyberterrorism 100
3.4.2.1 Conceptual Criticisms of Cyberterrorism 107
3.4.2.2 Rethinking Cyberterrorism 108
3.4.2.2.1 Cyber-enabled Terrorism 115
3.4.2.2.2 Cyber-Dependent Terrorism (Cyberterrorism) 123
3.5 Conclusion 135
Chapter 4. Methodology 139
4.1 Introduction 139
4.1.1 Research Design and Methodological Justification 142
4.2 Pre-Phase Data Collection 145
4.2.1 Literature Discovery by Academic Search Engines 148
4.2.1.1 Database Selection 150
4.2.2 Literature Discovery by Academic Publishers 153
4.2.2.1 Refining the Search via Filtering 155
4.2.3 Identifying and Removing Duplicates 156
4.2.3.1 Merging the Collected Datasets 157
4.2.4 Data Screening 158
4.2.4.1 Defining High Impact Articles 159
4.3 Bibliometric Analysis 162
4.3.1 Knowledge Mapping Framework 163
4.3.1.1 Performance Analysis via Bibliometrics 165
4.3.1.2 Science Mapping via Bibliometrics 166
4.3.2 Analysis of Bibliographic Data 168
4.4 Taxonomic Content Analysis 171
4.4.1 Quantitative (Basic) Content Analysis 172
4.4.2 Content Analysis and Epistemological Positioning 175
4.4.2.1 Validation and Reliability within Quantitative Content Analysis 176
4.4.4 Taxonomic Framework 178
4.4.5 Analysis of Collected Definitions 180
4.4.5.1 Data Preparation 181
4.4.5.2 Building the Taxonomy 183
4.5.4.3 Coding 187
4.5 Methodological Limitations 190
4.5.1 Peer Review Journal Articles 191

4.5.2 Citations as a Measurement of Impact 192
4.5.3 Content Analysis of Academic Definitions 194
Chapter 5. Findings 196
5.1 Introduction 196
5.2 Part One: Bibliometric Findings 197
5.2.1: Basic Analysis 197
5.2.2 Citation Analysis 226
5.2.3 Summary of Bibliometric Findings 249
5.3 Part Two: Quantitative Content Analysis of Definitions 253
5.3.1 Overview of Analysis 255
5.3.2 Comparison of Distribution by Definitions 263
5.3.3 Synthesising the Taxonomy 301
5.3.4 Summary of Quantitative Content Analysis 304
Chapter 6. Discussion 306
6.1 Introduction and Project Aims 306
6.1.1 Key Findings and Contribution 307
6.1.2 Outline of Discussion 310
6.2 A Bibliometric Analysis of Cyberterrorism and Hacktivism Research. 311
6.2.1 A Domain of Stagnation or Fragmentation? 312
6.2.2 Knowledge Dispersion and Consistency 316
6.3 Identifying Distinctions Using Taxonomic Mapping of Cyberterrorism and Hacktivism Definitions: 324
6.3.1 Lack of Actor Specificity 326
6.3.2 Violence versus Non-Violence 330
6.3.3 Conflicting Intentions and Spectacle 332
6.3.4 The Means and Practicality of Cyberterrorism and Hacktivism 335
6.3.5 The role of Ideology and Motivation in Cyberterrorism and Hacktivism Research.. 338
6.3.6 Targets and Security Narratives of Cyberterrorism and Hacktivism Research 342
6.4 Strengths and Limitations 347
6.5 Conclusion 349
Chapter 7. A Conceptual Ontology for Ideologically Motivated Disruptive Cyber-Events 354
7.1 Introduction 354
7.2 Background to Ontologies 356
7.3 Developing the Ontology 359
7.3.1 Design Science Research Methodology 361

7.3.2 From Taxonomy to Ontology 365
7.3.3 Developing the Ontology in Protégé 373
7.4 Evaluation of the Ontology 380
7.5 Conclusion 385
Chapter 8. Conclusion 387
8.1 Introduction 387
8.2 The Health of Cyberterrorism and Hacktivism Research 389
8.3 The Conceptual Comparison of Cyberterrorism and Hacktivism 393
8.4 Moving the Needle Forward Towards More Cohesive Research 395
8.4.1 Future Directions 397
References 400
Appendix 458

List of Tables

Table 3.1 Typology of Cybercrime Groups (Choo, 2008)..... 128
Table 3.2 Key Classifications of Cyberterrorism 133
Table 4.1 Academic Search Engine Results 149
Table 4.2 Academic Search Engine Comparison 152
Table 4.3 Academic Publisher Comparison..... 154
Table 4.4 Total Results Articles with “cyberterrorism” & “hacktivism” keywords..... 155
Table 4.5 Manual Review Stages..... 159
Table 4.6 Modified Knowledge mapping framework..... 163
Table 4.7 Distribution of Collected Definitions 180
Table 4.8 Example of Definition Database..... 181
Table 4.9 Example Hacktivism Coding..... 189
Table 5.1 Ten Highest Cited Articles 219
Table 5.2 Core Researchers within the Collection of Articles..... 222
Table 5.3 Top Information Sources 232
Table 5.4 Top Cited Authors 239
Table 5.5 Distribution Count of Total Terms by Definition..... 257

List of Figures

Figure 3.1 Digital Activism Classification (George and Leidner, 2019) 91
Figure 3.2 Terrorist Activity Framework (Jangada Correia, 2022) 114
Figure 4.1 Single-Phase Triangulation Multilevel Research Design Structure 144
Figure 4.2 Dataset Consolidation Structure 157
Figure 4.3 Average Distribution of Google Scholar citation score by year 160
Figure 4.4 Orange Data Mining - Concordance View 171
Figure 4.5 Definition taxonomy (Al Mazari et al., 2015; Plotnek and Slay, 2021) 183
Figure 4.6 Merged Cyberterrorism Taxonomy Term Distribution 186
Figure 4.7 RQDA coding interface 188
Figure 4.8 Example Hacktivism Definition 190
Figure 5.1 Sample Article (n126) Distribution by Year 198
Figure 5.2 Distribution of Article Affiliation Organised by Country 201
Figure 5.3 Journal Distribution 202
Figure 5.4 Annual Distribution of Journal Output 203
Figure 5.5 Authorship by Country Affiliation 205
Figure 5.6 Distribution of Author Appearance by Continent 206
Figure 5.7 Distribution of Gender by Year 208
Figure 5.8 Distribution of Gender by Country Affiliation 209
Figure 5.9 Distribution of Gender by Author Position 211
Figure 5.10 Distribution of Discipline Groups by Author count 213
Figure 5.11 Distribution of Author Discipline by Gender 214
Figure 5.12 Citation Distribution per Year 218
Figure 5.13 Denning (2000a) citation distribution over time 220
Figure 5.14 Distribution of Author Contribution by Year 224
Figure 5.15 Group Clustering via Bibliographic Coupling 228
Figure 5.16 Co-citation of Article Sources 231
Figure 5.17 Co-citation of Cited Authors with a minimum of 5 appearances 236
Figure 5.18 Co-citation of Cited Authors with a minimum of 10 appearances 238
Figure 5.19 Cyberterrorism Term Distribution 255
Figure 5.20 Hacktivism Term Distribution 256
Figure 5.21 Distribution of Total Terms by Definition 258
Figure 5.22 Cyberterrorism Distribution of Classifications by Year 260
Figure 5.23 Hacktivism Distribution of Classifications by Year 261
Figure 5.24 Yearly Distribution of Actor Classification 264
Figure 5.25 Total Frequency Distribution of Coded Actor Terms 266
Figure 5.26 Actor Code Distribution by Year & Frequency 267
Figure 5.27 Network Distribution of Extracted Actor Terms 269
Figure 5.28 Yearly Distribution of Effect Classification 271

Figure 5.29 Total Frequency Distribution of Coded Effect Terms 272
Figure 5.30 Effect Code Distribution by Year & Frequency 274
Figure 5.31 Network Distribution of Extracted Effect Terms 276
Figure 5.32 Yearly Distribution of Intent Classification 277
Figure 5.33 Total Frequency Distribution of Coded Intent Terms 279
Figure 5.34 Intent Code Distribution by Year & Frequency 280
Figure 5.35 Network Distribution of Extracted Intent Terms 282
Figure 5.36 Yearly Distribution of Means Classification 283
Figure 5.37 Total Frequency Distribution of Coded Means Terms 284
Figure 5.38 Means Code Distribution by Year & Frequency 286
Figure 5.39 Network Distribution of Extracted Means Terms 288
Figure 5.40 Yearly Distribution of Motive Classification 289
Figure 5.41 Total Frequency Distribution of Coded Motive Terms 290
Figure 5.42 Motive Code Distribution by Year & Frequency 291
Figure 5.43 Network Distribution of Extracted Motive Terms 293
Figure 5.44 Yearly Distribution of Target Classification 294
Figure 5.45 Total Frequency Distribution of Coded Target Terms 296
Figure 5.46 Target Code Distribution by Year & Frequency 298
Figure 5.47 Network Distribution of Extracted Target Terms 300
Figure 5.48 Updated Merged Cyberterrorism Taxonomy Term Distribution 302
Figure 5.49 Overview of Hacktivism Taxonomy Term Distribution 303
Figure 7.1 Bottom-Up breakdown of Schema 366
Figure 7.2 Conceptual Ontological Model 369
Figure 7.3 Example of Protégé user interface 374
Figure 7.4 Example Class Structure 375
Figure 7.5 Example of Class Annotation 376
Figure 7.6 Example of Object Property Annotation 377
Figure 7.7 Example of Individual's Annotation 379
Figure 7.8 Offensive Event Perspective of HSE ransomware attack 381
Figure 7.9 Actor Perspective of Wizard Spider 381
Figure 7.10 General Perspective of Sony Pictures Hack 383

Chapter 1. Introduction

1.1 Background and Context

The increasing global use of the internet has given rise to academic interest in the use of ICT (Information Communication Technologies) for cybercrime (Brenner, 2002; Yar, 2005a; 2005b; Wall, 2001), including the areas of cyberterrorism and hacktivism (Denning, 2000; 2002a; 2002b). The internet, along with its associated technologies, offers opportunities for individuals and collectives to participate in various criminal behaviours. Over two decades ago, cyberterrorism and hacktivism were acknowledged as a significant and rising threat, as evidenced in the foundational scholarly works of Brenner (2002), Denning (2000a), Embar-Seddon (2002), and Pollitt (1998) raising concerns of the role ideological motivation towards the use of ICT to engage in various online transgressions.

Leveraging social and political ideologies for the motivation and cohesion of groups has historically been employed in driving political initiatives offline (Post, 1990). According to Holt and colleagues (2016; 2017:358), factors influencing participation in political actions can similarly apply to both offline and online activities. As emphasised by Malešević, “Ideologies appeal to moral norms, individual or collective interests, or superior knowledge to justify potential or actual social action” (2006:89). Consequently, individuals involved in activities classified as “cybercrimes” may not perceive their actions as such but rather as justifiable responses against opposing groups (Rid, 2013)

This thesis focuses on two such phenomena, cyberterrorism, and hacktivism. Within cyberterrorism research, potential incidents are frequently characterised as catastrophic occurrences, for example, breaches of air traffic control systems, disabling power stations, and triggering meltdowns in nuclear plants (Chen, 2014) with emphasis towards using digital technology and the internet to inflict physical harm or violently disrupt society (see Jarvis et al., 2016a; 2016b; Jarvis and Macdonald, 2015; Mayer Lux, 2018). The potential ramifications of a cyberterrorism event are far-reaching, encompassing substantial financial losses (Neagu and Savu, 2019) and physical harm and loss of life (Brenner, 2012), all within a similar lens often discussed within terrorism studies (Hoffman, 2006; 2017; Gaibulloev and Sandler, 2019; Windle et al., 2018). Nevertheless, the concept of cyberterrorism has faced substantial scrutiny (see Conway, 2011a, 2014a; 2014b), often criticised for its tendency to be nebulous, ambiguous, and lacking in precision with such events never truly materialising (Kenney, 2015:112). One significant point of contention is the broad application of the term. That is, it encompasses a wide spectrum of "cyber" activities that do not sufficiently distinguish themselves from other malicious cyber activities (see Akhgar et al., 2016; Jarvis and Macdonald, 2015; Mayer Lux, 2018; Plotnek and Slay, 2021).

Further, within academic research concerning cyberterrorism, there exists two conceptual frameworks. Firstly, those who view cyberterrorism as a distinct and unique phenomenon isolated within ICT. Often termed "pure cyberterrorism" (Gordon and Ford, 2002:637), this framework largely positions cyberterrorism as an independent act that uses ICT in which to target and disrupt cyber-based targets such as servers with little to no "physical"

impact or associated with kinetic “off-line” terrorism (Jarvis and Macdonald, 2015:55). Secondly, ‘cyber-enabled’ terrorism (Jangada Correia, 2022; McQuire and Dowling, 2013) sees cyberterrorism as an extension to terrorism in which terrorists use ICT to engage in planning and potentially expanding the effectiveness of physical acts of terrorism (Jangada Correia, 2022).

The second phenomenon of this thesis is hacktivism. Hacktivism is commonly described as a form of activism that employs hacking and other digital techniques to advance political or social objectives (Auty, 2004; Baldi et al., 2003; Di Salvo, 2017; Fuchs, 2009) often through non-violent means of disruption (Holt et al., 2017:2016). It is characterised as a type of social deviance that challenges the established order and aims to effect change by disrupting the prevailing status quo (Denning, 2000a; 2000b; 2000c). However, as hacktivism exists within a “genus” of other sophisticated cyber-malicious activities (Kenney, 2015), the phenomenon has frequently been conflated with cyberterrorism, often lacking details concerning the intent, or underlying motivation. This confusion and potential misapplication of both terms can hinder the progress of empirical research due to the resulting conceptual confusion. Hacktivists have directed their actions against various entities, including governments, corporations, and religious institutions. Their tactics have evolved over time and encompass distributed denial-of-service (DDoS) attacks, website defacements, and data breaches (Castells, 2014), of which are tactics commonly seen associated with cyberterrorism (see Addicott, 2007; Kerr, 2004) and various other cybercrime activities. The internet has played a pivotal role in facilitating the dissemination of propaganda and extremist ideologies, serving as a powerful

recruitment and radicalization tool for extremist groups (Awan, 2017; 2014), thus pushing concerns towards cyberterrorism and hacktivism as increasing threats.

Despite the growing body of academic research on cyberterrorism and hacktivism, a consensus on how to distinguish and define these topics remains elusive. Kenney (2015:112) has identified both cyberterrorism and hacktivism as sharing "a common category with other sophisticated malicious cyber activities such as cyberattacks, cyberwarfare, and online exploitation" consequently, overlaps are inevitable adding further ambiguity to both phenomena. Often distinctions between cyberterrorism and hacktivism become blurred due to both sharing similar intentions to cause disruption, and often adopt similar tools and techniques (Baldi et al., 2003:18, Yar and Steinmetz, 2017; 2019). This sharing of tools and techniques for virtual activities makes efforts to distinguish between cyberterrorism and hacktivism difficult, leading both too often to be conflated to one another (Baldi et al., 2003). This unintentional conflation tends to blur the boundaries of both concepts, potentially defining them as identical phenomena. Such inadvertent blurring has significant consequences for future research. As highlighted by Merton (1968:114), a considerable aspect of theoretical work involves clarifying concepts, which DiRenzo (1966) considers indispensable tools for scientific explanation, stressing that "precision in this fundamental area is imperative for the production of significant theory" (1966:3). Consequently, the unintentional blurring of these concepts makes achieving conceptual precision for either cyberterrorism or hacktivism challenging. Gerring (2012) argues that conceptual challenges hamper social science endeavours because, without the ability to clearly label a topic (whether cyberterrorism

or hacktivism), addressing even the most basic research questions becomes difficult, leading to the question, “What are we even talking about?” (Gerring, 2012:112).

As noted, the lack of agreement and ambiguity in understanding unique factors differentiating both phenomena potentially limits the production of new research and fostering of fresh perspectives. As a result, this thesis argues that academic progress in this area has been slow, with a predominant focus towards literature reviews over the past two decades, limited by cohesive understanding and primary data-driven empirical studies. This situation mirrors the state of pre-9/11 terrorism research which, earlier in its research cycle, grappled with a shortage of empirical studies from primary data (Silke, 2001), provided by only a handful of researchers and limited resources (Silke, 2008). For example, a notable earlier effort to understand growing terrorism in response to the events of 9/11 is Rapoport's (2003) concept of generational waves. In their study, Rapoport suggests that anti-state terrorism occurred over 40-year periods driven by ideological motivations: anarchist (c. 1880-1920), anti-colonialist (c. 1920-1960), New Left (1960-1980s), and religious radicalism (c. 1979-present). Despite its influence, this model has been criticized for oversimplifying historical contexts, and lacking empirical evidence (Millington, 2024; Parker and Sitter, 2016). However, although criticised, Rapoport (2003) provided an important recognition to the potential role of ICT, and its’ impact in decentralising terrorist activities, and revolutionising their operations, recruitment, and execution, with later researchers calling for the necessity to re-examine and move beyond these traditional models (Chertoff et al., 2020; Millington, 2024).

As pointed out, albeit somewhat controversially (see Stern, 2014), Marc Sageman in the context of the stagnation of terrorism research, highlighted the absence of relevant and comprehensive data, of which could encourage academics to rely on extrapolations from robust studies in unrelated fields, effectively acting as armchair investigators in their research (Sageman, 2014:571).

Although terrorism studies, and more specifically; Islamic terrorism received considerable attention, especially in the aftermath of September 11th (Haghani et al., 2022:20), it is important to acknowledge the concurrent emergence of research on cyberterrorism and hacktivism. This field of inquiry developed alongside contemporary terrorism studies, but despite their shared temporal origin, they diverged in focus and discourse within the academic domain. Unlike Islamic terrorism studies, cyberterrorism and hacktivism did not attain a similar level of prominence during this period, making it challenging to discern key academic understandings of both phenomena. Although it's broader domain 'cybercrime' has seen extensive research, data-driven studies, this can be seen to primarily focus on the operational impact cybercrime can have, and investigations towards mitigation. As noted by Holt et al., (2017), the limited criminological understanding towards the role 'motivation' plays as a justification to engage in online-disruption, cyberattacks, and similar is relatively limited to understanding numerous subcultures, often focusing on industry-specific experiences, excluding victim experiences or actor motivations, with much of the criminologically leaning studies adopting a techno-centric approach to understanding the phenomena (see Yar and Steinmetz, 2017).

Emphasising concerns towards the scarcity of primary data within cyberterrorism and hacktivism research, along with the lack of definitional coherence have been key concerns discussed within the literature (see Conway, 2011a, 2007; Jarvis and Macdonald, 2015; Macdonald, Jarvis, and Lavis, 2019), the initial review of literature for this thesis revealed two notable concerns; 1) a marked paucity of empirical and primary data and analysis in both domains, and 2) the significant academic attention towards the lack of consensus regarding their precise definitions.

Concerning the lack of empirical studies and reflecting on similar issues observed early within post 9/11 terrorism research literature, Andrew Silke (2004) observed a reliance on qualitative research methods, such as case studies. Silke further acknowledged that given the real-world focus of terrorism, there will always be avenues for exploratory or descriptive research, suggesting that fields of study, including terrorism studies, strive to advance understanding by progressing from descriptive to explanatory levels, and towards prediction-based research. Additionally, issues concerning a definitional consensus of terrorism can be seen as early as 1988 (Schmid and Jongman, 1988) with Schmid (2011:42) later going on to reiterate an earlier quote by British sociologist Phillip Schlesinger, that;

> *"no commonly agreed definition can in principle be reached, because the very process of definition is in itself part of a wider contestation over ideologies or political objectives"* (Schmid and Jongman, 1984:7)

Further, when asked what definitions they use, Schmid and Jongman (1988) found that of the 200 academics questioned, 58% admitted to using their own definition. No similar study has been repeated towards academic definitions of either cyberterrorism or hacktivism, however. Macdonald et al., (2019) conducted a qualitative survey in follow up to earlier 2012 survey of terrorism researchers discussing the concept of cyberterrorism. In their survey, Macdonald et al., determined that, when asked; "What are the major limitations, gaps, or weaknesses within academic research into cyberterrorism", over 30% of respondents noted issues concerning access to data as a considerable weakness within cyberterrorism research (2019:20), similar to that raised by Silke nearly two decades earlier concerning the state of terrorism studies, and its reliance on secondary sources (2004).

A second leading concern identified by Macdonald, Jarvis, and Lavis (2019) focuses on the need for a definitional consensus, with the latter considered more necessary when compared to results of an earlier survey (Macdonald, Jarvis, and Chen, 2013b). The inability to establish conceptual agreements, as noted by Macdonald and colleagues, often leads to fragmented knowledge gaps, paraphrasing a participant who stated that; without a clearly articulated definition, research of a topic descends into a fascicle of competing assumptions based on a disjointed foundation (Macdonald, Jarvis, and Lavis, 2019).

Inspired by the earlier self-reflections and critiques of terrorism studies, this thesis argues that much of the earlier limitations and key issues identified within earlier terrorism research, are equally present, if not currently emerging within the domain of cyberterrorism and hacktivism research. In similar findings to Silke's (2001) evaluation

of the "health" of terrorism studies, this thesis is the first critical evaluation of the "health" of cyberterrorism and hacktivism research. Further, this thesis contributes towards the wider field of cybercrime research, moving the discussion away from a pursuit towards consensual definitions of either cyberterrorism and hacktivism, and instead towards viewing both phenomena as complex forms of ideologically motivated form of cyber-deviance with multidimensional characteristics warranting evaluation.

1.2 Overview of Research Project

The central argument of this thesis contends that the limitations in academic understanding of cyberterrorism and hacktivism research mirror that of earlier terrorism studies (Silke 2003; 2008) and can be attributed to two long-standing difficulties. First, there appears to be an overemphasis among researchers attempting to establish a consensus definition for cyberterrorism, leading to a disproportionate focus that has resulted in a neglect of the critical need for empirical evidence and in-depth research focus. To provide an analogical explanation, research domains such as journals are like specialised crop fields, and definitions are its seeds. If nurtured in a consistently rich and fertile field, a seed can grow roots that reap the benefits of the soil, potentially yielding crops which further benefit researchers and society. Thus, if too many seeds are spread across an inconsistent number of fields, the likelihood of any one seed growing to yield is significantly reduced. Secondly, the prevalent tendency among researchers to conflate cyberterrorism and hacktivism has hindered the progress of empirical research due to the resulting conceptual confusion, further adding to the inconsistent dispersion and fragmentation of knowledge.

Returning to academic comparisons, unlike earlier terrorism studies literature, which Schuurman (2019) highlighted as being highly event-driven, a claim reiterated by Haghani et al. (2022:20) in their scientometric analysis of terrorism research, terrorism studies has illustrated that key events have a significant influence on the focus and trajectory of research, for example, the events of 9/11 were followed by increased government funding for terrorism research, new data on terrorism, and new terrorism journals (Phillips, 2023:416).

Cyberterrorism and hacktivism have yet to see such an impactful event occur (Conway, 2011a) as to lead to an expansion of the domain's academic productivity or has resulted in the publication of dedicated annual journals. Thus, this thesis presents the following research questions:

1) *How has the academic development of cyberterrorism and hacktivism research evolved over time.*
2) *What distinct, key definitional characteristics have emerged for both phenomena.*

The following sections will further explore the research objectives, and the methodologies used in this thesis.

1.2.1 Research Objectives and Rationale

The primary objective of this study is to examine the current state of academic literature regarding cyberterrorism and hacktivism. This will be achieved through the development and analysis of two databases: i) a compilation of key high-impact academic journal articles containing definitions of cyberterrorism and hacktivism, and ii) a taxonomic framework encompassing key terms used within these definitions. The creation of these databases will accomplish the following:

1. Trace and evaluate the academic development and status of cyberterrorism and hacktivism research through analysis of high-impact peer reviewed journal articles.
2. Identify key themes contained within the academic literature on cyberterrorism and hacktivism using content analysis.
3. Recognize challenges in cyberterrorism and hacktivism research and suggest possible solutions to tackle these issues.

Rationale for this study comes from the preliminary review of the literature on cyberterrorism and hacktivism, a potential gap has been identified in the academic literature. Critiques towards the dearth of empirical studies, and fragmented research collaborations and outputs has raised two notable concerns by policy makers and researchers (see MacDonald, Jarvis, and Lavis, 2019:20), with one notably acknowledging the lack of definitional cohesion amongst researchers and policy makers, stating that without a cohesive definition, the topic would become a “largely amorphous

mass of competing assumptions based on a shifting base" (MacDonald, Jarvis, and Lavis, 2019:7).

Definitions and conceptualizations play a crucial role in academic inquiry and policy formulation (Newman et al., 2016), guiding policymaker decision-making (MacDonald, Jarvis, and Lavis, 2019:7), and warranting significant attention in research endeavours. They provide a means of clearly differentiating concepts from one another (Schmid, 2023), and if research is to effectively address the potential threat of cyberterrorism and impact of hacktivism, researchers must go beyond rigid consequentialist views of kinetic harm and embrace a more dynamic conceptualization, to develop and implement suitable countermeasures (Straub, 2021:2). Likewise, for a concise unilateral definition to even be proposed, an academic domain needs to be in a healthy state of strong concise research output and collaborative academic community ventures. Developing a definition without a consistent network of related peers to adopt, and more importantly *use* such a definition within their own research efforts may only add to the trail of proposed but overlooked definitions that came before. Thus, akin to a farmer checking the fields before deciding on which crop to grow, an evaluation of the domain's academic output and its composition is warranted to assess its ability to yield a concise definition of either cyberterrorism or hacktivism.

To understand how conceptual understandings of cyberterrorism and hacktivism has evolved within academic research, and if the domain is in a state of hosting definitional consensus, this study aims to deconstruct academic understandings of cyberterrorism and hacktivism research output through an analysis of existing definitions and key

publications, employing a technique akin to Schmid and Jongman's (1988) approach in the field of terrorism studies. To achieve the objectives of analysing the evolution of cyberterrorism and hacktivism research and establishing a robust empirical framework for future investigations, a mixed-method approach will be employed. This approach will enable the accomplishment of the following objectives:

1. Use bibliometric analysis to map how the domain of cyberterrorism and hacktivism research has developed, and identify prominent peer-reviewed authors, literature, journals, and definitions of cyberterrorism and hacktivism.
2. Conduct a taxonomic content analysis to identify the most prevalent recurring terms and concepts within the definitions of cyberterrorism and hacktivism, facilitating comparative analysis.

By undertaking this mixed-method approach, the research aims to evaluate and realign the trajectory of cyberterrorism and hacktivism research, addressing empirical research gaps, and providing a comprehensive understanding of the key theoretical elements within its conceptualisations. The study, through its ontological and taxonomic approaches, attempts to fill these gaps by establishing a basis for systematic data collection and analysis, which is crucial for building robust theoretical frameworks in cyber studies. Lastly, mapping the distinctions and similarities identified between hacktivism and cyberterrorism, findings from this study can potentially aid researchers from various fields, such as criminology, information technology, and security studies, aligning their methodologies and insights more effectively.

1.3 Methodological Approach

This section will outline the methodology employed in this research project. Prior to detailing the methodological approach, it is essential to clarify the main research aim of evaluating the domain of cyberterrorism and hacktivism research.

To establish an answer to the research questions of how the academic development of cyberterrorism and hacktivism research has evolved over time, and what distinctions have emerged from their definitions, it is first necessary to break down this question to establish and answer the following sub-questions:

1. What is the current landscape of academic productivity on cyberterrorism and hacktivism, and how has this research evolved over time?
2. What are the most prominent academic definitions of cyberterrorism and hacktivism research, and the distinguishing characteristics of both?
3. What are the key issues present within the domain of cyberterrorism and hacktivism research, and how might these issues be mitigated?

To address the research question and sub-questions adequately, an inductive approach is adopted. The aim is to establish a robust framework for collecting empirical data that can be used in future research. Critically reviewing and analysing established definitions of cyberterrorism and hacktivism, a framework can be developed to differentiate cyberterrorism and hacktivism from the often-compared phenomena of traditional terrorism and activism.

By adopting an inductive approach, this research project will draw upon peer-reviewed academic literature as its primary data source. For this study, a sample of 126 peer-reviewed journal articles were analysed. These articles were identified using 8 database sources; 3 publisher databases (Taylor and Francis, SpringerLink, Sage), and 4 academic search engines (Scopus, Web of Science, BASE, JSTOR), and limited to studies primarily focused on researching the phenomena of cyberterrorism, hacktivism, or both, and limited to articles with a Google Scholar citation metric of 10 (further known as *high-impact peer-reviewed articles*). The following sections provide an overview of the methodological stages employed.

1.3.1 Scientometrics via Bibliometric Analysis

The evaluation of scientific research provides insight into productivity and output of scholarly endeavours (Cohn and Farrington, 2014:275). Bibliometrics, a field dedicated to analysing article data and providing quantitative insights into written works, occupies a unique position as one of the key subfields focused on measuring the output of scientific research (Garfield, 2006:3). It facilitates the description of research within specific domains or organisations, offering a quantitative assessment of research output. Moreover, bibliometrics serves as an evaluation method to assess the impact of technologies, the effectiveness of authors, or the research organisations themselves. Additionally, it functions as a monitoring tool, enabling the tracking of research activity levels within a particular field over time. Frequently, bibliometric methods, which often employ content or citation analysis, are used to extract, and manipulate pertinent data (Wallin, 2005).

Therefore, to measure the growth and impact of ICT, definitions, and understandings related to cyberterrorism and hacktivism, the initial stage of this research project aims to establish an empirical overview of the current state of research in these domains. This assessment will cover a 20-year period (2000-2020), employing well-established bibliometric techniques such as citation analysis, and frequency occurrence. By using these methods, the analysis will provide a map and evaluate the evolution of cyberterrorism and hacktivism research.

1.3.2 Content Analysis

As Cohn and Farrington (2014) note, a limitation of bibliometrics is that it measures the quantity associated with bibliographic data such as citation counts, and an author volume of output rather than the quality of that publication (Cohn and Farrington, 2014:257). Although this is beneficial in evaluating the 'health' of a research domain's productivity over time, it does not necessarily permit the evaluation of its conceptual development.

To evaluate and map the conceptual evolution of cyberterrorism and hacktivism, a basic content analysis approach is used to code academic definitions of both phenomena as part of a combined analysis of the domain. Content analysis is a systematic method used to examine textual data with the objective of revealing underlying concepts, themes, and relationships present within a collection of academic literature. Through rigorous scrutiny, content analysis endeavours to reveal the inherent qualities of the information, thereby generating valid and reliable inferences (Krippendorff, 2018).

Used for the analysis of unorganised data towards ontological discovery, content analysis provides a systematic and objective means of exploring phenomena at a theoretical level (Elo and Kyngäs, 2008; Kyngäs et al., 2020:13). This enables researchers to gain detailed insights of a given research topic by delving beyond the superficial aspects of authorship and citations and examining the actual textual content produced by the authors. Consequently, for this thesis, content analysis facilitates an objective and text-driven examination of definitions of cyberterrorism and hacktivism, allowing for a comprehensive and rigorous review of its content.

Schmid (2023) contrasts definitions of social phenomena to that of a mathematical equation, in that; unlike more exact sciences that replace language with formulas and equations, definitions require the amalgamation of common language and established terms. What quantity of terms, and the depth of understanding needed to define a social phenomenon is difficult to determine, for example, Schmid and Jongman (1984) identified twenty-two different terms within an analysis of 100 definitions, with Schmid later arguing that this may be too many (see Schmid, 2023). Recognising this, the objective of the content analysis for this thesis is to organise and consolidate key terms from definitions identified within the collected peer-reviewed journal articles for analysis. The analysis of these key terms will be used to provide clarity and distinction between both cyberterrorism and hacktivism. To achieve this, a taxonomy developed by Al Mazari et al. (2015) and extended by Plotnek and Slay (2021) is adopted to organise and measure these terms towards a quantitative content analysis of identified definitions of both cyberterrorism and hacktivism.

1.4 Contribution of Study:

As research concerning the role of ideologically motivated ties between hackers and their behaviours grows, (see Holt et al., 2017; Rogers, 2006; Seebruck, 2015), alongside an increased availability of more accessible internet enabled devices and services, knowledge towards understanding the role of political, religious and social ideological motivations, such as that seen in cyberterrorism and hacktivism research has been limited (Holt et al., 2020). Research on cyberterrorism and hacktivism is multi-faceted, made up of researchers within a varied combination of disciplines and backgrounds. However, as noted by MacDonald, Jarvis, and Lavis (2019), the domain remains fragmented, and challenged with conceptual confusion towards both phenomena, with Kenney (2015) arguing that similarities between cyberterrorism and hacktivism contributes towards a conceptual blurring of these phenomena, due in part to sharing similar tactics, and cyber-dependencies (see Baldi et al., 2003:18, Yar and Steinmetz, 2017; 2019). To date however, no known study has looked to compare conceptual academic understandings of both cyberterrorism and hacktivism, nor assess how the current body of academic knowledge has developed throughout its recent inception.

This study maps the production of knowledge of cyberterrorism and hacktivism research within the academic paradigm, and destandardise conceptual definitions to further evaluate the domain's development and changes, identify potential issues contributing to the domain's fragmentation, and contribute towards a stronger research domain. The purpose behind this study is not to evaluate nor criticise researchers' contribution nor intellectual understanding of the domain, but rather, to survey the scientific ecosystem in

which this research and intellectual development is hosted within. This marks a 'branching off' when compared to more methodological evaluations of the 'state of play' seen in similar criminological research (see Brands and Van Doorn, 2022; Windle and Silke, 2019) often termed 'systematic reviews' or 'meta-analysis,' by instead focusing on its bibliographical structures, and how such structures shape the domain.

Using a combination of bibliometric analysis and basic content analysis, a methodology not commonly applied in cybercrime focused domains, this integrated approach supported identifying nuanced understandings of academic landscapes and the evolution of key concepts within emerging fields. Thus, by mapping both the quantitative output and the qualitative content of research (see Jick, 1979), the study provided a comprehensive overview of how the domain of cyberterrorism and hacktivism has developed over time and where gaps and opportunities for future research potentially exist.

The study addresses significant empirical and theoretical gaps within the domain by providing detailed empirical data that supports earlier suggestions of fragmentation within the field (see MacDonald et al., 2019), and that much of the highly cited literature within the domain were dispersed amongst a high number of individual journals, making it difficult for researchers to attain a cohesive understanding of the knowledge landscape. Second, the inclusion and integration of a content analysis of definitions provided a conceptual timeline of cyberterrorism and hacktivism illustrating that beyond operational tactics, both phenomena are distinct with hacktivism often associated with 'real world' events compared to cyberterrorism hypothetical descriptions. These contributions are

unique in that they move beyond the descriptive and delve into the causal and comparative analysis, which has been lacking in the field.

Further, the output of the content analysis contributed towards the creation of an extended taxonomy based on the analysis of academic definitions and literature, of which is a unique aspect of this study. This taxonomy contributes towards clarifying the often-ambiguous definitions and categories within cyberterrorism and hacktivism research. By providing a structured and detailed classification system, the thesis contributes to standardising the terminology and concepts used in the field, which can facilitate better communication and collaboration among researchers and practitioners.

Extending this contribution forward towards more practical utility, the study developed an ontological framework based on the refined taxonomy and provides a significant contribution due to its potential to standardise data collection and analysis across studies without the dependency of definitions. This framework can serve as a foundational tool for future research, enabling more systematic and replicable studies, which are crucial for advancing theory and practice in cybercrime research. By developing tools and frameworks that can be used across disciplines, the study uniquely contributes to facilitating interdisciplinary research. This is particularly valuable in the field of cybercrime, which intersects with technology, law, sociology, and criminology, among others (see Wall, 2001; 2007).

1.5 Thesis Structure

This thesis is organised into four distinct parts. Part one encompasses the present introductory chapter, and reviews of literature topical to this thesis (chapters 2 and chapter 3). Part two is dedicated to explaining the selected methodological framework in (chapter 4), and includes the data collection, bibliometric analysis, and quantitative content analysis. Part three, provides a comprehensive overview and description of both bibliometric and quantitative content analysis findings (chapter 5). Following this, these findings are further discussed and compared to the wider body of academic literature, identifying key issues and topics for further detailed discussion (chapter 6). Chapter 7 proposes an ontological framework as a potential instrument for data collection, which can enhance the research landscape pertaining to cyberterrorism and hacktivism, fostering more cohesive and collaborative research. Part four concludes the thesis with Chapter 8, summarising key findings and contributions, and includes additional material produced during the research project.

1.5.1 Chapter Outline

Chapter 1 introduces the study's background, context, research aims, objectives, methodologies, and contributions to the cybercrime research field.

Chapter 2 places the thesis in the context of scientific revolutions and evaluations, using terrorism studies as a case example and highlighting the use of scientometrics and bibliometrics for domain evaluation. Thomas S. Kuhn's paradigm shift framework (Kuhn,

1970; 1977) is explored, alongside its influence towards its use within scientometrics, enabling empirical analysis of paradigmatic shifts. This chapter case-studies terrorism studies, in which bibliometric techniques reveal shifts influenced by noteworthy events like 9/11 (Phillips, 2023), and demonstrates scientometrics as a valuable tool for understanding and navigating the dynamic evolution of scientific knowledge.

Chapter 3 explores the interrelated concepts of hacking, hacktivism, and cyberterrorism, tracing the evolution of these phenomena across different "generations." It begins by detailing the progression of hacking from creative technological experimentation to sophisticated, targeted cyber-attacks, emphasising the need to understand the complex motivations behind such activities. The chapter then shifts focus to hacktivism, highlighting the ideological underpinnings and vigilante actions that characterise this movement.

Incorporating Karagiannopoulos's (2018a) generational framework to classify hacktivism within distinct technological eras. Further, the chapter addresses the often-vague nature of cyberterrorism, positioning it as a cyber-dependent activity within the broader framework of terrorism activities. It underscores the unique methods and implications of cyberterrorism, aligning them with traditional terrorism's characteristics while recognizing their distinct digital context. This comprehensive examination advocates for specialised studies in cybercrime to better understand the intricate dynamics of technology, society, and behaviour in the digital age.

Chapter 4: This chapter outlines the initial pre-phase data collection stages of the study, describing the literature search process guided by the PRISMA-flow method to identify and evaluate 126 high-impact articles. Later sections present the methodological approaches from the study to provide a cohesive analysis of cyberterrorism and hacktivism research. Adopting a positivist and realist framework, the chapter emphasises reliability and the empirical nature of research, underpinned by ecological validity for systematic and rigorous methods. It details a mixed-methodological approach, combining a modified single-phase multilevel triangulation method (Creswell and Clark, 2007; 2017; Tashakkori and Teddlie, 1998) that uses bibliometric analysis, performance analysis, and science mapping techniques, supplemented by a quantitative content analysis using a structured taxonomic framework.

It further discusses the application of Reid and Chen's (2006) knowledge mapping framework for analysing research output and productivity. The chapter concludes with a detailed manual review of the articles, analysing 237 definitions of cyberterrorism (68.3%) and hacktivism (31.6%), with coded terms classified within the same taxonomic framework for deeper examination and discussion.

Chapter 5 is organised into two parts and presents findings from part one; the bibliometric analysis of 126 high impact articles, providing a detailed overview of the bibliographic development of the cyberterrorism and hacktivism research domain, including author position, gender, citation frequency, and key authors identified within the sample. This is followed by part two, focusing on the content analyses of 237

definitions of cyberterrorism and hacktivism. These definitions are coded using the earlier mentioned taxonomic framework and classified into six distinct categories: actor, effect, intent, means, motive, and target, discussing the empirical findings of each category in detail.

Chapter 6 discusses the findings in the context of cyberterrorism and hacktivism research, addressing challenges, developments, and conceptualizations within the domain. Examining the data extracted from 126 peer-reviewed articles on cyberterrorism and hacktivism, this chapter explores notable key issues identified within the domain. This chapter argues that the domain suffers from the issue of fragmentation instead of stagnation, including conceptual recycling, reliance on informal networks, gender and geographical biases, and a lack of collaboration.

The concluding chapter of part three, **Chapter 7** proposes an ontological framework for collecting and analysing details of ideologically motivated cyber-events, based on the taxonomic framework developed in the content analysis. The ontology is explained, and two case studies are used to evaluate the utility of the ontology as a data capturing tool suitable for various interdisciplinary researchers at various skill and career levels.

Part four ends with **Chapter 8,** which summarises research findings, discusses accepted knowledge, highlights study limitations, and suggests directions for future research. This part also includes the list of references, and the included appendix list.

Chapter 2. Understanding The Cycle of Scientific Revolutions: The Role of Bibliometrics within Criminological Research

2.1 Introduction

To begin the literature review section of this thesis, it is pertinent to first delve into its broader context, specifically, the assessment of epistemological structures pertaining to emerging scientific fields, and the role of bibliometrics within the wider criminological field. The emergence of scientific disciplines holds substantial importance for both the scientific community and society at large, exerting a noteworthy influence on policy planning, societal impact assessment, and the advancement of sound scientific practices (Sun et al., 2013). Therefore, although this study explores how cyberterrorism and hacktivism has been defined throughout a specified timeframe, this chapter aims to explore and present the purpose and utility of bibliometrics in the wider domain of criminological research.

Researchers have dedicated substantial efforts towards investigating various facets of scientific emergence within criminology (Birch at al., 2023; Dooley and Goodison, 2020), and the sociology of deviance (Merton, 1999; Pisciotta, 1981) with notable attention directed towards the seminal work of Thomas S. Kuhn in the second edition of his article “The Structure of Scientific Revolutions” (1970). Kuhn's primary contribution lies in his proposition of the cyclical nature of scientific progress by means of shifting paradigms.

2.2 Scientific Development and Paradigm Shifts

Traditionally, the prevailing understanding in the philosophy of science posited that the institutions contributing to scientific discovery operated through a rational and positivist process aimed at achieving a state of truth equilibrium, employing a gradual and incremental approach to progress (De Langhe, 2017:507). However, Kuhn challenged this perspective, contending that these systems are intricate and often misleading, and that science operates amongst alternating phases of development, such as seen in the shift from Newtonian mechanics to quantum physics (Firinci Orman, 2016:48). These sciences function without fixed objectives, operating as endogenous systems that establish their own rules and regulatory mechanisms (Kuhn, 1977:336). According to Kuhn, intellectual frameworks of which he defines as 'paradigms' (Firinci Orman, 2016:47) assume a pivotal role in shaping the trajectory of scientific inquiry, exerting a profound influence on the focus and direction of research. This influence arises from several factors:

1. Paradigms serve to systematise and highlight specific natural connections.
2. They bring certain relationships to the forefront, emphasising their importance.
3. Conversely, paradigms may obscure other relationships.

Due to these emphasised points, paradigms shape the intellectual outlook of scientists, steering the course of research. Consequently, elements that the current paradigm overlooks or underplays are less likely to garner prioritisation within the broader research community (Gordon and Neumann, 1979).

Within this framework, Kuhn argues that the advancement of science undergoes several distinct transitional phases: initially, the pre-paradigmatic stage, followed by the establishment of normal science, then the appearance of anomalies leading to crisis, and finally, the scientific revolution, which occurs with the introduction and integration of a new paradigm. This illustrates that a scientific discipline progresses through various distinctive stages during its development.

Kuhn's (1970) framework begins with the 'pre-paradigm stage', marking the emergence of a new paradigm as the most promising theory among several that coexist simultaneously. The subsequent stage, termed 'normal science,' represents a phase of scientific progress operating within the established paradigm, where knowledge is built upon the existing conceptual framework (Kuhn, 1970:180). The third stage, revolutionary in nature, arises from a 'scientific crisis.' In this phase, an old paradigm fails to account for crucial observations, prompting the emergence of a new paradigm that challenges the previous one by offering comprehensive explanations and a broader understanding of established facts. This cycle then repeats.

2.2.1 Normal Science

Kuhn's central thesis asserts that the advancement of scientific knowledge does not arise from practitioners' intellectual openness, but rather paradoxically, from their intellectual rigidity. He contends that 'normal' scientific inquiry is guided by paradigms, which encompass interconnected assumptions (theoretical, methodological, and empirical) embraced by those operating within a specific scientific domain. Most of the scientific research involves attempts to solve problems stemming from the paradigm without

fundamentally questioning its underlying assumptions (Dooley and Goodison, 2020). Kuhn posits that it is precisely because adherents of a paradigm view their cognitive framework as firmly established that they could focus on minutely resolving issues considered problematic within their research domain (Firinci Orman, 2016). Thus, scientific communities achieve cumulative intellectual progress by establishing a robust internal consensus regarding which types of problems, techniques, and solutions are valid, and by excluding those who do not adhere to the current framework.

According to this perspective, most scientific innovations are perceived as foreseeable extensions or minor alterations to existing paradigms. Scientists are thus more inclined towards confirmation rather than falsification of their proposed framework (Marx and Bornmann, 2010:442). However, Kuhn argues for a second, more radical form of innovation that occurs when one paradigm supersedes another. Due to the stringent definition of scientific paradigms and scientists' strong allegiance to successful ones, this kind of intellectual transition necessitates open rebellion against the prevailing intellectual orthodoxy. Such revolutions are typically instigated by a mounting accumulation of anomalies and persistent unresolved issues, leading to a loss of faith in the existing paradigm, or as Kuhn describes; a 'scientific crisis.'

2.2.2 Paradigm Shifts

Kuhn views paradigms as more than current or leading theories, but as worldviews in which science exists within, alongside the associated implications. Thus, every paradigm eventually accumulates a considerable number of implications, which inevitably gives

rise to anomalies that cannot be consistently reconciled with the specific cognitive expectations derived from previous scientific achievements and acknowledgments that guide ‘normal science’ (Kuhn, 1970:10). Typically, these discrepancies may seem inconsequential when compared to past successes and ongoing research. However, over time, the efficacy of research and evaluative efforts driven by the paradigm reveals these anomalies, which simply cannot be addressed within the existing framework. Scientists are then “forced to reconsider some fundamental assumption that had up to then seemed obvious” (Boghossian 2006:119).

The widespread occurrence of these anomalies prompts the search for more appropriate rules, especially by emerging researchers who are less bound by traditional mindsets (Tabah, 1999). This leads to the proposal of numerous alternative frameworks, undermining the predictability of ‘normal science’ and culminating in a crisis where universally accepted criteria of scientific significance become elusive (Cole, 1992:22). In most cases of this nature, a new paradigm gradually gains acceptance through competition among proponents of rival theories, establishing a new orthodoxy in the field.

2.2.3 Critiques of Kuhn’s Structure of Scientific Revolutions

While Kuhn's conceptual framework has been influential, it is not without its critiques. This is to be expected, given that he calls on scientists to question their prevailing beliefs established by the social structure of science. For instance, Kuhn's definitions of ‘paradigm,’ ‘normal,’ and ‘revolutionary science’ have been criticised for lacking operational precision (Gordon and Neumann, 1979:135), leading to challenges in the

consistent application of Kuhn's ideas. Further criticism revolves around Kuhn's assumptions that scientific orthodoxies are rigid and resistant to gradual modification over time. Mulkay (1975:516) for example, argues that Kuhn's framework suggests that scholarly memberships are composed of committed individuals, confined to their paradigms and communities, of which they pursue for opportunity and recognition, and are unwilling or limited from exploring alternative scientific areas.

Kuhn's seminal concept of paradigm shifts in scientific disciplines, whether agreed with or not, has spurred further evaluative theories. For example, Mulkay's three-model approach (1975) critiques Kuhn, suggesting that the conception of scientific orthodoxies as being 'rigid' is incorrect. Mulkay proposes that in science, new problem areas regularly emerge and branch off into specialised disciplines, forming new social networks of researchers (1975:520). Shneider's four-stage model of scientific discipline (2009) offers another perspective, differing from Kuhn in that Shneider believes individual researchers within a scientific community experience different paradigm stage at different rates, as opposed to Kuhn's suggestion that this change occurs at an equal rate. Additionally, Kuhn's framework has been paired with concepts from cognitive sciences (Andersen et al., 2006), political sciences (Fuller, 2001), and philosophy (Hoyningen-Huene, 1993). However, interest in Kuhn's structural paradigms gradually waned with the introduction of dataset-driven scientometrics and the digitization of scientific literature in the mid-90s (De Langhe, 2017:504), introducing further means to map and track paradigm changes within scientific publications.

2.3 The Adoption of Scientometrics as an Evaluative Framework

The development and widespread adoption of scientometric evaluations in scientific fields has become commonplace (Miller and Page, 2007). Despite still being in its initial stages, Kuhn acknowledged the potential of scientometrics in substantiating many of his earlier assertions regarding paradigmatic shifts (1970:178). This recognition has led to a resurgence of interest in Kuhn's theory of "paradigms," following an earlier decline in interest upon the introduction of scientometrics (Marx and Bornmann, 2010:442).

Moving from Kuhn's conceptual framework of paradigm shifts to the empirical methodologies of scientometrics has provided a means to quantitatively analyse these non-linear transformative and progressive moments in science. As Kuhn posited, scientific revolutions entail not just extensions of previous knowledge, but shifts in fundamental beliefs and practices within a scientific community (Kuhn, 1970; 1977). Scientometrics offers a robust set of quantitative techniques to examine scientific productivity, trace the evolution of disciplines, and pinpoint pivotal moments in the advancement of knowledge (Glänzel, 2012; Glänzel and Lange, 2002). This offers a nuanced understanding of how scientific communities evolve and adapt in response to groundbreaking discoveries and conceptual disruptions, or, in accordance with Kuhn's theory of paradigms, in response to unresolvable anomalies and deficits.

As described by Glänzel and Schoepflin (1994), scientometrics, also commonly referred to as "*bibliometric analysis*" is a branch of science that uses mathematical and statistical

methods to quantitatively analyse various aspects of scientific research and scholarly communication. One of its primary applications is citation analysis, which involves scrutinising the citations that scientific papers receive to assess their impact and significance (Garfield, 1955; 2006), thus allowing for an overview of the epistemological structures that contribute to this knowledge.

Bibliometric Analysis, further referred to as; "*Bibliometrics*" encompasses a set of methodologies aimed at quantifying and measuring literature output. In scholarly terms, Wilson provides a general definition of bibliometrics as the "application of mathematical and statistical methods to books and other media of communication" (1999:13), with the term itself being first coined by Pritchard in 1969. Concurrently, during the 1960s Nalimov introduced the term scientometrics in the same period, focusing on quantifying citation values of scientific literature to assess academic impact (Hood and Wilson, 2001). Notably, scientometrics shares significant overlap with bibliometrics, and are often used interchangeably (Glänzel and Schoepflin, 1994).

The origins of bibliometric methods can be traced back to as early as 1873 when Candolle examined influential factors associated with the success of scientific nations based on memberships in scientific societies (van Raan, 1999). Over time, modern bibliometric methods such as co-citation analysis and bibliographic coupling emerged, using academic databases to observe and summarise scientific fields (Zupic and Čater, 2015). These methods have proven instrumental in mapping the interconnectedness and

developments within academic research fields, enabling scholars to better understand the complex dynamics of scientific knowledge dissemination and impact.

Bibliometrics finds application in both the "hard," social and behavioural sciences, with the latter benefiting significantly from its contribution to the knowledge construction process. Zupic and Čater (2015) highlights the existence of "information scatter" within the social sciences, indicating that various disciplines such as sociology, psychology, and communication contribute to the study of other fields and subfields such as criminology, which can often be overlooked through traditional literature review methods.

Scientific article evaluation has become a central element in understanding bibliometrics as a set of tools for analysing article data and providing quantitative insights into written articles. It stands as one of the few sub-fields concerned with measuring the output of science (Garfield, 2006:3). Bibliometrics can describe the research landscape of a particular field or reveal the quantity and focus of research output by specific entities such as journals, authors, and publishers. As an evaluation method, it helps determine the impact of a technology or assesses the effectiveness of an author, their research organisation, or a publisher. Furthermore, it serves as a monitoring tool to track the level of activity in a research field over time.

One of its primary applications is citation analysis, which involves scrutinising the citations that scientific papers receive to assess their impact and significance (Garfield, 1955). When a research paper is cited by other scholars, it indicates that the work has been deemed valuable, pertinent, and influential by peers in the academic community

(Bornmann and Daniel, 2008). This reflects the recognition and validation of the findings, methodology, and conclusions of a study by other experts in the field (Garfield, 1972). Additionally, scientometrics plays a crucial role in examining co-authorship networks, revealing patterns of collaboration among scientists, and identifying influential figures or research groups within a field (Glänzel and Lange, 2002), often integrated into further bibliometric analysis. Further discussion and details concerning bibliometrics as a methodology is provided in detail later in this thesis (see 4.3 Bibliometric Analysis).

Scientometrics has been instrumental in elucidating shifts in paradigms across various disciplines. For instance, Haggbloom et al. (2002) conducted a citation analysis of eminent psychologists, uncovering a distinct transition from behaviourist-oriented psychologists in the early 20th century to cognitive psychologists in the latter half. This aligns with Kuhn's theory of paradigm shifts, which entail a fundamental change in the underlying assumptions and methods of inquiry within the field of psychology.

2.3.1 The Role of Bibliometrics in Criminology

Despite the advantages, bibliometric approaches have only seen sparse adoption in criminological research when compared to other fields such as business management or nursing studies (Kokol and Vošner, 2019). Research which has seen wide use of bibliometrics can be seen associated with the evaluation of terrorism studies, seeing its adoption often as part of a mixed approach to knowledge discovery (Cohn and Farrington, 2014), and providing valuable insights in potential paradigm shifts, or in assessing the ‘health and trajectory’ of an academic field (Schuurman, 2019; Phillips,

2023) with bibliometrics often used as a diagnostic method to either identify potential issues within a scientific domain, to conceptually map the domain, or test an earlier hypothesis.

For example, earlier terrorism studies focused on state-centric terrorism, emphasising acts perpetrated by states or state-sponsored groups (Jackson, 2007). However, following the transformative events of 9/11, the nature of terrorism evolved, leading to a paradigmatic shift towards a broader understanding of terrorism as a global phenomenon involving non-state actors (Hoffman, 2006). This transition and growing interest in the field gave rise to a host of anomalies, akin to a ‘scientific crisis’ in Kuhn's framework, prompting the call for the proposal of new paradigms of theories and methodologies (the third stage of scientific revolution).

While earlier recognized (see Gibbs, 1989), the catalyst for this scientific crisis was highlighted by Schmid (2004b), who noted a prior anomaly of conceptual confusion in terrorism studies, emphasising a lack of consensus on key terms. Silke (2004) later echoed these concerns, also noting persistent challenges in the field, including an abundance of prescriptive content and a dominance of political scientists. Similarly, in the assessment of the psychology of terrorism, Horgan and Sageman challenged established assumptions about terrorist behaviour, drawing attention to the shaky empirical, theoretical, and conceptual foundations underpinning the search for a 'terrorist personality' (Horgan, 2008; Sageman, 2004). These seminal studies spurred the development of alternative frameworks and further evaluative approaches for engaging and reviewing terrorism studies, with key temporal evaluative studies (see: Silke, 2001; Silke, 2006; Silke, 2008;

Reid and Chen, 2006; Reid and Chen 2008; Gordon 2010; and Schuurman, 2020) offering a comprehensive overview of the field.

The increased adoption of bibliometric techniques to map the domain of terrorism studies has been in steady use since as early as 1997 when Reid evaluated a sample of 130 articles (derived from a population of 1166 studies) spanning 30 years (1960-1990).

In her analysis, Reid (1997) employed bibliometric methods to identify key articles for content analysis, a process like the one later adopted in this thesis. Using these key articles, Reid later applied a four-phase typology to map the evolution of knowledge concerning researcher specialisation, dispersion of work and ideas, influence on decision-making, mapping their impact on knowledge growth (Reid, 1997:93). Reid's methodological contribution toward the adoption of bibliometric analysis has seen an increased output of evaluative and reflective studies by Reid and colleagues in the years following the events of 9/11. For example, Reid et al. (2004) further incorporated computer-aided ‘network-based’ bibliometric techniques to establish a series of 'knowledge portals' for a deeper understanding of the evolving threats of terrorism. Subsequently, Reid collaborated with Chen (Chen et al., 2008; Reid and Chen, 2006; 2008) and Gordon (2004) to produce a series of research papers contributing to a broader mapping of terrorism studies scientific output. This work later influenced further studies adopting non-network oriented scientometric and bibliometric methods to better evaluate the expanding domain of terrorism studies (see Silke and Schmidt-Petersen, 2017; Magnone, 2014), with more recent examples of evaluative studies focused towards understanding the ‘health and trajectory’ of terrorism research such as Bart Schuurman

(2018; 2019), who adopting a similar approach used by Silke (2004; 2009) and colleagues (Silke and Schmidt-Petersen, 2017) adopting a more generalised informatic and meta-analysis approach to scientometrics, albeit with a much wider dataset of articles published between 2007-2016. Schuurman's analysis of terrorism research identified that, although having developed past Silke's (2008) earlier criticisms of the lack of primary data used in terrorism research, with researchers adopting a wider variety of methodologies and data gathering techniques (Schuurman, 2018:1022), the domain was limited by a predominantly singular focus on jihadism at the 'almost' exclusion of other subjects (Schuurman, 2019:475-476), with these findings further confirmed in a later evaluative study of by Ahmed and Lynch (2021) when exploring research pertaining to Far Right terrorism.

Such 'state of play' evaluations, however, are not without criticism. For instance, Phillips (2023) contends that many of the key evaluative studies focused primarily on the methodologies adopted by researchers, drawing considerable attention to anomalies like the scarcity of primary data sources, often at the expense of other notable issues. Phillips argues that the studies included in these evaluations often encompass both 'pre' and 'post-9/11' articles, which were themselves published shortly after the events of 9/11 (2023:410). According to Phillips, the limited number of years post-9/11 may not provide an accurate observation of research trends during such a paradigmatic 'worldview' shift. Moreover, by narrowly focusing on terrorism journals, there is a risk of excluding important terrorism attributed studies published in non-specialized peripheral journals such as Criminology and Political Science (Phillips, 2023), which leads to a selective mapping rather than a comprehensive evaluation of the topic.

In response to these concerns, Phillips conducted an evaluative study aimed at addressing the issues. By employing more network-oriented bibliometric techniques as opposed to the more 'informatic' meta-analysis approaches of earlier researchers, Phillips (2023) examined 6,880 academic articles on terrorism published between 1970 and 2019, spanning over 2,000 journals. Through this analysis, Phillips identified a notable paradigm shift in terrorism studies. Initially dominated by males and the work of political scientists, there was a significant shift towards psychology-based disciplines, with psychologists emerging as the most prolific researchers. This transition increased the representation of women within the domain, coming from behavioural science disciplines particularly in the first decade after the events of 9/11. Although there was a return towards political science dominance in 2012, the percentage of women conducting research on terrorism continued to grow (Phillips, 2023:422).

2.3.2 Network-Oriented Bibliometrics in Criminology

Although as noted by Phillips (2023), the use of non-network oriented evaluative studies may be limited in providing wider representation of research trends and trajectories within broad overviews of terrorism studies, earlier use of more network-oriented bibliometric analyses within terrorism studies exist to more closely map the production of terrorism research, and aid towards confirm earlier concerns of scientific domains. For example, Gordon (2004) identified that early terrorism research was largely relegated to 'peripheral journals' (a journal that occasionally publishes articles about terrorism but is dedicated mostly to another field of study), and that 'core' terrorism knowledge was published in a

few ‘non-visible’ journals (Gordon, 2004:415), suggesting the domain lacked a centralised ‘core’ journal in which to unite contributors. Mumtaz and Sultan (2011) would later conduct a bibliometric analysis of papers on terrorism published in journals from 1981 to 1990, analysing 402 citations. In their analysis, Mumtaz and Sultan (2011) were able to empirically confirm Gordon’s (2004) earlier findings, in which they identified that the annual growth of terrorism research was largely uneven, spread across a wide variety of journals making it difficult for researchers to be fully aware of the literature available on the topic (Mumtaz and Sultan, 2011:42).

Earlier evaluative studies adopted a more network-oriented bibliometrics within broader domains of criminology to identify key contributors. Shichor (1982) would use citation analysis to map the citational distribution of introductory criminology textbooks. Recognising the value of introductory textbooks as a means of “socialising” new and interested academics to the field, Shichor adopted citational analysis to identify and rank 19 key and impactful contributors within the domain based on the number of citations present within the textbooks in which to provide interested parties a foundation in which to begin their studies (Shichor, 1982). A similar study by Wright (1998) would later conduct a citation analysis simultaneously on both criminology textbooks and expanded to include criminal justice textbooks, later merging the results to identify both key contributors, akin to Shichor’s (1982) work, but also to identify the presence of an “elite group” of 16 scholars who have made substantial contributions both within criminology and criminal justice textbooks (Wright, 1998:319).

Observing criminology as a multidisciplinary field of study (see Sykes, 1974), the adoption of bibliometrics as a knowledge mapping technique would see its use in more specialised domains, fields and use cases, focusing on research of a particular crime, phenomenon, or even a specific individual's impact. For example, Alalehto and Persson (2013) would adopt bibliometrics via 'co-citation analyses to track the impact of Sutherland's contribution to criminology, analysing 2596 articles that cite Sutherlands' work, and concluding that Sutherland continues to have a long, and enduring impact on the theoretical development of criminology. González-Alcaide et al., (2013) conducted a citation analysis of articles published in 31 journals from 2005 to 2009 on the topic of criminology and penology. In their study, they identified an increased preference towards multi-author publications within the domain, further identifying that much of these publications were predominantly "national collaborations," with sparse inter-connectivity between journals from 'other' geographical areas and languages (González-Alcaide et al., 2013:35) raising concerns towards a potential lack of trans-national collaboration within criminology and penology literature.

2.3.3 Conceptual 'Knowledge' Mapping within Criminology

Advancements in computer-aided bibliometrics have seen a notably recent increase in the use of bibliometrics for the visual mapping and charting of themes and trends within scientific publications. Introducing the term "knowledge mapping," Shiffrin and Börner (2004) describe it as the synthesis of findings from a wide range of techniques used for charting, mining, analysing, sorting, facilitating navigation, and displaying knowledge.

As mentioned earlier, Reid and Chen (2006) incorporated the use of computer-aided bibliometric techniques to establish a series of visual 'knowledge portals' to provide a broad conceptual and bibliographic mapping of terrorism studies' scientific output, including research clusters of specialised researchers. Reid and Chen would later co-edit a special collection of terrorism study publications specialising in Informatics (Chen et al., 2008), which would see the continuation of their earlier study (Reid and Chen, 2006), further expanding on the use of mapping techniques within bibliometrics as a means of domain mapping (see Reid and Chen, 2008).

More recently, the use of knowledge mapping within criminological domains, such as the use of scientometric analysis in evaluating research trends towards understanding 'online hate', has seen increasing use with Waqas et al, (2019) adopting the use of bibliometrics to evaluate the productivity, dispersion, and conceptual mapping of 3,371 articles to provide a broad overview of online hate research. In their study, Waqas et al. (2019), identified that the domain was composed of studies within psychology and psychiatry disciplines, and limited to high-income countries with focus on the impact towards public health. Further usages of knowledge mapping would see similar use within public health to map broader understandings. Karystianis et al., (2023) would adopt knowledge mapping techniques such as text-mining to map 100 randomly selected PubMed article abstracts associated with publications researching epidemiological criminology, identifying significant themes such as infectious diseases, mental health, and alcohol and drug use, confirming earlier concerns raised in their previous study by people in

Australian prisons and Australian prison health service directors (see Simpson et al., 2021).

The use of conceptual mapping within criminology has seen broader usage as a means of consolidating wider understandings of the discipline. For example, Vander Beken, Vandeviver and Daenekindt (2020; 2021) mapped the topical dispersions of 11,724 presentations from 2001 to 2019 and held at the annual conferences of the European Society of Criminology, as a means of mapping topic prominence and evolution over time. Asking, "what is European Criminology", Vander Beken, Vandeviver and Daenekindt (2020; 2021) identified 50 topics using further bibliographic methods such as citation counts to determine top contributors and 'key topics' within the wider domain such as; 'desistance', 'victims and the CJS', 'cybercrime', 'environmental' or green criminology, and 'research methods' as leading topics within European criminology.

Thomas Bryan Smith and colleagues (2023) would adopt a similar approach in evaluating English-language peer-reviewed publications associated with "criminology" under the Australian and New Zealand Standard Research Classification. In their study, the use of topic modelling was adopted to identify and visually map research behaviours and collaboration trends within wider criminological research structure, identifying that researchers within criminology disproportionately favour familiar collaborators within similar subdisciplines (Smith et al., 2023:16), and that researchers who seek out collaborators outside of their immediate fields (such as terrorism studies, cybercrime, and

similar), often do so by engineering innovative research projects via subfield integration, confirming earlier hypotheses (see Leahey and Moody, 2014).

2.4 Conclusion

In conclusion, the adoption of scientometric and bibliometric methodologies has enhanced the evaluation of research within criminology. As previously discussed, the concept of paradigm shifts introduced by Kuhn (1970) offers a way to comprehend the dynamics and evolution of scientific fields. This perspective challenges the widely accepted view that institutions support scientific discovery through a rational and positivist process characterised by gradual and incremental contributions (De Langhe, 2017:507). This theoretical evolution of 'knowledge' structures such as academic publications has led to the adoption of bibliometrics to quantifiable measure the research output and influence of scientific paradigms, offering insights into understanding the structural shifts that have occurred within criminological research, as well as in the broader domain of scientific inquiry.

The wider role of scientometrics within criminological research has seen frequent use as a means to systematically evaluate the quality of research within a domain, focused on evaluating the distribution of data collection and analysis methodologies (see Schuurman, 2018; Schuurman, 2019; Silke, 2004; Silke, 2006; Schuurman, 2018; Schuurman, 2019; Silke and Schmidt-Petersen, 2017; Windle and Silke, 2019), often categorised under the remits of systematic reviews or meta-analysis. Although important to assessing the "state of play" for a research domain, Phillips (2023) suggests that the concentration on data-

collection and analysis methodologies adopted by researchers may divert attention towards other notable issues or shifts within a paradigm.

In addition to the robust number of systematic reviews and meta-analysis within criminological research, the use of bibliometrics has seen a steady growth within criminological specialities as a systematic means of mapping intellectual structures and confirmation of earlier hypotheses (Mumtaz and Sultan, 2011). More recent adoptions of bibliometrics have seen researchers take advantage of innovations in computational analysis, and visualisation by incorporating the use of network-oriented and conceptual mapping techniques to provide a 'wider picture' of criminological domains (Vander Beken, Vandeviver and Daenekindt, 2020; 2021). Thus, providing visual and empirical demonstrations of leading paradigms, emerging anomalies, and shifts in such ontological structures aligning with earlier conceptions of scientific paradigms earlier mentioned by Kuhn (1970), allowing researchers to empirically view the innovative and significant developments of domains not as relatively minor alterations to existing paradigms, but as a 'rebellion' of researchers within a paradigm, superseding against existing assumptions and theories due to the mounting accumulation of anomalies and persistent recognition of unresolved issues. This highlights the transformative potential of scientometrics and bibliometrics in furthering our understanding of criminological and broader scientific research landscapes. Or, to return to earlier agricultural analogies, allows for a detailed evaluation of a field's compensation, observing its historical futility, and robustness for further research.

Chapter 3. Introduction to Cybercrime and Ideological Hacking

3.1 Introduction

Information and Communication Technologies (ICTs) have become deeply entrenched in societal structures, impacting domains such as finance, health, education, and business (Stalans and Finn, 2016:501). More recently, ICTs have permeated the political sphere on a global scale. However, the excitement surrounding these technological prospects has been accompanied by public apprehension regarding the potential for increased criminal opportunities that may arise in this context (Wall, 2007).

Society has embraced this expansion and could be considered to have matured into an over-reliance on ICT. From a criminological perspective, this over-reliance has led to a series of unintended outcomes, of which Merton (1936/2006) described as the tendency to neglect unintended consequences when there is an excessive emphasis on achieving the intended outcomes. With the ease of access and freedoms provided by Internet technologies, the unintended consequences of these liberties' present individuals and groups opportunities to exploit and prey on the services and those who use them (Hunton, 2009:526). Further, as later noted by Merton (1938/2006), unrealistic goals of success are often the result of societal and cultural pressures, thus where legitimate means of achieving these goals are inaccessible, individuals may turn to prohibited means. The expansion of commercial markets via ICT, and thus economic opportunity leads to a reinforcement of goals providing more means in which to achieve them illegitimately,

part of which has collectively become known as cybercrime. Additionally, difficulties to enact legal consequences for cybercrime, and the inadequacies of capable guardianship has provided many opportunities for offenders to use ICT for the creation of new or extended criminal ventures, such as markets for the sale and exchange of illegal weapons and drugs (Hout and Bingham, 2013).

It's well recognised that increasing adoption of information and communications technologies leads to an ever-increasing risk of cybercrime (Jordan and Taylor, 2004; Wall, 2007; Seebruck, 2015; Yar and Steinmetz, 2019). Academic efforts to understand the exploitation of ICT often categorised actors of such exploitations as hacker(s), with different variations often expanding into "spaghetti western" approaches of hat colour; white-hat "good" hackers to the black-hat "bad" hackers, and grey for everything in-between (Yar and Steinmetz, 2019:53). However, a trend that will see repeated emergence throughout this thesis, and one all too familiar with researchers is that; over-simplification often creates difficult challenges and conflicting perspectives amongst understandings of motivational factors associated with illicit "hacking," or to echo earlier sentiments, a scientific crisis (Kuhn, 1970).

Therefore, this chapter, although exploring the fluidity of terms hacker, hacking and their associated 'cyber-activities' such as cyberterrorism and hacktivism, does not aim to propose yet another collection of concise definitions of either only to be added to an ever-increasing throng of unused definitions. Instead, it intends to present the epistemological evolution of these topics, focusing on how the understanding of hacking, cybercrime, and motivations of such actions has evolved over time. As Windle, Morrison, Winter, and

Silke (2018:8) have argued, such historical research can provide context for current debates and correct the entrenched misconceptions about both the past and the present knowledge pertaining to our understandings of these social phenomena.

The following sections will firstly introduce a general understanding of cybercrime, later focusing on the epistemological development of hacking, its motivation evolution, and eventual emergence towards what became later defined as hacktivism and cyberterrorism.

3.2 A Brief Overview of Cybercrime

As earlier noted by Kenney (2015); cyberterrorism and hacktivism exist within the same genus as other cyber-malicious criminal activities more commonly termed; cybercrimes. Attempts to better understand the collection of these malicious activities, or "cybercrime" has led to the proposal of a variety of research definitions and taxonomies to better separate hackers and understand the variety of crimes involving the use of digital technologies including; computer related crimes, computer crime, internet crime, electronic crime (e-crime), digital crime, technology crime (techno-crime), high-tech crime, online crime, computer misuse, cyber-enabled crime, and most prominent; cybercrime (McQuade, 2009:44). Increasingly discussed within academia, public discourse, media, and numerous policing and policy reports, through a variety of differing viewpoints however, the term *cybercrime* has yet to be universally defined (Brands and Van Doorn, 2022; Brenner, 2004; Gordon and Ford, 2006; Holt and Bossler, 2014), with Clough (2015:9) ambitiously suggesting that; "there are as many terms used to describe cybercrime as there are cybercrimes". Thus, in preparation to explore cyberterrorism and

hacktivism research, more specifically concerning how such phenomena have been defined, it is fitting to first be primed to epistemological efforts that attempt to define the broader term of cybercrime.

Previous attempts to understand cybercrime have focused on the impact of ICT, i.e. the *"*cyber*"* element, and how this contributes towards crime. By focusing on the element of cyber, Thomas and Loader (2000) defined cybercrime as.

> *"computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"*

Thomas and Loader's (2000) definition acknowledge that cybercrime can occur within a structured setting formed through interactions facilitated by a network of interconnected computers using the internet (Castells, 2014), such as the selling for fictitious items online, or targetted abuse using social media platforms. Although the mentioned definition identifies the cyber element from a practical perspective, the broad use of illegal and illicit within the definition leaves many defining characteristics open to interpretation and strives away from the necessary consensual factors required to provide a collectively agreeable definition within academic research.

Further definitions of cybercrime have attempted to expand beyond the network element with Gordon and Ford offering an exceptionally broad description of cybercrime as "*any crime that is facilitated or committed using a computer, network, or hardware device*," (Gordon and Ford, 2006:14). This definition of cybercrime suggests that the phenomena

can occur in “non-virtual locations,” Thus, Gordon and Ford propose that any criminal act using any form of presumably ‘electronic’ hardware can be defined as a cybercrime. Gordon and Ford (2006) addressed the breath of this definition by proposing that the term cybercrime be broken down to two distinct typologies:

> **Type 1 Cyberattacks** typically involve a singular, discrete event as perceived by the victim. These attacks are often conducted by deploying malicious software like keystroke loggers, viruses, rootkits, or Trojan horses into the victim's computer systems, akin to Gordon and Ford’s (2002:641) earlier depictions of ‘pure’ cyberterrorism, in which activities that are conducted entirely in the virtual world. The introduction of these programs may or may not exploit existing vulnerabilities.
>
> **Type 2 Cyberattacks** are facilitated by programs that do not fall under the category of crime-ware. For instance, communication might occur through Instant Messaging (IM) clients, or files may be transferred using the FTP Protocol. These attacks typically entail repeated contacts or events from the user's perspective (Gordon and Ford, 2006, pp. 14–15).

Gordon and Ford's definition (2006, pp. 14–15) of Type 1 cybercrimes assumes that cybercrimes are individualistic acts as perceived by the victim. However, this overlooks a broader range of online criminal activities, such as large-scale data breaches (Peretti, 2008) and disruptive denial of service attacks (Peretti and Slade, 2014). While some cybercrimes can be seen as individualistic, differing perspectives on what constitutes

cybercrime hinder the establishment of a universally agreed definition. Various approaches to framing cybercrime acts themselves have been suggested, including the earlier works of Wall (2001; 2007) and Yar (2005a; 2005b), who propose viewing it as a spectrum of illicit activities linked by the central role of ICT, or the 'cyber' element, as mentioned earlier (see Thomas and Loader, 2000). For example, earlier attempts to categorise various cybercrimes would see Wall (2001:3-7) attempt to expand the practicality of cybercrime definitions by operationalising the phenomenon into four distinct subdivisions based on areas of criminal activity and behaviours. As opposed to focusing on specific offences, Wall (2001) reflects not only various bodies of law, but also incorporated specific courses of public debate; cyber-trespass, cyber-deceptions/thefts, cyber-pornography/obscenity, and cyber-violence. Yar (2005a; 2005b) acknowledging Wall's classification, recognised that such a classification, although practical, did not aid in discerning how these emerging crimes were distinct from their legal-framework counterparts.

Efforts towards providing more nuanced understandings of cybercrime in separation to their more "offline counterparts" sees the adoption of observing the phenomenon as two distinct avenues: cyber-enabled crimes, and cyber-dependent crimes, weighing the integration and use of ICT as key distinguishable factors:

> **Cyber-enabled crimes** are traditional crimes that are increased in their scale or reach using computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT.

> **Cyber-dependent crimes** are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e., the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud (McQuire and Dowling, 2013).

The increasing techno centrism of cybercrime research would see Yar attempt to bring attention to the dearth of social understanding if cybercrime offenders and victims by evaluating criminological narratives of cybercrime through a conceptual application of routine activity theory (Yar, 2005b:418), considering each element of routine activity theories' (RAT) schema of the criminogenic situation (i.e. motivated offenders, suitable targets, and absence of capable guardians). Yar however, would come to recognise that theories such as RAT's dependency towards the 'organisation of time and space is central' for criminological explanation (citing Felson 2000: 148), and that 'cyber' operates very much spatio-temporally disorganised (Yar, 2005b:424), concluding that criminological theories such as RAT proves incompatible in adequately understanding cybercrime.

Returning to this concept in their 2016 study, Leukfeldt and Yar (2016) revisited routine activity theory (RAT) and cybercrime by analysing eleven earlier studies that employed the theoretical framework. Their findings indicated a lack of consensus on RAT's utility and the absence of a compelling reason to formulate new criminological theories. Instead,

they emphasised the need for additional empirical studies, highlighting issues such as the limited scope of analysed cybercrimes and insufficient empirical data (Leukfeldt and Yar, 2016:277).

Holt, Freilich, and Chermak (2017) contended that both Criminological and Sociological studies have historically focused on the subculture of cybercrime groups, and not its scope, echoing Leukfeldt and Yar's (2016) earlier comments on a dearth of available statistics, and that available data often focuses on industry-specific experiences, excluding victim experiences or actor motivations (Holt, Freilich, and Chermak, 2017:37). Efforts towards understanding of offenders remains difficult, due to in part the opportunism provided by the internet and its ability for offenders to maintain a high degree of anonymity (Van der Bruggen and Blokland, 2021). This anonymity makes evaluating the ideological motivations of those who commit a targeted cyberattack outside the generalised understandings of economic gain and desire to cause disruption, difficult, furthered by the lack of an agreed singular definition (Brands and Van Doorn, 2022; Brenner, 2004; Gordon and Ford, 2006; Holt and Bossler, 2014). Similarly raising concern towards the limitations of empirical data, Bossler and Berenblum (2019:495) note that both historically and currently, the lack of official statistics on most forms of cybercrime has become a significant challenge for cybercrime scholars, and that in response, a 'scientific revolution' of new directions in cybercrime research has arrived to move the field forward.

Recognising the need to move the field towards more robust and holistic understanding of cybercrime and cybercriminals (see Landreth, 1985; Hollinger and Lanza-Kaduce,

1988; Rogers, 2006; Seebruck, 2015), researchers often criticised earlier typologies and classifications of hackers and cyber-actors as being rigid, failing to address the rising increase of socially complex and ideologically motivated hacking such as hacktivism, and somewhat technocentric focus of cybercrime research. Yar and Steinmetz (2017) suggests adopting a modifiable and expandable understanding of cybercrime ranges due to the continually evolving environment cybercrime exists in, which can be summarised as effort to future-proofing understandings.

Such example towards a futureproofing of epistemological understandings is seen with Seebruck (2015), who argues that hacking has evolved to include a wider subset of motivational factors, later expanding upon an existing typology (Rogers, 2006) by including an additional two categories "hacktivist" and "crowdsourcing" alongside initial cyber-actors proposed by Rogers (2006). This expanded typology was later expanded further to include Plotnek and Slay's (2021) definition of "cyberterrorist" as a distinct class of ideologically motivated cyber-actor(s), more specifically separate to hacktivists and Rogers (2006) conception of a "cyberwarrior" (see Hosford, 2021) allowing for more complex evaluation of hacker types based on both the degree of skill and motivational characteristics.

More recent research efforts within criminology have seen an increasing diversity in cybercrime research with a focus towards more complex forms of cybercrime, moving away from descriptive studies under a singular 'cybercrime' umbrella, and instead providing more specialised studies. More recent examples such as Perkins, Howell, and Dodge (2022) sees the focused application of routine activity theory to better understand

malware and spam distribution patterns in target suitability, identifying that certain factors associated with nation states (corruption, political freedom, gross domestic product) are associated with an increase in victimisation, with the presence of capable guardianship having little impact towards reducing levels of targeting (Perkins, Howell, and Dodge, 2022:206). As the seminal work of Berger (1963) suggest; when theories are applied too broadly, they may fail to capture the nuances of different social settings, leading to misleading or incomplete understandings of social phenomena. Thus, Perkins and colleagues (2022) study may suggest that, unlike in Yar's (2005b) earlier efforts, the application of routine activity theory within the domain of cybercrime research may be better utilised in more focused and specialised branches of studies, as opposed to broader applications in order to better capture the nuanced factors such as motivation and guardianship, of which are difficult to determine within wider more disorganised settings such as those based within ICT networks.

Reflecting on earlier literature concerning cybercrime research demonstrates an early shift towards the broad technological or infrastructural impact of cybercrime. Understandably, as the technological development and wide adoption of ICT significantly increased at a rapid pace, the academic interest and focus towards understanding the techno-central role of cybercrime, and its' potential harm towards critical infrastructure would divert the focus of researchers and policymakers from the social and psychological causes of cybercrime (Pasculli, 2020). Returning to the earlier works of scientific paradigms (see Kuhn, 1970; 197), Kuhn's assertion implies that researchers evaluate the potential impact of theories, favouring those with promising futures and their anticipated

ability to address unresolved challenges in the field. This concept, when applied to cybercrime research, suggests a trend where researchers prioritised technocentric approaches over exploring the social and psychological dimensions of cybercrime, instead concentrating on technological aspects driven by expectations that these aspects are more likely to yield innovative solutions to emerging cybercrime issues and threats.

Thus, when comparing domains such as cyberterrorism and hacktivism to other subjects within contentious politics, international relations, and potential targeting of critical infrastructure it is unsurprising such topics and their increased focus towards ideological and social motivations within cybercrime research are under-theorised (see Holt, Stonehouse, and Freilich, 2019). Asal et al. (2016) recognised a similar imbalance within the role of politically motivated DDOS attacks, citing that much of the academic research often approached the problem from a "computer science lens" focusing on methods of detection and deterrence (citing Lee et al. 2008; Jin and Yeung 2004).

Equally noted by Asal et al., (2016:237), the general terrain of hackers and their motivations have also been explored within technical disciplines. Therefore, to better understand the social and motivational understandings of hackers, the following sections will explore epistemological understandings of hackers, and their genealogical and subcultural growth. Later sections of this literature review chapter will explore academic understanding of hackers as ideologically motivated actors, more specifically within the domain of hacktivism and cyberterrorism.

3.3 The Emergence of Hackers and Cyber-Deviance

Scholarly interest in cyber-deviants (alias; hackers), and their participation in cybercrime has increased significantly over the past two decades. Several aspects of 'hacking' have often been identified using singular definitions, with these definitions focused on specific transgressive acts of digital exploitation or more often, lumped together by numerous technology sectors making use of 'hat colour' approaches to simplify and categorise actors (see Yar and Steinmetz, 2019). Advancements in technologies have, however, led these singular definitions and *'*spaghetti western*'* approaches of differentiating hacker impact and intentions to become an incompatible and outdated representation of hacking (Seebruck, 2015), as such models pose a risk of undermining the severity imposed by acts of cyber-criminality, and fail to explain the complex and diverse range of activities associated with contemporary hacking and the motivational factors that drive these actions.

As academic circles expand their interest in understanding ICT and its greater societal impacts, an array of definitions are produced, all competing to better understand and categorise hackers (see Clough and Mungo, 1992; Duff and Gardiner, 1996; Jordan and Taylor, 1998; Nissenbaum, 2004; Chiesa et al.,, 2009; Al-khateeb *et al.*, 2016). The existence of competing definitions is common within any academic field, especially one which is new and must continuously adapt to a rapidly changing environment such as information technology.

However, Jordan and Taylor (2004) noted that by the mid-1990's, key understandings associated with the term 'hacker' were solidified. Hackers' and their technological ability

were frequently “equated largely towards illicit, illegal or unwanted computer intrusion” (Jordan and Taylor, 2004:5), adopting connotations such as ‘computer criminal’ and ‘electronic vandal.’ This criminogenic evolution of what the term entails can be partially considered a result of the amplification of its use by journalist, who often associate the term with those committing criminal, and often unrealistic, activities through ICT (Internet Communications Technologies), with Horton (1978) suggesting that the media often compose dramatic narratives and portrayals of deviant behaviour in effort to increase viewership and readership, contributing to the creation of folk devils and moral panics. Similar narratives appearing throughout the development of ICT and expansion of hacking as a skillset has made hacking synonymous with cyberattacks. That is, while there are different definitions available, there is somewhat of a consensus that the action of hacking is criminal, and thus hackers are criminals.

The Mercurial state of the term hacker and its practical term hacking contribute to the confusion and difficulties in establishing a consensual and uniformed definition. Hackers and hacking have a long history of interest and have been explored within a multitude of scholarly articles ranging from etymological accounts (Levy, 2010) to more populistic outputs (Jordan and Taylor, 1998) with much of the literature appearing throughout the mid-1980s to late-1990s. While these writings offer interesting insights into the practices and etymology of hacking, they provide little critical observation of the phenomenon. Instead, they favoured more idealistic and romantic reviews of hacking subcultures. These non-critical reviews, followed by an increasing public interest in computer technology through depictions in early films such as War Games and more modern depictions such

as Mr Robot, contributed to the distortion of public perceptions surrounding hackers and its affiliation with criminal intent (Wall, 2007).

Yar and Steinmetz (2019:54) argue that the lack of consensus on hacking has allowed various entities, including researchers, governments, law enforcement, information security experts, and the media, to create their own definitions, often focusing on criminal aspects. This tendency to associate hacking with criminality causes confusion and contributes to labelling individuals engaging in hacking as criminals. Drawing from Becker's (2008; published in 1963) concept of labelling, Yar and Steinmetz (2019) emphasise that perceptions of hackers and hacking groups are socially constructed and intertwined with reactions towards them.

3.3.2 Hacking as Subcultures

The actions of hackers are often complex, and difficult to understand. Consequently, society and its influencers such as state institutions and media are free to interpret hackers and hacking by any means, often identifying "hackers" as operating outside of standard society and law, leading to "the crystallisation of the 'super-hacker' stereotype as the archetypal cybercriminal" (Wall, 2007:16). This labelling parallels the detached conspiracy theories of organised crime research (Windle *et al.*, 2018): here moral panics about hackers identify them within folk-devil narratives as outsiders, or the "other", who is not like us, often described as dangerous youths or foreigners attempting to undermine our way of life (see Cohen, 2002).

Hacker stereotypes, labels, and eventual folk-devils have led to an array of scholarly attempts to consolidate the varying understandings and perceptions of hackers and the associated act of hacking, with many often adopting an etymological overview in effort to better understand these terms (Baumard and Baumard, 2017; Jordan, 2017). To look beyond the view of hacking and hackers as what Wall (2007) earlier described as 'crystalised stereotypes', it is worth returning to these etymological overviews of which makes notable reference to Levy's (2010) personal observation of hackers (see Holt et al., 2020; Jewkes and Yar, 2013; Loader and Thomas, 2013; Yar, 2013; Yar and Steinmetz, 2017; Yar and Steinmetz, 2019). Originally published in 1984, Levy's writings have retrospectively been identified as categorising the first wave of hacker's generations and their motivations, with Jordan and Taylor (2004) evaluating these generations with extensive overview of the topic, which was itself an attempt to provide a more structured and linear generational overview of hacking and their associated motivations and ideologies, extended with the addition of a "second wave" of hacker classifications.

As this thesis focuses on the use of ICT for ideologically motivated cyber-activities such as cyberterrorism and hacktivism, it is worth exploring the earlier uses of these technologies in order to grasp how concepts such as motivations and their fostering ideologies applied to ICT, and in parallel; how ICT was used to take action based on ideological and motivational reasons.

First Generation Hackers

The first-generation hackers, according to Steven Levy's anecdotal account, adhered to a set of ethical principles that support their motivations on how 'they' believed ICT, and

digital technologies should develop. These principles included unrestricted access to computers and information, a belief in decentralisation, and prioritising hacking skills over conventional criteria like degrees or age (Levy, 2010, pp. 28–34). These principles ran counter to the commercial and regulatory trends of the burgeoning computer industry.

Levy's observations align with the early '*original hackers'* motivations to explore and extend emerging technologies, often through unorthodox operations (Shinder and Tittel, 2002:52). The concept of free access to information, as championed by figures like notable American writer Stewart Brand, allowed for greater creativity. This contrasted with the more materialistic focus of *hardware hackers*, who played a key role in decentralising computing hardware (Jordan and Taylor, 2004:10). *Phreakers*, a subset of hardware hackers, delved into the illicit exploitation of telecommunication technologies. These 'Phreakers' manipulated audio frequencies to route calls, showcasing a more transgressive approach compared to the original hacker ethos (Turgeman-Goldschmidt, 2008:383).

The later emergence of *software hackers* marked a shift in motivations towards self-interests, particularly in gaming software (Wall, 2007), with actors amongst the software hacker generations being more interested in financial incentives rather than earlier creative priorities (Clough and Mungo, 1992). This represented a significant motivational deviation from the earlier anti-capitalist ethical values shared among much of earlier hacker subcultures. In more recent times, a resurgence of software hackers has emerged, driven by a desire to challenge the closed ecosystems of technology giants such as Apple Computers and in part Microsoft.

Second Generation Hackers:

Second-generation hackers, as described by Jordan and Taylor (2004), form a loosely associated network, not confined by specific ethical tenets. This generation encompasses groups like the Hacking & Cracking community, Microserfs, the Free Software Movement (later known as FOSS), and Hacktivists.

The *Hacking & Cracking* group focused on unauthorised access and exploitation of ICT, leading to the emergence of the term "cracker" (Raymond, 2003) to distinguish their activities from traditional hacking. "Microserfs", a term originally coined by Douglas Coupland (Coupland & Faye, 2001) in his fictional analysis of Microsoft, were computer programmers working for large corporations like Microsoft, deviated from the original hacker ethos by aligning with corporate structures, and often negatively depicted as "geekish" and obsessive (Jordan and Taylor, 1998:493).

The Free Open-Source Software Movement (FOSS) emphasised collaborative, open-source software development, motivated in opposition to the commercialization seen in the Microserfs generation (Jordan and Taylor, 2004:12). Richard Stallman, creator of the General Public License (GPL), a copyright licence ensured software developed under FOSS principles remained free and modifiable, preserving the ethical principles of early hackers.

Hacktivists emerged as a response to perceived injustices or policies (Coleman, 2012). They adopt hacking techniques for social or political change, translating

> the principles of activism into virtual actions (Jordan, 2001). This movement grew from an anti-globalization sentiment, particularly against economic globalisation implemented by organisations like the WTO, IMF, and G8 (Jordan, 2001; 2007; 2017; Jordan and Taylor, 2004:43).

As ICT became more globalised and integrated within the atypical operations of a modern society, and viewing the use of generational overview of hackers confusing and insufficient in understanding the increase of trans-national hacking from a practical and operational environment, those within Microserf groups transitioned towards what later became known as the information security ('InfoSec') community and established the use of 'Hats' to provide a simplified distinction between the ethical and moral motivation of hackers (see Lange, 1997). The Hat typology was also compatible with the corporate adoption of hacking as a work ethic: reminiscent of the United States categorisation of labour into "white" and "blue" collar workers. The concept of hacking groups distinguished by 'hats' establishes its origins from old spaghetti westerns of black hat and white hat cowboys where black hat hackers engage in unlawful online activities, using their deep understanding of computer systems and networks to exploit weaknesses, potentially for criminal purposes, and white hat hackers often employed to seek out weaknesses in computer systems, software, and networks to make them more secure. These distinctions according to Chiesa, Ducci, and Ciappi (2009:47) were developed; "spontaneously in the hacker underground to quickly identify a hacker's approach and use of *their skills for constructive or destructive ends…." Later, a third "grey hat" was introduced, due to confusions amongst hacker communities and private industries regarding the degree of involvement and how much information was released in the form

of public disclosure of exploits and vulnerabilities when discovered by independent hacker groups.

Although the mentioned distinction of using “hat shades” is a frequently adopted and discussed approach to differentiating “bad or good” and at a later stage “middle-ground” hacker within the private sector's approach to information security and its commercialisation, and continues to see similar adoption within academic research as a means to define hacker motivations (see Caldwell, 2011; Kwon and Shakarian, 2018; and Silic and Lowry, 2021). These distinctions often suffer from their oversimplification and provide little to represent the broad and varied nature of those within hackings diverse range of topics and subcultures, of which includes websites, articles, and conferences attended by thousands of people throughout the world (McQuade, 2009). Furthermore, the concept of hacking as a work ethic has been discussed previously by Turkle (2005) and Chiesa, Ducci, and Ciappi (2009). These discussions, however, overtly romanticise the hacker subculture with the latter falling within sensationalistic views of ‘criminal profiling’ more fitting of a semi-fictional novella.

The transition away from earlier generational understandings of ‘hackers’ and towards the more ‘operational’ intent of hackers (via good, bad, and in-between) can be seen to have diverted attention towards further understanding of hacker motivations. Holt, Freilich, and Chermak (2017), alongside colleagues (2022) acknowledge that previous research primarily which focused on understanding hackers' motivation were often limited to financial and informational gains with a focus towards the use of ICT for cybercrime, later admitting to a notable gap in research regarding phenomena more

ideologically linked uses such as cyberterrorism and hacktivism, where hacking is driven by political, nationalist, and religious ideologies (Holt, Freilich, and Chermak, 2017). However, as seen throughout earlier literature concerning the generational development of hacking, there exists a rich plethora of ideologically motivated pursuits intrinsically linked to the exploitation of ICT for various causes and expressive purposes worthy of exploring.

3.4 Ideologically Motivated Disruptive Hacking

The embeddedness of information and communication technologies (ICT) within societal, economic and government structures, has given new avenues of social expression. As noted by Taylor (2005:5), this development has given means for various groups - such as the US-based *Electronic Disturbance Theatre* (EDT) in 1998 - to exploit such technology and develop towards the use of disruptive DDoS software as a form of targeted action. One such software, called "Floodnet," was used to support Zapatista rebels, a far-left political and militant group who were protesting the mistreatment of Indigenous people within the Chiapas state. EDT used Floodnet to disrupt various websites operated by the Mexican government (Wray, 1999) temporarily bringing the services provided by the website offline. Although EDT's efforts proved ultimately unsuccessful, this event, followed by the successful defacement of 300 websites with anti-nuclear text by British hacker "JF" in the same year, further reinforced by the emergence of "hackathons" in several countries marked the beginning of the use of information communication technology (ICT) as an avenue of political and social activism (Wray, 1998; Conway, 2007).

As discussions concerning the increased use of the internet technologies for disruptive actions, defacement of websites, and further uses of ICT for political action grew, similarly did academic interest concerning how such technologies could be used for ideologically motivated violent and extremist cyber-events. Thus, to begin, this chapter will firstly briefly discuss the concept of ideologically motivated disruptive hacking, of which will see this chapter later diverge into the overview of two principal social phenomena; hacktivism and cyberterrorism, discussing the academic epistemology and key academic discussions concerning their defining characteristics.

Many recognise the importance of having a more robust and structured understanding of the ideologically motivated ties between hackers and their behaviours (see Landreth, 1985; Hollinger and Lanza-Kaduce, 1988; Holt et al., 2017; Rogers, 2006; Seebruck, 2015), with far less research having focused on hacking such as cyberterrorism and hacktivism for political, nationalist, and religious ideological reasons (Holt et al., 2020).

Reactions to such discontent have generally seen the formation of groups, often discussed in reference to those within stratified populations, who are affected by differential ownership or access to resources, and as stated by Hechter (1978:297); often results in group solidarity that leads to further perceptions of stratification that stimulates hostility (Grant, 1991; Levine and Campbell, 1972). In the context of hacking and ICT, individuals who engage in equally privileged interactions, like the 'Microserf' generation of hackers discussed earlier, tend to behave more uniformly. Conversely, those experiencing interactions marked by differing levels of privilege (such as marginalisation, exclusion,

discrimination) often view the source of such privilege discontentedly, leading to conflicts and the formation of various opposing groups (Hechter, 1978). Examples include Free and Open-Source Software (FOSS) groups, which emerged in opposition to the commercialization of information due to restrictions such commercialization's have on software access and modification, and more disruptive entities tied to social and political issues, like hacktivism and cyberterrorist groups (Hechter, 1978).

The use of social and political ideologies to motivate and maintain group solidarity have long been used to take 'offline' political action (Post, 1990), with Holt et al. (2016:358) suggesting that similar factors that affect participation in political action can mediate across both offline and online actions. As Malešević stresses, "Ideologies make an appeal to moral norms, individual or collective interests or to superior knowledge with the purpose of justifying potential or actual social action" (2006:89), thus actors engaging in deviant behaviour such as those considered 'cybercrimes' may not define their actions as such, but instead as justifiable acts against an antagonist group (Rid, 2013).

Academic research on 'justified' cyberattacks via hacking is limited, often focused on the use of hacking techniques for security evaluation (Smith et al., 2001) and tied to the infosec 'white-hat' literature, or discussions concerning the use of "Hack-Back" counter-behaviours often adopted by law enforcement (see Jayaswal et al., 2002; McGuigan, 2019; Pool and Custers, 2017). More theoretically focused studies exploring the justification of cyberattacks has seen the use of Sykes and Matza's (1957) "techniques of neutralisation" to better understand actors' willingness to engage in disruptive-hacking behaviours, such as cyberattacks (Bossler, 2021; Chua and Holt, 2016), however these

studies are limited by focusing only on college students' participation and assumed (un)willingness to engage in cyberattacks.

Further perspectives see the adoption of such technologies and techniques to deliberately undermine authority through subversive actions, intentions similarly seen within offline counterparts; activism (see Lugg, 2017; Samoilenko, 2018), and terrorism (see Bjorgo and Horgan, 2008; Horgan, 2008). Thomas Rid (2013:22) suggests that this undermining is motivated by the desire to erode social bonds, beliefs, and trust in the state, often achieved through non-violent influence on individuals and citizens' loyalties. Rid continues by contrasting subversion with insurgency, stating that, unlike insurgency, subversion neither requires violence nor necessitates the overthrow of an established order to be successful (Rid, 2013). Expanding on the use of non-violent subversion, Russian interference with the 2016 US presidential election, and the continuing Russian campaign against EU member states over their policies on Ukraine (Omand, 2018:14), has ignited academic interest on the use of ICT information operations and the spreading of intentionally fabricated information or "fake news" (see Hossová, 2018; Omand, 2018). Indeed, Paterson and Hanley (2020:449) suggest that adoption and exploitation of social media for propaganda, alongside malicious programming, are being used for the promotion of political distrust. The use of ICT and the dissemination of information, whether intentionally for bringing awareness to political causes (Jordan, 2002; Levesque, 2006), spreading of radical propaganda (Conway, 2006; Garcia and Belim, 2016), or sharing of practical and malicious resources (Epiphaniou, French, and Maple, 2014; Zhang, 2014), has undeniably become a central focus to the understanding of ideologically motivated cyber-based groups such as hacktivists and cyberterrorists. Thus,

as the internet and its technologies evolve further into societal integration, and in turn "influence," these current changes necessitate evaluative understandings as to how these "cyberterrorists" and "hacktivists" with such ideological motivations embrace technologies to further pursue ideological goals, and how these academic understandings have evolved over time.

3.4.1 The Emergence and Definition of Hacktivism

As with many social phenomena, hacktivism has an array of various definitions proposed by a large cohort of stakeholders with the most cited definition proposed by Dorothy Denning (2000a:263):

> *"Hacktivism is the convergence of hacking with activism, where "hacking" is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ("hacking tools")."*

Denning's early definition, while fundamental in its principles, has seen frequent reference and debate. Effectively combining earlier hacking concepts alongside established knowledge and histories of activism, Denning's definition of hacktivism provides a framework that relies heavily on the reader's interpretation, albeit guided by the incorporation of notable events. Among the events used by Denning are the EDT group's DDoS attack on Mexican state websites and the Internet Black Tigers, an offshoot of the Liberation Tigers of Tamil Eelam, who conducted an email bombing campaign against Sri Lankan embassies (Denning, 2001). By juxtaposing the definition with a

collection of events and their associated features, Denning indirectly shapes the characterization of hacktivism. The intricate details of these events serve to portray individuals labelled as hacktivists as inherently politically motivated hackers.

Later definitions and adoptions of the term hacktivism would further acknowledge this political association by either associating hacktivism as a purely politically motivated act of hacking (Fowler, 2016; Gardner, 2014; Wright, 2008), being more varied in their motivations such as political, social, and religious (Andress and Winterfeld, 2014; Juliadotter and Choo, 2015), or having criminal motivations and ideologies (Andress and Winterfeld, 2014; Fowler, 2016; Gardner, 2014). These various motivational associations with hacking introduce a significant challenge in identifying unique characteristics that solidify hacktivism as a unique social phenomenon separate from other similarly situated phenomena such as cybercrime, cyberterrorism, or cyberwarfare.

Additionally, previous discussions of hacktivism localise the social phenomena within a similar generational overview akin to others previously discussed hacker-based cultural generations such as Crackers, Microserfs, and the Free Software Movement that is largely introduced or associated with both Levy's (2010) personal account and Jordan and Taylor's (2004) academic accounts, however. Previous generations of hacker cultures were definitive in their motivations. As discussed in the previous chapter, they attribute those motivations to the events of their time and are frequently tied to a specific group that functioned as instigators of such a generation. Hacktivism from a generational perspective, however, does not have a clear motivational attribute nor any singular

instigator that can be identified and has instead seen itself being applied as an operational framework, similarly to how activism is adopted (Hosford, 2021).

Thus, understanding hacktivism as a social phenomenon existing outside the generational evolution of hacking culture, and instead as an operational framework, allows hacktivism to be observed as a natural and thus inevitable branch of activism. Therefore, in a similar vein of attempting to define, or view hacktivism under some definitive definition, it would be more fruitful to instead observe the term as a framework that embodies digital skills and associated complexities.

Further, hacktivism should not be considered as simply activism extended by various degrees of hacking skill sets (i.e. cyber-enabled), those who partake in hacktivism may not necessarily follow similar methods or ethics as those typically associated with acts of activism, and instead, introduce newer or more niche tendencies. For example, partakers of hacktivism, or 'hacktivists' access and communicate within a wider potentially global network in comparison to more localised participants of activism by virtue of having access to global communication platforms (Jordan, 2001).

For example, the Hacker Manifesto, written by "The Mentor," aka Loyd Blankenship in 1986 wrote: "*We [hackers] exist without skin color, without nationality, without religious bias*" (Goode, 2015:81), later adopted by hacker group Anonymous, emphasising the decentralised nature of online groups engaging in activism.

This more globalised participation and dissatisfaction towards mainstream politics see those refrain from pursuing more localised party-based endeavours of activism to change the status quo but instead seek change by pursuing more universally political environments such as climate change, anti-war, and other similarly globalised issues (Jordan, 2002:46). Further distinctions between activism and hacktivism are also observed by the participatory membership of online groups such as those seen within hacktivist collectives, which are more fluid and reactive in their formation and are often made up of a variety of different ideologies which converge into collaborative work towards a specific cause or goal, noting Jansen (2011:83); hacktivism sees a lack the political solidarity and sensitisation traditionally seen in activist group memberships of which can be frequently seen as a defining characteristic of these groups.

This difficulty in selectively identifying characteristics, motivations, and methods unique to hacktivism and its actors makes acknowledging a definitive or working definition difficult. Equally, attempting to view hacktivism as merely an extension of earlier depictions of activism provides little support in solidifying an understanding of the social phenomena (Hosford, 2021:34). Lastly, the fluid participatory membership of hacker groups makes establishing common traits gleaned from a generational timeline of past events challenging as who is considered a member of a hacktivist group, if such a group can be identified, or what classifies an act of hacktivism is not codified.

As noted by Goode (2015), the current body of literature presents diverse evaluations of hacktivism. For example, discussing Anonymous (Coleman, 2011:511) and hacktivism

in a broader sense (Liu, 2004:361–367), both are considered inherently fluid when attempting to identify any distinct ideological categorization. An alternative perspective associate's hacktivist movement like Anonymous with "information anarchism" and libertarian values (Jordan, 2007:77), with another viewpoint suggesting that groups such as Anonymous embodies liberal ideology while concurrently harbouring elements of a socialist worldview (Fuchs, 2013). Challenges amongst academics to definitively agree distinct criteria necessary for a definition of hacktivism have led researchers to instead propose hacktivism, not as a singular definable phenomenon but instead through a lens of multiplex categories such as electronic civil disobedience (Delmas, 2018; Deseriis, 2017; Jordan, 2017; Karagiannopoulos, 2018a; 2018b) *alias* 'disruptive disobedience' (Edyvane and Kulenovic, 2017) and digital activism (George and Leidner, 2019) of which will be explored in following sections.

Hacktivism as Electronic Civil Disobedience

Significant research has often placed hacktivism within the lens of civil disobedience. For example, Denning frames hacktivism as a technique of "electronic civil disobedience, which brings methods of civil disobedience to cyberspace" (Denning, 2000a:263) portraying hacktivism as a cyber-enabled exercise of civil disobedience. This is later echoed by O'Malley (2013:140) and Karagiannopoulos (2018a; 2018b) who describes hacktivism within a generational framework which distinguishes between a first and second era of hacktivism. This first era Karagiannopoulos (2018a) titled as the 'birth of electronic civil disobedience' focuses on key hacker groups and notable events of the late-1990s and early-2000s.

Similarly, earlier works of Jordan and Taylor (Jordan, 2002; Jordan and Taylor, 1998, 2004; Taylor, 2005), the doctoral work of Alexandra Samuel (2004), and the writings of the activist group Critical Art Ensemble (Raley, 2009) discusses the act of hacktivism within a generational evolution of civil disobedience. Most notably, hacker group *Critical Art Ensemble* describes electronic civil disobedience as a transition of the traditional tactics of blockades and trespasses considered recognisable acts of civil disobedience onto an internet platform (Critical Art Ensemble, 1996). Karagiannopoulos (2018a) contributes academic clarity to these discussions by organising electronic civil disobedience into three distinct groups; virtual demonstrators, artivists, and information purists, allowing for the various approaches associated with electronic civil disobedience to be more critically explored and discussed.

Virtual Demonstrators

Hacking, as a form of political expression, has evolved with early groups like Critical Art Ensemble (CAE) establishing a blueprint for hacktivism, emphasising non-destructive actions (Karagiannopoulos, 2018a). These groups valued avoiding unnecessary damage and refrained from targeting critical services yet acknowledged the potential for unintended consequences and collateral damage (Critical Art Ensemble, 1996:120; Karagiannopoulos, 2018a).

In a virtual parallel to activist sit-ins, hacktivists employed distributed denial of service (DDoS) attacks, slowing, or blocking access to online services, akin to a virtual demonstration (Krapp, 2005:88). Electronic Disturbance Theatre (EDT) and

Electrohippies adopted CAE's principles, developing, and distributing their own DDoS tools for electronic civil disobedience. However, facing increased punitive measures and legal consequences, these groups eventually reduced or dissolved their demonstrations (Krapp, 2005).

Artivists

Hacktivism, as observed through a more public and spectacle-oriented lens termed "Artivists" by Karagiannopoulos (2018b), involves performative and expressive tactics in electronic civil disobedience. Artivists use various methods, such as distributing viruses with political messages, exemplified by harmless pro-Palestinian virus messages in the early 2000s (Meserve, 2001). Others defaced websites to protest perceived injustices, like the case of Jember Hacker Team (JHT) targeting Indonesian President Susilo Bambang Yudhoyono's website due to dissatisfaction with his leadership (Lukman, 2013).

Beyond traditional hacktivist methods like website defacement, Karagiannopoulos (2018a; 2018b) highlights groups like EpidemiC and "0100101110101101.org." These groups use viral code projects to communicate ideas and prompt discussions on intellectual property rights, reproducibility, and the uniqueness of digital assets in virtual spaces (Castle, 2000). These topics remain relevant today, with ongoing discussions surrounding non-fungible tokens (NFTs) in the online creative sphere (Rae, 2021).

Information Purists

Recognizing the foundational hacker principles of unrestricted access to information and anti-censorship, Information Purists, as discussed in Chapter 3 (see section 3.2 Hacking as Subcultures: 53), engage in modifying data or disrupting computer systems to draw attention to their political messages (Karagiannopoulos, 2018b:23). Groups like Cult of the Dead Cow and Hacktivismo employ digital tools, including encryption technologies and anonymization tools, to facilitate secure and anonymous communication, especially in evading authoritarian regimes and potential censorship (Samuel, 2004:183).

Cult of the Dead Cow (cDc), for instance, created 'Back Orifice' in 1998, identifying potential exploits within the Microsoft Windows operating system for remote access and control (Caswell et al., 2007). However, the original intentions of these hacktivist groups, centred on electronic civil disruption, diverged as the software, along with tools like *Six/Four*, *ScatterChat*, and *Torpark*, found use in encrypted communication and file sharing (Jordan, 2007; 2017). Unfortunately, these tools, including *Goolag Scanner* for searching vulnerable websites via Google (Fitri, 2011), were later adopted for malicious purposes by non-affiliated groups and independent actors, deviating from the initial hacktivist goals.

Proponents of ECD agree, however, that the actions of hacktivists that meet the criteria of traditional civil disobedience belong to the category of "electronic civil disobedience." Even as Karagiannopoulos (2018a; 2018b) introduces a concise generational overview of the emergence of hacktivism as electronic civil disobedience, based on numerous case studies and notable events, it is not without its criticism.

Opponents of comparing hacktivism to civil disobedience (i.e Delmas, 2018), suggest that few hacktivist acts can satisfy most criteria mentioned above. Taking Himma's (2007:74) framework of ECD, hacktivism can only fall under electronic civil disobedience if it does not cause damage to innocent third parties, if those taking part are willing and prepared to accept authority, and if it is in pursuit of a plausible political agenda (Delmas, 2018:66). While many hacking and cyberterrorism researchers, (see Brunst, 2010; Holt, 2012; Jangada Correia, 2022) frequently argue that the 'online world' is assumed to be analogous to the offline world, they fail to recognise the traditional landscape of streets and public forums for observed protest (Delmas, 2018; also Hosford, 2021). Simply, ECD is non-comparable to traditional means of civil disobedience as internet technologies introduce significantly unique means of protest distinct from previous forms of civil disobedience, they may share moments of cross-collaboration such as with the use of internet technologies in support of traditional activist activities in terms of mapping, communication, or event planning, however, this collaboration often service-based and of such common occurrence that it would be distinctly different from actions such as website defacement and targeted DDoS to consider both uses of internet technologies as separate.

3.4.1.1 Hacktivism as Digital Activism

Excluded from the earlier discussion on hacktivism, more recent academic literature has attempted to position hacktivism in a much wider framework as demonstrated in George and Leidner's (2019) Digital Activism Classification model:

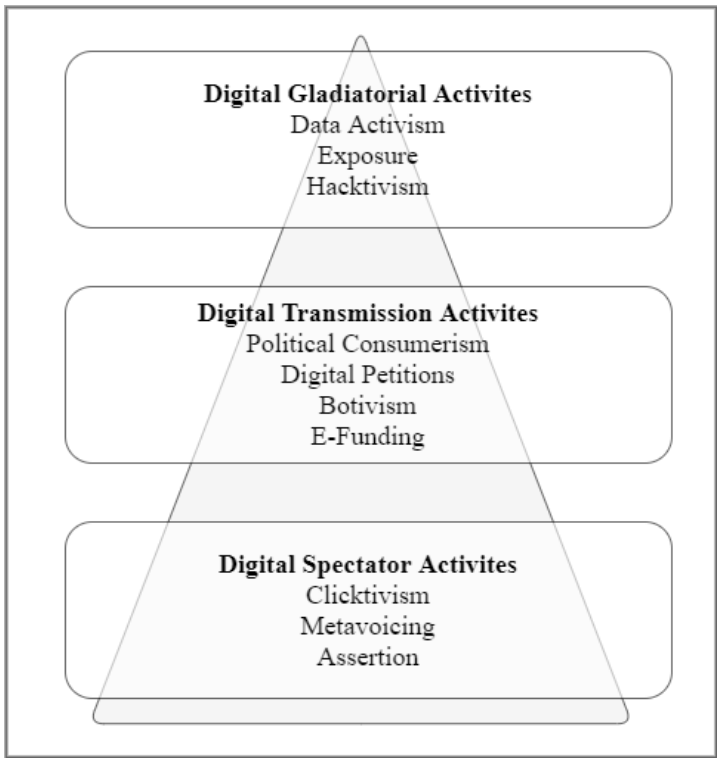


Figure 3.1 Digital Activism Classification (George and Leidner, 2019)

This classification places hacktivism as part of the much larger multiplex of digital activism skills-based framework that ranges from more generally accessible methods such as "clicktivism", "metavoicing", and "assertion" categorised under *Digital Spectator Activities*, to more sophisticated methods such as data activism, exposure, and hacktivism of which George and Leidner categorise as *Digital Gladiatorial Activities*. In their description, George and Leidner (2019) provide a detailed exploration of digital activism

and describe Hacktivism as part of a "digital gladiatorial" collection of activities as seen in *figure 3.1* using a modified variation of Milbrath's political participation model introduced in 1965 (see: Olsen, 1973) that looked at political participation from an individual level. George and Leidner (2019) extend this model by including both individual and organisational participants and identifying those operating within digital activism as change makers, not as influencers nor affiliated to any specific political party (George and Leidner, 2019:9) instead, George and Leidner identify these groups as being composed of a loose coalition who take strategic action towards making changes which impact society, government, and organisations (George and Leidner, 2019). More specifically, hacktivism, which both authors describe as involving direct, targeted and resource-heavy action against those both inside and outside tech-focused organisations.

Although George and Leidner extend their overview of hacktivism to include three subsets; "cyberterrorism" (Denning, 2001), "civic hackers" (Schrock, 2016), and "patriotic hackers" (Lokot, 2017), the topic of cyberterrorism will be reserved for its own chapter, a distinct category.

Civic Hacking:

Within increasingly information and communication-rich societies, the emergence of civic hackers, which the Open Science Foundation describes as those "deploying information technology tools to enrich civic life, or to solve particular problems of a civic nature, such as democratic engagement" (Hogge, 2010:10), involves members of the

public living within urban environments using their technical computer coding skills to better their immediate environment.

Many of those who align (Manion and Goodrum, 2005) with the civic hacking ethos encourage more collaborative approaches seldom seen in other hacking subgroups, frequently sharing their creations and hacks freely and publicly as open-source projects on digital repositories, such as GitHub[1], to allow others to use and modify their creations for their specific purpose and need. An example of such a tool is "*vTaiwan*" developed by the civic hacking group "*g0v*", a collective of independent developers who, unhappy with the lack of transparency and non-participation of the public within policy decision-making, created a mixed-reality, scaled listening exercise allowing politicians to listen to the public debate on numerous issues within their communities, allowing politicians to take on board discussions and comments made during these debates (Miller, 2020).

Although Hogge's (2010) ethos of civic hacking is described as a more localised example, due to an increased rate of ICT adoption the general framework can be considered to have scaled towards a more global approach which can be seen with the platforms such as the development and use of the "OpenLitterMap" service developed by Seán Lynch, a freelance software developer whose service allows for the crowdsourced collection and consolidation of data on litter and pollution allowing researchers, and various stakeholders such as local and state level agencies free access to the available data to encourage direct action (openlittermap.com).

[1] Github is an online repository for storing, sharing and publishing developer coding projects (see: https://github.com/about)

A prominent example in academic circles is the controversial platform Sci-Hub (www.sci-hub.se). This freely accessible online service attempts to disrupt the academic publishing domain (Marple, 2018) in offering unrestricted access to scientific articles, encompassing both open-access content and articles behind subscription paywalls. Aligning with the principles of the open-access movement, a cause intricately linked to earlier hacker generations and the free-software movement, as explored, and discussed earlier (see Chapter 3: 3.2 Hacking as Subcultures: 52). The second tenet of this movement asserts that "All information should be free." Sci-Hub goes beyond this by establishing a sharing network specifically for scientific articles. When viewed through the anti-capitalist lens shared by many in the earlier hacker community, this initiative appears to challenge the perceived privileged access held by key commercial and for-profit publishers and institutions, providing a means of disseminating knowledge freely to those often outside of more established institutions with the available resources needed to access these walled research publications (Windholz, 2019).

Patriotic Hacking:

George and Leidner (2019) describe Patriotic Hacking as non-state-sponsored hackers who focus their efforts on what they perceive to be in the best interest of the state, using this patriotism as a means of legitimising their actions. Lokot (2017:16) suggests that patriotic hackers "present themselves as a legitimate element of a greater strategic narrative in the conflict" often targeting their efforts toward enemy countries and their citizens (George and Leidner, 2019:11). Patriotic hacking can be considered a political

and ideological phenomenon, with their motivations for conducting hacks often focused on maintaining or returning to previously established beliefs and/or retaining the status quo associated with their country and its political sphere.

This differs from civic hacking which focuses on implementing improvements to communal infrastructure, quality of life, and transparency which can be shared with different nations and nationalities, as opposed to patriotic hacking more nationalist-oriented actions, and a sense of patriotism. For example, the US hacker known as "th3j35t3r" (leetspeak for "The Jester'') targeted Wikileaks which at the time was distributing leaked confidential information of government documents known as 'The United States diplomatic cables leak', taking down the site for an extended period for what was perceived as attempts to endanger the lives of US troops, "other assets" & foreign relations (Wong, 2010).

Unlike more traditional concepts of hackers as having more globalised world views (Jordan, 2002), patriotic hackers have more narrowly defined, nationalistic and parochial views often identifying themselves within nationalistic terms (Dahan, 2013:2) such as the Pakistan Haxor Crew (PFC), and Bangladesh Black-Hat Hackers. Offensive actions are motivated by strong nationalistic values, often reflected by the language and rhetoric adopted in provided statements, both publicly and frequently within the hack itself. For example, an early instance of patriotic hacking as noted by Dahan (2013) as an "interfada" a play on the term's internet and intifada or rebellion uprising was that of the frequent defacement of government websites by both pro-Israeli and pro-Palestinian hackers in a

sort of back-and-forth showcase of capabilities pro-Israeli and pro-Palestinian (Hershman, 2001).

3.4.1.2 Hacktivism as a Skilled Practice

The remote nature of hacktivism or hacking, in general, makes attempting to measure the ability of hacktivists and hackers a challenging task. However, an observation of the variety of discussions used to explain and discuss hacktivism and its actors could be summarised as technically skilled individuals and groups. For example, Jordan and Taylor (2004) express the use of hacking techniques by describing hacktivism as being "a form of social protest that grew out of the hacker culture, combining the transgressive politics of civil disobedience with the techniques of computer hackers" making use of "ambiguous digital tools to develop hacks that counteract the techno-legal regimes designed to regulate content distribution" (Jordan and Taylor, 2004:4). Similarly, von Busch and Palmås linked hacktivism closely to its original hacker roots by defining it as

> *"The online strategies and tactics of activists that more or less follow the autonomous anarchist tradition – squatters, phreaks, scammers, crackers, and cultural jammers engaged in anti-globalisation, direct action, and resistance"* (Von Busch and Palmås, 2006).

In their publication, hacktivists are characterised as adept inventors within the hacktivism domain, describing their approach as "craft-based, breaking open, probing, and exploring computer systems in order to bend or re-systemize them into a more desirable direction"

(von Busch, 2015:230). Xiang Li (2013) provides a more ambiguous definition when discerning the level of sophistication, proposing that hacktivism takes root within the online environment, and involves "the use of technology hacking mechanisms, often in the form of cyberattacks" (2013:302) a concept shared by several researchers (see: Holt, 2012; Milone, 2002; Scheuerman, 2016; Warren and Leitch, 2016).

Hacktivism as Hacking

This sophisticated use of technology mirrors those associated with understandings of hacking as the environment in which hacktivism and the more general category of hacking operates within the same domain. Operating within the same domain however does not describe hacktivism as being analogous to more malicious actions such as those seen in cybercrime or cyber-exploitation. Therefore, to describe hacktivism more accurately as a form of hacking, the two more commonly adopted methods used by hacktivists as cited by the variety of definitions; website defacement and direct denial of service (DDoS) will be discussed below.

Website Defacement

Website defacement involves unauthorised access to web servers, manipulating and replacing original content to disrupt or convey political/social messages (Krapp, 2005; Lindsay, 2017; Solomon, 2017). Hacktivists employ this tactic to discredit website owners and harm their reputation, with at least 32% embedding URLs to promote causes (see Trend Micro, 2018). Solomon (2017) considers it the most adopted but least damaging form of hacktivism. Maggi et

al. (2018:4) propose that those who engage in website defacement are ideologically motivated and part of an organised, coordinated team.

As a frequently used hacktivist method, website defacement is often employed for information dissemination. For instance, the Impact Team, a decentralised group, defaced Ashley Madison's website due to moral objections to its promotion of extramarital affairs, threatening to release 32 million customer profiles (Mansfield-Devine, 2015).

Direct Denial of Service (DDoS)

DDoS, the intentional disruption of a computer system, targets web servers by overwhelming them with high volumes of internet traffic (Mehrabov, 2016:504; Cloudflare, n.d.). Groups like Electronic Disturbance Theatre (EDT) used DDoS software Floodnet in 1998, allowing individuals with minimal technical literacy to participate in online protests (Taylor, 1998; Taylor, 2005:2; Deseriis, 2017:132).

An illustrative case of DDoS is “Operation Payback,” where Anonymous targeted MasterCard for ceasing Wikileaks donations. This DDoS attack made the financial site inaccessible to MasterCard clients, illustrating the widespread participation facilitated by the tactic (Addley and Halliday, 2010).

Hacktivism as 'Slacktivism'

Although a wide variety of definitions and descriptions of hacktivism exist, placing the phenomenon within a technically sophisticated setting, it is not without criticism. Critically comparing hacktivism to more traditional understandings of activism Sauter (2014:5) posits that whereas activism is difficult with only a select few capable of conducting a successful act of activism, and while acknowledging that hacktivism does make use of sophisticated disruptive tactics such as DDoS, Sauter suggests that these actions nonetheless fall within what he describes as a concept of "slacktivism."

Defining slacktivism as a willingness to engage in small often menial token acts of support for a cause, Kristofferson et al. (2020) note that slacktivism is an unwillingness to "devote significant effort to enact meaningful change," this starkly negative description reinforces the concept that online-based activist actions are less impactful than their physical counterparts.

This slacktivist critique of hacktivism isn't limited to Sauter. In an article written for the National Public Radio (NPR) an American media organisation, Morozov (2009) argues that hacktivism could be considered the "ideal type of activism for a lazy generation" proposing that due to the media fixation towards online social networking platforms; "every click of your mouse is almost guaranteed to receive immediate media attention" however. This oversimplification of online activism having little to no impact if not paired with traditional means of activism is applicable if we disregard the varying degree of

sophistication and complexity digital technologies and the Internet provide. For example, returning to George and Leidner (2019), in addressing slacktivism, and preferring to adopt the term '*clicktivism*', they identify clicktivism as the lowest classification within their digital activism hierarchy (see Figure 3.1 Digital Activism Classification (George and Leidner, 2019):91) amongst a range of digital spectator activities noting that, although an indicator of advocacy, clicktivism does not provide participant voice or their original views as it is noncommittal and impersonal as a means of activism (Kavada, 2015; Majchrzak et al., 2013). Albeit a low-level means of public engagement towards activism, clicktivism in large volume, can lead to a legitimate and actionable change in support of a particular cause.

Further, as the adoption of online technologies increases, Piat (2019:165) suggests that; "young people are creating new and more connections online – perhaps even international connections – we must understand that these are real relationships", reinforcing the concept of power in numbers as a stimulant towards social action and change, however. To return to the original portmanteau etymology of hacktivism, it should not be ignored that hacktivism is placed within the origin of hacker ethos from both practical and ideological practice.

3.4.2 The Emergence and Definition of Cyberterrorism

Efforts to achieve an academic consensus definition of cyberterrorism are difficult, and share parallels seen in earlier pursuits towards a consensus definition of terrorism. For

example, Hodgson and Tadros (2013) argued that the defining characteristics of terrorism can be subject to the observations of those who witness such events. So difficult and full of challenges these earlier pursuits towards a consensual definition of terrorism were, early academics jokingly referenced the search as a "quest for the Holy Grail" (Levitt, 1986). This "quest" to better define and more importantly understand terrorism within the academic literature, led to a vast array of research and methodologies engaged to provide clarity to a complex phenomenon, with these efforts drastically increasing post the events of 9/11 (Windle, 2018). Therefore, unsurprising, when met with the emerging concept of cyberterrorism, it is expected for such a potentially serious aspect of cybercrime to be equally contested.

When attempting to understand contradictions within reports of cybercrime, Wall (2008) acknowledges the existence of a mythology or series of myths about cyberspace and cybercrime. This mythological emergence can be viewed as the result of fictional misconceptions framing understandings of cybercrime, which in turn results in the reinforcement of public fears and anxieties towards current and emerging technologies (Wall, 2008). Notably, these public fears become further magnified as new avenues of technologies increase. For example, the *Internet of Things* (IoT) enabled devices to have become more prominent in the daily on-goings of our lives, increasing the likelihood of being targeted by cyberattacks. This increased adoption followed by more aggressive discourse adds further contradictions, and results in the establishing of an environment for fear to manifest itself. These manifestations, if left unresolved, can result in a cycle of

increasing anxiety towards newer technologies, feeding into perceptions of “what-if" scenarios of what cyberterrorism could entail.

As previously noted, observational myths, particularly prevalent in academic discussions of cyberterrorism, are evident in the widespread proliferation of fictional scenarios within the literature. Many scholarly works often initiate their discussions by citing Barry Collin’s (1997) introduction or “coining” of the term "cyberterrorism" (refer to Conway, 2002; Matusitz and Minei, 2009; Pollitt, 1998; Riglietti, 2016), a statement that may be subject to debate.

To navigate the array of conflicting and contested narratives present within the expanding collection of cyberterrorism literature, this section will not attempt to operate under a distinct individual definition, nor attempt to in-itself define one. Doing so may only introduce a further array of misconceptions and myths based on individual observation, of which is often promoted as a frequent issue within both terrorism (Hodgson and Tadros, 2013; Maskaliunaite, 2002) and cybercrime literature (Holt and Bossler, 2014). Therefore, to provide clarity, this chapter will comprise a review of the relevant literature exploring the concept of cyberterrorism. This will be achieved by firstly discussing the historical definitions of this social phenomenon followed by modern understanding of the specific activities and their various academic definitions presented, including the multitude of means adopted by “*cyberterrorists*.”

In effort to evaluate the current academic research concerning definitions of cyberterrorism, the formation of these definitions must first be discussed. Although

consensus on the concept of *cyber* within the context of communication technology is generally agreed to have been derived from the term "cyberspace" (see Iqbal, 2003; Kenney, 2015), a term ascribed to science fiction writer William Gibson in 1982, with this term later being shortened to the prefix cyber and referring largely to "online activity" (Iqbal, 2003:398) having network technologies noted as a necessity (Ottis and Lorents, 2010). The term "terrorism" understandably is not so readily defined or accepted (Hodgson and Tadros, 2013:494). Further, it is understandable that definitions are crucial in academic research as they help to clarify and operationalize the concepts being studied (Greene, 2017). Therefore, when exploring the array of proposed conceptual definitions of cyberterrorism, attention should be given to the formation of such definitions and the range of characteristics associated with them between both the "cyber" and its "terror" component.

As seen in the seminal article: *The future of cyberterrorism: Where the physical and virtual worlds converge*, Collin's (1997) who at the time was a senior research fellow at the Institute for Security and Intelligence in California (Conway, 2002; Pollitt, 1998) provides the first albeit brief predictions of imaginative scenarios. Collin proposes various scenarios of cyberterrorism ranging from the hacking of processing control systems for cereal manufacturers, to his most recognizable of possible cyberattacks against the next generation air traffic control systems. In these scenarios, Collin posits that systems in place to prevent such exploitations are compromised by unspecified hacking, resulting in large civilian aircraft colliding, albeit without any suggestions of how these events can occur (Collin, 1997). These hypothetical events add colour to Collin's otherwise meagre

definitional description of cyberterrorism as "the convergence of cybernetics and terrorism" (Luiijf, 2014:11).

These examples of cyberterrorism within Collin's testimony lack any recognition of risk assessment or oversight of the very systems targeted, something Pollitt (1998) was critical of Collin's predictions towards acts of cyberterrorism resulting in physical harm. Pollitt (1998), in conclusion to Collins stated scenarios of the risks of cyberterrorism noted that although there exists a serious risk within cyberspace, sufficient human involvement and oversight are in place, and that cyberterrorism does not at the time of their article. posed a significant risk in the classical sense (1998:10).

Extending from their earlier conclusion that cyberterrorism had yet to pose a risk, Pollitt's developed conception of the phenomenon is an aggregation derived from two primary sources, including Collin's (1997) perception of cyberspace, and the US Department of State's definition of terrorism.[2] Adopting these as a baseline interpretation, Pollitt developed the following operational definition:

> "*Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents*." (Pollitt, 1998:9)

[2] See Terrorism Report 1996 (FBI) available at: https://www.fbi.gov/file-repository/stats-services-publications-terror_96.pdf/view

At the time of Pollitt's composed operational definition of cyberterrorism, the concept of ICT being used to conduct violence against non-combatants was vague. An understandable but frequently ignored acknowledgment is that little was known about how ICT and the Internet would develop during earlier iterations of the service and the potential opportunities it would enable, however. Pollitt recognised that to define cyberterrorism sufficiently, it must exist within its own merits, separate from other forms of cybercrime such as *cyber-espionage* or *cyberbullying*. Therefore, adopting a narrow approach towards its definition.

Equally prominent and a frequently cited definition within cyberterrorism literature is that provided by Denning (2000a, originally presented in 1999) testimonial statement to the US House of Representatives.

> *"Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt*

nonessential services or that are mainly a costly nuisance would not." (Denning, 2000a:288)

In Denning's definition of cyberterrorism, the concept of violence attributed to cyber-based terrorism was present. Like Pollitt and later noted by Conway (2018), this definition is extremely narrow, with Conway arguing that Denning's conception of cyberterrorism renders "the target or consequences of an attack a determining feature alongside the required socio-political aim" (Conway, 2018:1), Denning primarily assumes that cyberterrorism must cause offline physical harm beyond that of information infrastructures, and despite growing research interest and increasing risk, it is unknown if cyberterrorism, unlike conventional terrorism, has yet to directly threaten life and limb, leading to very little attention being paid to the psychological and metaphysical effects cyberterrorism may have on civilians (Gross et al., 2017).

Although awash in ambiguity, since these foundation definitions had been conceived (Collins, 1997, Pollitt, 1998, and Denning, 2000a) the interest and desire to further conceptualise and define cyberterrorism can be seen to be tied to the growth of domestic use of the internet, itself, incurring a rapid adoption rate in the late 1990s and early 2000s. Throughout this period of adoption and increasing dependency on internet technologies, several predictive studies focusing on the potential risk of an 'information society' have emerged (Weimann, 2005). Admittedly, despite this interest in understanding and defining cyberterrorism, it can be noted that two notable issues arise (Jarvis and MacDonald, 2015:68-90). The first is what does cyber-terror refer to? Followed by; how cyberterrorism

compares to or differentiates itself from terrorism, or equally, other forms of online political behaviours, most notably digital-activism or hacktivism.

3.4.2.1 Conceptual Criticisms of Cyberterrorism

The term “cyberterrorism” is commonly employed to characterise various malicious activities leveraging digital technology and the internet to inflict harm or disrupt societal functions (Jarvis, Macdonald, and Whiting, 2016a; 2016b; Jarvis and Macdonald, 2015; Mayer Lux, 2018). However, the conceptual framework of cyberterrorism has faced considerable scrutiny (Conway, 2011a; 2011b, 2014a; 2014b), with critics highlighting its frequent usage in a manner that is vague, ambiguous, and lacking precision. A significant critique centres on the broad application of the term, encompassing a diverse array of activities that fail to distinguish it clearly from other forms of cyber-malicious activities (Akhgar et al., 2016; Jarvis and Macdonald, 2015; Mayer Lux, 2018; Plotnek and Slay, 2021). This criticism is inherent, as noted by Kenney (2015:112), who argues that cyberterrorism shares a common “genus” with other sophisticated cyber-malicious activities like cyberattacks, cyberwarfare, and online exploitation, leading to inevitable overlaps in their definitions.

Further difficulties concerning attempts to define cyberterrorism are due to the term being ambiguous. For example, the tag “cyberterrorist” can have a variety of subjective meanings ranging from “script-kiddies" blocking their school’s server to professional terrorists (Giacomello, 2004) and have little indication of the level of skill required to conduct such complex acts described. Those who apply the term cyber-terrorist often bolster this

ambiguity, due in part to the frequent exaggeration and sensationalism-based narrative of the threat of cyber-attacks. The media and policymakers may be inclined to label any high-profile cyber-attack as an act of cyberterrorism to generate headlines or justify increased security measures. This can lead to a distorted perception of the nature and scale of the threat, which may not be accurate or grounded in facts.

3.4.2.2 Rethinking Cyberterrorism

Given the history of academic research pertaining to cyberterrorism, and its referrals to various 'hollywoodised' depictions, there has been a growing recognition of the need to rethink our understanding of the phenomenon (Yannakogeorgos, 2014, Montasari, 2023:18). One such reasoning is the changing nature of the threat itself, and those with the resources to engage in acts described as cyberterrorism. In the past, highly sophisticated cyber-attacks were assumed to be carried out by nation-states or state-sponsored hackers due to the necessary resources needed to engage in such acts, often with the goal of collecting intelligence or disrupting the operations of their rivals (see Cherry, 2010; Hunter et al., 2022; Miller et al., 2021). Although much the same can be seen today, in recent years, as technology becomes increasingly accessible, there has been a shift in research interests towards smaller, more loosely organised groups of decentralised hackers and activists using internet technologies to conduct highly sophisticated attacks (Nurse and Bada, 2019). These hacker groups are often motivated by ideological, political, or social causes and may operate independently or in collaboration with other groups and states.

Further justification towards rethinking and challenging our academic understanding of cyberterrorism is the increasing complexity of the social and political context in which it occurs. The internet and other digital technologies have created new spaces for the expression of radical ideas and the recruitment of followers and has facilitated the spread of propaganda and misinformation (Holt, 2012). This has made it difficult to distinguish between genuine threats and less serious forms of online activity and has posed challenges for law enforcement and intelligence agencies trying to identify and disrupt terrorist networks.

Recognising this criticism and acknowledging the degree to which internet technologies are embedded in the actions of which a definition is applied, it is clear in Brunst's (2010) work that discussions concerning cyberterrorism needs to move away from ambitious descriptions of "digital Pearl Harbours" and "electronic Chernobyl's" (see Isenberg, 2000) which Brunst describes to only muddles efforts towards clear and precise terminology (2010:51).

To encourage distinction, Brunst (2010) discerns between two observational views of cyberterrorism as: *"broad"* and *"narrow"* definitions. Discussed originally by Foltz (2004), the concept of broad and narrow definitions would later be expanded on, with Brunst (2010) citing Pollitt (1998) to describe narrow definitions as being *o*ften worded close to common terrorism definitions and might be limited to politically motivated attacks against information systems and only if such attacks result in violence against noncombatant targets (Brunst, 2010:51). Brunst would later cite the National Conference

of State Legislatures, originally published in 2002 when describing broader approaches to cyberterrorism of, including:

> "*Other forms of terrorist use of the Internet and therefore, might define cyberterrorism as almost any use of information technology by terrorists"* (Brunst, 2010:51).

The recognition of a natural distinction between broad and narrow concepts of cyberterrorism can be seen in the early works of Gordon and Ford (2002). In describing the definition presented by Denning (2000a), Gordon and Ford note that Denning's definition was limited to attacks against "computers, networks, and the information stored therein", both of which Gordon and Ford define as 'pure Cyberterrorism' (2002:637). Two decades later, similar calls are still being made for such a distinction to be recognised (see: Jangada Correia, 2022). Attempts to develop distinctions between terrorism, cyber-enabled terrorism and 'pure' cyberterrorism has seen a recent uptake. This uptake often denotes the lack of consolidation and conceptual agreement amongst previous academic discussions (Akhgar et al., 2016) and lack of situational data as reasons (Conway, 2014).

Recent attempts to identify and define unique characteristics of cyberterrorism to distinguish the phenomenon from non-ICT concepts and the myriads of terrorism definitions can be seen in the work of Plotnek and Slay (2021). In their work, Jordan J. Plotnek and Jill Slay made use of an updated variation of a pre-existing taxonomy (Al Mazari et al., 2015), organising extracted keywords from a select group of pre-existing

definitions into defined categories (actors, motive, intent, means, effect, target) later concluding with the following definition:

> *"Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace to cause real-world consequences in order to induce fear or coerce civilian, government, or nongovernment targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychosocial, political, economic, ecological, or otherwise that occur outside of cyberspace."* (Plotnek and Slay, 2021).

Unlike earlier definitions such as the frequently cited definition proposed by Denning (2000a; 200b) discussed earlier, Plotnek and Slay's definition of cyberterrorism encapsulates broader impacts such as psychological impact, a concept explored extensively by Gross et al., (2017:55). In their paper, Gross et al., concluded that cyberterrorism has significant non-lethal impacts such as aggravation of anxiety, exacerbates perceptions of threat and personal insecurity, equally including significant economic impacts due in part to significant and intentional disruptions.

Another recent example of emerging and changing perspectives towards cyberterrorism, and one of significant importance in shaping this chapter, is that of Victoria Jangada Correia's (2022) taxonomic framework of terrorist activity. Itself, an extension of Smith's (2015) categorisation of "traditional" terrorist activity, incorporating a modified variation of McQuire and Dowling's (2013) binary description of cyber-enabled and cyber-

dependent crime. Understanding the field of terrorism studies is extensive and broad, the addition of "cyber" only broadens this field further, introducing new emerging threats and investigative pursuits to be challenged both within academic discourse and legislative drafting. Although having not originally included cyberterrorism, Jangada Correia (2022) adopts McQuire and Dowling's (2013) concept of cyber-enabled crime.

The concept of 'cyber-enabled crimes' can be defined as crimes that are increased in their scale or reach using computers, computer networks or other ICT, and unlike cyber-dependent crimes, can still be committed without the use of ICT. This allows for the compatibility of a defined concept of cyberterrorism to be incorporated alongside the United Kingdom's definition of Terrorism outlined in The Terrorism Act 2000. Jangada Correia, informing to have adopted key themes from definitions proposed by Foltz (2004), Holt (2012), and Plotnek and Slay (2021) proposed the following definition of cyberterrorism:

> *"Cyber terrorism encapsulates cyber enabled activity which intends to advance political, social, or religious ideologies against the public, and cyber dependent activity which further intends to threaten or facilitate damage against the public, properties, and/or systems. Cyber terrorism has the potential to coincide with traditional terrorism"* (Jangada Correia, 2022:83)

As can be seen, the above-mentioned definition incorporates both *cyber-enabled* and *cyber-dependent* elements, thus suggesting an inter-link between terrorism and

cyberterrorism. Although Jangada Correia admits the definition and its supporting framework are in their terms "generic," potential value can be gleaned from the latter presented framework. The proposed definition however, although potentially valuable for the intended context as being compatible with UK legislation as proposed by Jangada Correia, is, in this researcher's opinion, of limited use academically. The claimant and reference to the pursuit of the described "holy grail" is all but familiar and exhausted, with little gained for such pursuits beyond a collection of definitions only to be replaced by the next iteration of cyberterrorism and in per, hacktivism. Alternatively, the conceptual taxonomic framework presented by Jangada Correia (2022), itself a modified extension to Smith and Damphousse's *Flow Chart of Terrorist Group Activity* (Cothren et al., 2008; Smith and Damphousse, 2006) provides potential utility in further solidifying distinctions between cyber-enabled terrorism and cyber-dependent terrorism (alias; pure cyberterrorism) alongside key defining characteristics concerning the four presented classifications; recruitment, organisation and planning, preparatory conduct, and terrorist act).

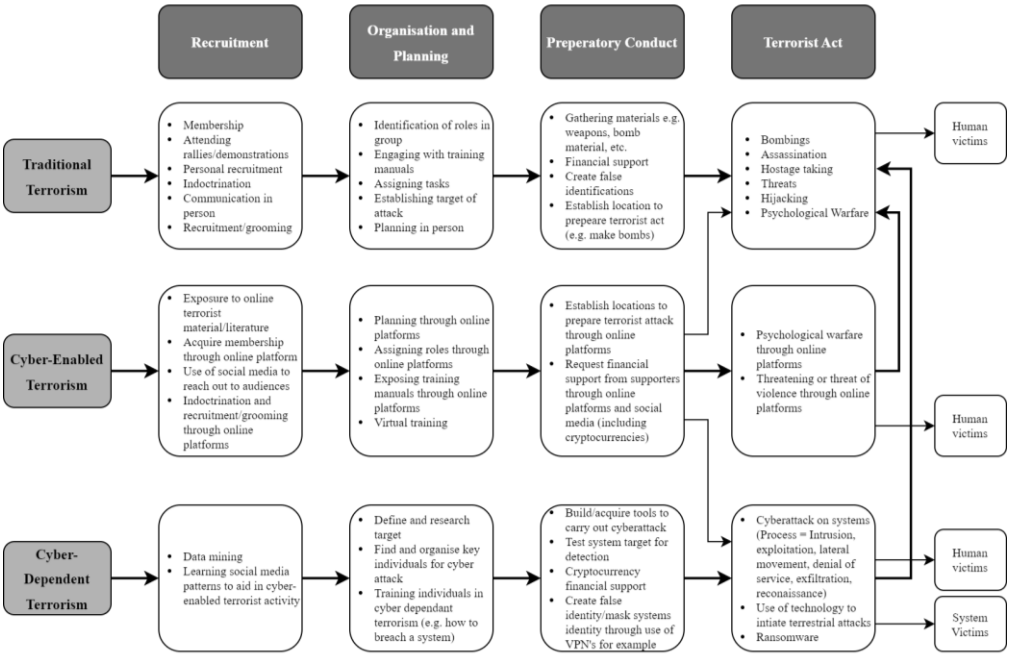


Figure 3.2 Terrorist Activity Framework (Jangada Correia, 2022)

By viewing existing research through the lens of cyber-enabled terrorism and cyber-dependent terrorism, a distinction can be better defined as compared to earlier calls for narrow and broad definition debates introduced earlier (see Foltz, 2004; Brunst, 2010). Therefore, to further explore distinctive characteristics, Jangada Correia's (2022) modified terrorist activity framework as illustrated in figure 3.2, which includes in *their* words; "traditional" terrorism, cyber-enabled terrorism, and cyber-dependent terrorism and will be discussed to further expand upon as distinct classifications of cyber-enabled terrorism and cyber-dependent terrorism further known as; cyberterrorism in which this thesis focuses upon. The exclusion of what Jangada Correia terms as "traditional" terrorism comes from the position that this thesis situates itself within a modern techno-centric perspective of ideologically motivated transgressive acts, and that establishing a dualism between "non-tech" and "tech" in present day does little to further our understandings, and

that similarly to Horgan and Boyle's (2008) argument against critical terrorism studies, only furthers such dualism. Instead, this section of the literature review explores the role of ICT, and in what capacity using Smith and Damphousse (2006) "Flow Chart of Terrorist Group Activity" by presenting the four classifications (recruitment, organisation and planning, preparatory conduct, and the act) to further discuss both phenomena within a modern techno-centric lens.

3.4.2.2.1 Cyber-enabled Terrorism

Although not specifically defined by Jangada Correia (2022), by taking McQuire and Dowling's (2013) concept of *cyber-enabled*, we can determine that cyber-enabled terrorism is the use of ICT to enhance or make easier the ability to engage in or support acts of terrorism. Therefore, network connected devices and their respective services are seen as additional, as opposed to being the main tactic or targetted focus of terrorist groups.

Recruitment

The scale, reach, and accessibility of ICT has allowed terrorist groups easier and more direct access to potential recruits. Extending their means of communication far beyond the scope of terrorism's more locally situated efforts (O'Shaughnessy and Baines, 2009), terrorist groups have adopted an increasing variety of interactive opportunities in which to engage with receptive individuals, and further indoctrinate susceptible listeners.

Observing the increasing adoption of ICT reliant mediums, Weimann (2016) notes that terrorist group recruitment makes significant use of various popular online social media

platforms to seek out and engage with potential recruits, with these platforms providing accessible means to host and share promotional and educational media such as literature, audio, and videos in support of their causes and goals (Just, 2015). Further, these media centric platforms by design encourage engagement, allowing members of terrorist groups to grow online communities and actively interact with potential recruits openly and in real-time (Saini and Bansal, 2021), providing answers and justifications to the various questions and intentions of those actively communicating with these groups, encouraging debate, and seducing listeners with their radicalised teachings and training for potential action in support of these groups (Weimann, 2016:80).

To better understand this evolution of recruitment seen in terrorism, Weimann (2016) adopted Daly and Gerwehr's: *Terrorist Selection and Recruitment model* (2006) to frame the recruitment of potential members using online technologies. The recruitment process for terrorist groups involves three stages: the net, the funnel, the infection, and the activation (Daly and Gerwehr, 2006; Weimann, 2016).

Starting in the "net" stage, targeted individuals are viewed as a homogeneous group, susceptible to recruitment with a uniform pitch (Daly and Gerwehr, 2006:76). Weimann (2016) suggests engaging the target population through online messages, videos, or lectures, using typical marketing practices to establish communication.

Later, the "funnel" represents the second stage, characterised by selection and refinement. Potential recruits undergo influence, education, and eventual radicalization, with doubters

or the unworthy culled (Daly and Gerwehr, 2006:77). Terrorism involves exchanges of religious or ideological material in remote online settings, exploiting social alienation and frustration (Weimann, 2016:82).

In the "infection" stage, dissatisfied individuals are directed to self-radicalise, with terrorist groups adopting agents to disseminate an "improvement narrative" (Daly and Gerwehr, 2006). Weimann (2016) highlights self-radicalization using online sources, gradually advancing commitment. Finally, the Activation stage involves releasing recruits for terrorist actions or joining on-foot fighters (Weimann, 2016:82). "Graduates" of such groups may further recruit or commit acts of terror, showcasing the group's capabilities (Weimann, 2016).

Organisation and Planning

As noted earlier, the concept of terrorism and *"new"* terrorism can be discerned by the geographical limitations often associated with earlier depictions of terrorism (see Field, 2009; Gofas, 2012). With "new" or more fittingly; "modern" terrorism adopting modern technologies, this limitation is mitigated by both improvements to infrastructure that allows for easier communication and travel, and online technologies such as the internet that permit the instantaneous exchange of information and resources. Additionally, the means and skills discussed concerning cyber-enabled terrorism and recruitment are equally transferable to the organising and planning of a terrorist attack.

For example, since 2003 the use of radicalised propaganda via the online magazine *Al-Battar* (the sharp-edged sword) has been frequently disseminated through online forums and private emails (Cohen-Almagor, 2017:60). This magazine served as an instructional guide, providing readers instructions on how best to manage weapons, create explosives including suicide vests, organize into cells, and other various practical skills needed to conduct a successful terrorist attack (Atwan, 2008). With this immediate access afforded by internet technology to specialised knowledge and guidance otherwise limited to those within the vicinity of established terrorist groups, individuals and groups could organise and plan more efficiently across a wider geographical range.

The use of knowledge and guidance shared online can also be seen used in the events of the July 7th London bombings and deaths of 56 people and injury of some 700 people. In preparation for the July 7th attack, Mohammad Sidique Khan, Shehzad Tanweer, Hasib Hussain and Jermaine Lindsay downloaded the instructions on how to build their bombs from the Internet (Hewitt, 2008). This adoption of Internet technologies was not isolated. In a 2017 article, Gill et al. (2017) provided a detailed account of online activities of 227 United Kingdom-based terrorist actors, covering the period from 1998 to 2013. Empirical findings from this study suggested that 54% of all cases used the Internet for learning, 44% for the spread of extremist online media, 32% for attack preparation (Gill et al., 2017). These findings illustrate an increasing trend in the use of online resources as they become more readily accessible.

Preparatory Conduct

The preparatory conduct seen within cyber-enabled terrorism goes unchanged from earlier understandings of terrorism, except for ICT allowing for such conduct to become more efficient and cost-effective. If we return to the previously mentioned similarities (nexus) between terrorist activity and that of organised crime, we can observe evidence suggesting that like cyber-enabled organised crime groups, cyber-enabled terrorist groups still need to rely on their established system of (offline) socio-economic opportunities for their criminal activities, with cyberspace mostly used in specific situations to facilitate communications and protect anonymity (Lavorgna, 2015; Leukfeldt and Yar, 2016), and also the procurement of operational funds, providing as noted by Carroll and Windle "a 'virtual bridge' across borders, allowing criminality to be conducted on a larger scale, at greater pace and with potential for greater return" (Carroll and Windle, 2018:287).

The adoption of encrypted communication platforms such as Signal, Wickr, and more familiar; WhatsApp and Telegram have facilitated the undetectable communication and exchange of information between terrorist groups, this technology increases the difficulty of identifying the originator, recipient, or content of Internet communications (UNODC, 2012:10). For example, in April 2016 the Islamic State released a 15-page guide titled "Sécurité Informatique" in its French online magazine *Dar al-Islam*, urging an increased adoption of ICT, and the importance of secure communications for the group (Hummel, 2016:23), however. The magazine notably recommended readers not to use the communication app Telegram. This occurred several months after the attacks on January 7th, 2015, in which the offices of the satirical newspaper *Charlie Hebdo* were attacked by

shooters identifying themselves as belonging to the Islamic terrorist group al-Qaeda. Investigators of the Paris attacks claimed to have found evidence the terrorists used the encrypted communications app Telegram to hide plotting for the attacks (Perez and Prokupecz, 2015),

The progression of financial services, and processes available on the internet has equally seen rapid development, and adoption by terrorist groups. Jacobson (2010:353) argues that terrorist groups have made 'extensive use of the Internet to raise and transfer funds' providing "broad reach, timely efficiency, as well as a certain degree of anonymity and security for donors and recipients" (see Carroll and Windle, 2018; Weimann, 2005).

The abundance of online payment facilitated by ICT makes it significantly easier and faster to transfer funds electronically between parties (UNODC, 2012:7). A notable increased attention can be seen towards understanding the transition and usage of cryptocurrencies by cyber-enabled terrorist groups (see Carroll and Windle, 2018; Juliadotter and Choo, 2015; Ibrahim, 2019; Majumder et al., 2019).

According to the Central Bank of Ireland, cryptocurrencies are a form of digital money. They allow for the exchange and payment of currencies (*cryptocoins*) like that of physical cash. However, unlike standard currencies that can be exchanged physically using notes and coins, cryptocurrencies are only exchanged electronically using lines of computer code. Cyber-enabled terrorist groups become incentivised to engage with cryptocurrencies due to the anonymity, and lack of strict national financial supervision (Wang and Zhu,

2021) associated with its decentralised design. However, cyber-enabled terrorists, akin to "non-cyber" terrorists, often require physical currency to be spent locally or physically sent to fund cells planning attacks in distant locations (Goldman et al., 2017).

It is more likely that cyber-enabled terrorists use methods associated with the procurement of finances like that of their non-cyber counterparts, albeit with the use of cyber, akin to other criminal groups that adopt cyber-based technologies to support their offline operations. For example, in their study of money laundering choices of organised crime offenders within the digital age, Kruisbergen et al. noted that in cases of offline crime, offenders exclusively used traditional methods of money laundering. They did note, however, that in the case of online drug trafficking via services such as the Silk Road, an online marketplace hosted within the darknet, bitcoins were used in the exchange of payment (Kruisbergen et al., 2019:576). The use of bitcoin is expected. The variety of established and emerging cryptocurrencies available is expansive, with bitcoin being notable for several reasons: 1) it is the most widely available and accepted within financial markets making the transaction between cryptocurrency to traditional currencies more seamless, and 2) the volatility of bitcoin in comparison to other cryptocurrencies are more predictable, meaning the loss of value can be less of a mitigating factor in its adoption.

Understanding that cyber-enabled terrorists require physical currency to adequately fund their offline operations, it can be assumed that the use of cyber-technologies for the accumulation of financial resources at the quantity necessary to fund these operations (Goldman et al., 2017). While also maintaining necessary anonymity, cyber-enabled

terrorism would be reserved to using legitimate transactions. For example, the use of online-markets or use of third-party services (eBay, Alibaba, Etsy) for the independent sale of real items, or ghost items, i.e., the selling of non-existing products for the intention of exchanging large sums of money. These legitimate markets allow for the acquisition of income without raising concerns of the service provider or policing agencies.

Offensive Action

Modern cases of terrorism provide ample examples of cyber use within terrorism. To reiterate earlier, cyber-enabled terrorism is the use of ICT to enhance or make easier the ability to engage in or support acts of terrorism. For example, according to an online questions and answers post by the United States Institute of Peace,[3] During the attack on September 11th, 2001, al-Qaeda operatives used the Internet to collect information such as flight times; to communicate reliably and in real time among themselves and with terrorist cells; and to share information and coordinate their attacks.

However, this usage falls under planning, and preparatory conduct, and not the offensive action. The offensive use of ICT to conduct an act of cyber-enabled terrorism is unclear. Research suggest that terrorist use of the internet has not included efforts where the internet has been directly attributed to bringing about physical violence (Henschke et al., 2021:72). Instead, as noted earlier, much of the use-cases of cyber-enabled terrorism have been largely 'supportive,' or to make 'easier' an act of terrorism. This observation doesn't mitigate the potential of cyber-enabled terrorism having an offensive act unique from

[3] See: United States Institute of Peace: Terror on the Internet: Questions and Answers, available at: https://www.usip.org/publications/terror-internet-questions-and-answers

terrorism beyond its more frequent and supportive role. Several scenarios inspired by key offensive events such as Stuxnet, have led to the suggestion that from the perspective of technical viability, an act of "cyberterrorism" is now a credible threat (Collins and McCombie, 2012:89), however.

As noted by Maura Conway, a frequent sceptic of the overapplication of the term cyberterrorism (see Conway, 2014a; 2014b, 2018), when applying a cost-benefit analysis to media interest concerning both the events of Stuxnet, and that of the 2013 Boston Marathon bombings, in which the attackers' following instructions published in the online Al-Qaeda magazine *Inspire*, manufacture two pressure cooker bombs (Winter, 2018).

The Boston Marathon Bombing took significantly less effort and financial cost. The attack also garnered more media coverage than Stuxnet (Conway, 2014a:12), suggesting that, although an event such as Stuxnet is *possible*, the use of ICT as a supportive element for terrorism remains the most favoured offensive tactic.

3.4.2.2.2 Cyber-Dependent Terrorism (Cyberterrorism)

The case for a cyber-dependent terrorism (hereafter, cyberterrorism) has been long debated, with frequent notable definitions amassed overtime to describe the phenomenon (see Clem et al., 2003; Collin, 1997; Conway, 2002; Denning, 2000a; Gordon and Ford, 2006; Holt, 2012; Matusitz, 2008; Pollitt, 1998). Briefly, the concept of a cyber-dependent terrorism denotes both the requirement of ICT as a primary tactic, but also as a limited and intentional target. Therefore, for the purpose of establishing distinction from the previously discussed *cyber-enabled* terrorism, this section adopts the narrow parameters established by Thomas

Rid in their article; *Cyberwar will not take place* (Rid, 2013). In his article, Rid describes that in the discussion of violence, a key factor associated with terrorism, software "code" differs from kinetic tactics. Unlike kinetic weapons such as firearms and bombs, code doesn't have its own force or energy, and that "even the most sophisticated cyberattack can only physically harm a human being by unleashing the violent potential that is embedded in that targeted system" (Rid, 2013:13).

The focused targeting of code as a defining factor of cyberterrorism provides a compatible distinction alongside cyber-enable terrorism's physical target focus that frequented past definitions of cyberterrorism (Denning, 2000a; Pollitt, 1998). This imposed limitation however does not suggest that outcomes of cyberterrorism are equally limited to effects on code. As Henschke et al., suggests, many elements associated with the increasing adoption of IoT (Internet of Things), provide a direct link between code and the physical world (Henschke et al., 2021). Physical objects are increasingly integrating cyber as to provide more convenient and interactive utility. Items such as cars, kitchen, and home utilities are increasingly adopting IoT connectivity, and although Henschke et al., dismisses Rid's premise that "code only acts on code" (Henschke et al., 2021:74), I challenge this in suggesting that code can only *target* code.

The targeting of a device such as those atypically seen in IoT environments must use a layer of translation that converts the code into a physical output, be it the unlocking of a door, or the disabling of safety gauges. Cyberterrorists in-of-itself cannot target the

physical object, but instead must first target the underlying operational code which controls that object.

In adopting a code-target-code approach, cyberterrorism can be more closely paired with understandings of cybercriminal networks, and its associated research. Thus, the preceding sections will, similarly to how cyber-enabled terrorism makes use of similarities shared across organised crime research, make use of cybercrime network research.

Recruitment

Much of the pre-existing literature pertaining to the recruitment of *cyberterrorists* share similarities from methods adopted in cyber-enabled terrorism (see Chen, 2014; Koehler, 2017; Saini and Bansal, 2021; Weimann, 2016; Weisburd et al., 2020), however. Much of this existing literature ignores recruitment of potential cyberterrorist actors that operate within a cyber-dependent environment.

Understanding cybercriminals overall is difficult. The absence of typical motivations and rationales associated with criminality is accentuated by the enhanced means of anonymity afforded with ICT (Ledingham and Mills, 2015). Further, operating or conducting nefarious acts within a cyber-dependent environment gives little reason for offenders to share physical locations or identifiable information. Considering that most research focusing on "*online convergence places*" adopted by cybercriminals tends to be non-theoretical and descriptive (Holt and Bossler, 2014), a lack of evidence-based

understandings towards the recruitment of cybercriminals makes inferring the recruitment process of cyberterrorism difficult.

What has been gleaned from numerous studies is the consensus that cybercriminal networks often contain core established and experienced members who may have pre-existing relationships and meet in either offline or online environments (Leukfeldt Kleemans, and Stol, 2017). This clustered social relationship is comparable to the *proximate-private* classification of the recruitment framework introduced by Daly and Gerwehr (2006) as discussed earlier in the recruitment process of cyber-enabled terrorist groups. In the proximate-private classification, core members engage with and evaluate potential recruits for membership within the group in a private and controlled environment. In the case of cyberterrorist recruitment, this may be the use of specific forums or private communication channels operated by core members. For example, the use of online forums and hosting of competitions to entice skilled individuals to participate in cybercrime activities has long been used as a means of recruitment within cybercriminal networks (see Digital Shadows, 2020).

The use of both offline and online forums for the recruitment and training of individuals within cybercriminal networks has been loosely discussed within the paradigm of ideologically motivated cyberattacks. In interviews with self-identified Turkish hackers, Holt et al., (2017) describes the ideological "mission" of several hackers as motivation to pursue meaningful targets, and train recruits familiar to the hacker for similar motivated purposes (Holt et al., 2017:224). The training of those familiar to the hacker is supported

by Leukfeldt et al., observations, in suggesting that social ties play a key role in the growth of cybercrime networks, and in finding suitable co-offenders (Leukfeldt, Lavorgna, and Kleemans, 2017:40). Those known to the hacker (*cyberterrorist*) may share similar ideological idealisms or be of a similar skill set. The recruitment of those known to core cybercrime network members offline may also have additional advantages over working with potentially unreliable online actors. As with the benefits afforded by ICT, actors may only be known by their online pseudonym (Nurse and Bada, 2019:9), suggesting that their affiliation and motivation to retain membership as being less rigid in comparison to offline relationships.

Organisation and Planning

Operating dependently online provides many opportunities and resources towards the organising and planning of a potential act of cyberterrorism, with one of the key draws for the adoption of ICT being the ease of communication and reach it provides. However, as noted by Connolly and Wall (2019) in discussion of the adoption of ransomware by online offenders, responses, and understandings of these technologies and their uses has been more technically focused (science) than 'non-technical' (social science). This lack of social understanding towards the organisation, and planning of cybercrime, although gaining significant traction within criminological research, is according to Leukfeldt, Lavorgna, and Kleemans., (2017), theoretically thin and not fully developed. Dishearteningly, Koops (2010), citing McCusker (2006) and Van der Hulst & Neve (2008) asserts that the lack of cited evidence to support these understandings 'quickly transform into hearsay and anecdote which are in turn recycled within other authors' assertions concerning

cybercriminal activity' (Koops, 2010:744), and as of recent, these conditions have seen little change.

To gain a brief perspective towards understanding of cybercrime groups such as cyberterrorists, researchers (see Donalds and Osei-Bryson, 2019; Leukfeldt, Lavorgna, and Kleemans 2017; Nurse and Bada, 2019; Von Lampe, 2015) make frequent use of Choo's (2008) typology of cybercrime groups. Within Choo's typology, groups engaged in *cyber-criminality* are defined briefly into three distinct categories:

Table 3.1 Typology of Cybercrime Groups (Choo, 2008)

	Description	**Example**
Type One	Consists of organised criminals who take advantage of cyberspace and technology to enhance their offline criminal behaviours.	Illegal online marketplaces involved in; drug trafficking; human trafficking; and similar
Type Two	Involves organised cybercriminal groups, such as underground credit card fraud groups or underground phishing groups who only operate online.	Online phishing, Ransomware, markets for the sale and distribution of illicit exploitation material.
Type Three	Comprises ideological and politically motivated organised cyber groups, including terrorists and hacktivists.	Defacing of websites, DDoS attacks, Dissemination of Propaganda.

Notably, the first two categories (type one, type two) represent clear distinctions between the enabled and dependent forms of cybercrime. For example, although methods such as the use of ransomware can be easily compared to its offline counterpart, the use, and target of ransomware can only exist within a cyber-based platform targeting code. In commentary

of the last category (type 3), Choo characterises such groups as those adopting characteristics seen in both type one and type two categories; ICT as an enabler, and ICT as the object of offending (Choo, 2008, pp. 283–286). If we are to focus on groups operating within cyber-dependency (type two), then Nurse and Bada (2019:5) echo Choo's suggestion that the internet acts as a centralised enabler for decentralised group members to organise and plan potential activities. Thus, most communication and planning methods amongst cybercriminal networks can be considered like typical privacy-focused online communications used by the general populations and corporate organisations.

As mentioned earlier, members within cybercriminal networks often receive training from more knowledgeable and experienced members (Holt et al., 2017), or alternatively may introduce new techniques within the group. Knowledge requisition and skill training within cybercriminal networks is open, and easily accessible. Introductions and advanced guides on hacking network infrastructure, computer systems, or distribution of various forms of malware has become an economic market, and readily available online as both paid and free courses. For example, a search of available online courses on the topic of 'hacking' within the Udemy online learning platform reveals nearly 6,800 available courses. The most popular course: '*Learn Ethical Hacking from Scratch*' costing €85 has had over 500,000 students enrolled.

Further, more internal guides or more appropriate; "crime scripts" (see Cornish, 1994) leaked from cybercrime networks have allowed for a better understanding into the training and operational methodology of cyber-dependant criminal groups. In August 2021, an

affiliate of the hacker group known as Conti (alias Wizard Spider) known for the ransomware attack on Ireland's Health Service Executive (HSE), leaked training information including a manual on deploying its tools and various help documents (Kupchik, 2022). The drafting and use of an operations manual containing the tactics and technologies used by groups such as Conti illustrates an organisational structure typically seen within the software development and web services sector.

Preparatory Conduct

The preparatory conduct of cyber-dependant criminal networks can be considered to stray from previously established understandings that often place cybercrime within a cyber-enabled perspective. As previously discussed, traditional means and connections to offline criminality are used to fund and support online criminal behaviours and acts, with cyber taking a more supportive role (Goldman et al., 2017). The distinction of a cyber-dependant model can be seen in the increased scale of ransomware attacks. Ransomware is a subset of malware (i.e. malicious software) that prevents or limits users from accessing their system and/or data until a ransom is paid (Connolly and Wall, 2019). The use of ransomware introduces a new, more secure, and easily deployable means of illegal monetary theft to support further criminal activities. Events, such as those seen in May 2017 in the case of the WannaCry ransomware attack, illustrate the scale and speed ransomware can disrupt and force victims to deposit currency directly into the criminal group's accounts.

Emerging on May 12, 2017, the WannaCry ransomware attack was unprecedented in scale, quickly impacting a quarter-million computers in over 150 countries (Trautman and Ormerod, 2018). The impact of such an attack was significant, both on a financial scale, but also societal. For example, although not directly targeting health services, due to the indiscriminate spread of the malware, almost 7000 NHS outpatient appointments were cancelled, with urgent care for at least 139 patients being delayed (Martin et al., 2018). Financially, ransomware is lucrative. Although reports suggest that WannaCry accumulated no more than around $386,905 in bitcoin (see WebTitan, 2020), CNBC report that according to a 2021 federal report, US Banks Reported having processed $1 billion in ransomware payments (Cox, 2022), triple what was processed the year prior. As mentioned earlier, the adoption of ransomware as a means for cyber-dependant groups to acquire funding provides a bleeding effect; when indiscriminately deployed, ransomware can continue spreading onto unprotected systems indefinitely (Goodchild, 2022; Palmer, 2019). This bleeding effect allows successful ransomware attacks to collect additional funds for cyber-dependent crime groups long after its peak effect stage.

Discussed earlier, the leaked guide developed by hacker group Conti provides insight into operation and targeting methods adopted by cyber-dependent criminal networks. For example, the use of web crawlers, phishing emails and port scanners are used to automatically conduct reconnaissance of potential targets, allowing for groups to better plan and execute a cyberattack (Kupchik, 2022). This reconnaissance is further complemented by the availability of *Ransomware as a Service* (RaaS), making the adoption

of cyber-dependent malicious software, skilled operatives, and tactics accessible even to non-technical criminal groups (Meland, Bayoumy, and Sindre, 2020).

Offensive Act

The offensive action of cyberterrorism is difficult to gauge, due in part to the inability or confusion in constituting exactly what defines cyberterrorism from both academic and legal paradigms. If we adopt cyber-dependency as a key defining factor then evidently, the actions which constitute an act of cyberterrorism from other cyber-dependant crimes become blurred. As with cyber-enabled terrorism, acts often associated with organised crime are frequently adopted by terrorist groups as a means of securing finances (Goldman et al., 2017; Kruisbergen et al., 2019; Windle, 2018).

Arguments often seen within terrorism become opaque when placed within a cyber-dependent environment. A notable argument is the use of indiscriminate terrorism conducted against civilians (see Goodwin, 2005; Homolar and Rodríguez-Merino, 2019; Kalyvas, 2004) is a frequent factor of terrorism. As mentioned in the case of WannaCry ransomware attack, the indiscriminate deployment of malware is a regularly adopted tactic by cyber-dependant criminal groups.[4] Due to the decentralised structure of ICT, the indiscriminate targeting of civilians isolated within a specific region, like those of terrorism, is difficult.

[4] See North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, available at: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Further, the use of spectacle and the self-identification of action, a necessity to bring attention to a terrorist group's cause (Cowen, 2006; Hoffman, 1999), is typically adopted by cybercrime networks as to establish prestige and legitimacy in their actions (Seebruck, 2015). These characteristics, when viewed within a cyber-dependent environment, do little to distinguish cyberterrorism from other cyber-dependent crimes.

To provide distinction, Hosford (2021) modified a pre-existing typological model of hacker types (see Rogers, 2006; Seebruck, 2015) to include cyberterrorism as a unique form of hacking. In this model, four categories were defined for cyberterrorism; prestige, profit, ideology, and revenge, of which when paired, distinguishes cyberterrorists as a unique group of hackers.

Table 3.2 Key Classifications of Cyberterrorism

Category	**Description**	**Degree**
Ideology	Adopted ideologies can be social, religious, political, or a mixture of each like offline-terrorism, and used as moral framework to legitimise the targeting of those deemed a threat to their existing ideology (Drake, 2007; Hosford, 2021)	4
Profit	Often borrowing techniques similarly seen within non-cybercrimes (Carroll and Windle, 2018; Windle, 2018) albeit cyber-dependent such as spam, sale of illicit content, ransomware (including Ransomware as a Service; RaaS)	3
Revenge	Motivated to function as a sense of moral or ideological responsibility in avenging a perceived injustice experienced by the attacker and their community.	2
Prestige	Relying on prestige to amplify and legitimise their goals, cyberterrorists exploit the theatre and spectacle to make their actions known (Cowen, 2006)	1

Notably, *ideology* was the main contributing category in setting apart cyberterrorists from other groups, with *profit* and *revenge* distinguishing cyberterrorists further from *hacktivists* and *cyber warriors* who also share ideology as their primary category. In adopting Hosford's (2021) characterised criteria of cyberterrorists, some clarity can be gained in exploring cyber-dependent attacks as potential examples of cyberterrorism.

Identifying offensive acts that adopt motivational factors such as ideology, profit, revenge, and prestige is common, with notable cyberattacks motivated by personal belief systems such as ideology, and revenge frequent. For example, in response to filming and marketing of the then unreleased film "*The Interview*", a comedy about a plot to assassinate North Korean leader Kim Jung-un, an online group identifying itself as "Guardians of Peace" leaked a release of confidential data from the film studio Sony Pictures Entertainment (see Zetter, 2014). In their attack, the group gained access to servers operated by Sony Pictures, harvesting data including personal information concerning employees and their families, employee emails and salaries, and copies of then-unreleased films, scripts, and plans for future films (Sullivan, 2015). In response to threats of terrorism if the film was to be released by Guardians of Peace, Sony Pictures removed the film from its Christmas holiday premier, a move strongly criticised by then President Barack Obama,[5] with some members of the US congress calling the hack an act of cyberterrorism (Wilson, 2015).

[5] See: Remarks by the President in Year-End Press Conference, The White House (Dec. 19, 2014), at https:// www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

Further acts of perceived injustice, revenge, and ideology have also contributed to the operation of cyberattacks. For example, in February 2022, Mykhailo Fedorov, Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine requested[6] those with the technical expertise aid in an "IT Army" and target select Russian websites and online services using DDOS attacks in support of Ukrainian efforts (Sattler, 2022). Further, pro-Russian support has been declared by established cybercriminal groups such as Conti has internally declared support for the Russian government with calls to target Ukrainian infrastructure (Kupchik, 2022).

3.5 Conclusion

To conclude, the epistemological understanding of hacking and cybercrime has shifted significantly over the past decades. The evolution of hacking and those who 'hack' as discussed in this chapter, included an extensive list of intricate motivations, ideologies, and behaviours. From its more mundane expression of creativity (Levy, 2010) and pursuit of knowledge discovery to extraordinarily complex and targeted attacks (Jordan and Taylor, 2004) which have resulted in a wide spectrum of opinions and literature of what hacking exactly is, including the true intentions of hackers. This critical view acknowledges the limitations of earlier classifications and technocentric research, shifting focus towards the importance of examining the complexities of hacker motivations and behaviours. Later, different approaches to understanding cybercrime are scrutinised, noting the challenges in arriving at a universally agreed definition. Various perspectives are considered, including

[6] See: Tweet from Mykhailo Fedorov; shorturl.at/dgE04

those focusing on the cyber element, types of cyberattacks, and the need for more robust empirical data.

The chapter, emphasising the importance of specialised holistic studies within the domain of cybercrime research, transitions to explore the intricate landscape of hacktivism and cyberterrorism, an essential aspect lies in comprehending the ideologically motivated ties that drive hackers to make actionable decisions (Landreth, 1985; Hollinger and Lanza-Kaduce, 1988; Rogers, 2006; Seebruck, 2015). As noted, there is a growing recognition among scholars regarding the need to further expand on the ideological motivations behind hackers' actions, moving beyond the earlier limited perspectives that associated hacker motivations with financial and informational gains (Holt et al., 2017a; Holt et al., 2020). This acknowledgment underscores the necessity for a more robust and structured understanding of the intricate interplay between hackers and their ideological foundations.

The concept of ideology, complex and operationally challenging to define, emerges as a critical factor shaping hackers' motivations and actions (Fine and Sandstrom, 1993; Malešević, 2006). Within the context of hacking and ICT, ideologies function as belief systems crafting rational resolutions for social and political issues. The discontent stemming from differentially privileged interactions within the hacking community can lead to the formation of antagonistic groups.

Academic research on hacktivism is expansive, exploring not only ideological identities and vigilantism but also revealing challenges in consolidating diverse opinions. Scholars

such as Dahan (2013), Goode (2015), and Klein (2015) delve into the complexities of hacktivism, highlighting its contentious nature amid the ever-evolving technological landscape. To unify perspectives, innovative frameworks, like Karagiannopoulos's (2018a) generational approach, align hacktivism with distinct technological eras. This resonates with the work of George and Leidner (2019), positioning hacktivism within a sophisticated hierarchy of digital activism, classifying it as a form of digital gladiatorial activity that changes alongside the level of sophistication taken by actors.

In parallel, the discourse on cyberterrorism seeks to address the longstanding vagueness and mythologies surrounding its definition (Wall, 2008). Scarcity of empirical findings, noted by Akhgar et al. (2016) and Conway (2011a; 2011b, 2007), has contributed to misconceptions, as evident in ambitious descriptors like "digital Pearl Harbours" and "electronic Chernobyl" (Brunst, 2010).

In summary, ideologically motivated hacking such as hacktivism and cyberterrorism, while distinct, share a common reliance on cyber-dependent tactics. Hacktivism, as a facet of digital activism, manifests a spectrum of skills and motivations, with ongoing efforts to categorise these traits within evolving technological paradigms. In contrast, cyberterrorism emerges as an umbrella term encapsulating malicious cyber-dependent activities designed to coerce targets. As the landscape continually evolves, a nuanced understanding of the technologies, motivations, and effects associated with these phenomena becomes increasingly imperative. Subsequent chapters of this thesis aim to deepen this understanding through bibliometric analysis and the cataloguing of key definitions,

providing a quantitative exploration of the methods employed by hacktivists and cyberterrorists.

Chapter 4. Methodology

4.1 Introduction

As noted earlier (see Section 4.3 The Emergence and Definition of Hacktivism:73), despite the growing body of academic research of both cyberterrorism and hacktivism, a consensus on these topics remains elusive (Brunst 2010; Holt et al., 2020; Jangada Correia, 2022; Kenney, 2015). This lack of agreement and ambiguity in understanding unique factors differentiating both phenomena potentially limits the production of new research and fostering of fresh perspectives. Earlier comparison was tied closely to similar domains, more notably the review of a then emerging field of terrorism studies by Silke (2001). Since then, the field of contemporary terrorism studies has seen a significant reaction post event of September 11th 2001. Such identified example is the overconcentration of research focused on Islamic terrorism, with a later study by Schuurman (2019) reiterating the reactionary behaviour of researchers within the field focusing largely on Jihadi terrorism and Al Qaeda. Ahmed and Lynch (2021) further confirmed this finding, positing that the success and frequency of acts of terrorism by groups such as Al Qaeda understandably influence research focus, of which is evident by the volume of literature focusing on the Far-Right during these periods being significantly lower in comparison (Ahmed and Lynch, 2021:2).

While studies associated with Islamic terrorism gained significant prominence and widespread attention in the aftermath of September 11th (Haghani et al., 2022:20), it is noteworthy to recognise that research on cyberterrorism and hacktivism also emerged

contemporaneously, often alongside contemporary terrorism studies, however. Despite sharing a temporal origin, both fields of inquiry diverged in focus and discourse within the academic domain, with an unequal level of focused prominence during this period, which makes discerning key academic understandings of both cyberterrorism and hacktivism difficult.

Returning to the research questions of this thesis, the research project expands understandings of the research domain by answering the following questions:

1. *How has the academic development of cyberterrorism and hacktivism research evolved over time.*
2. *What distinct, key definitional characteristics have emerged for both phenomena.*

This study, does not attempt to achieve a consensus definition of either cyberterrorism or hacktivism, but instead focuses on mapping the academic development of cyberterrorism and hacktivism research through researcher outputs, interpretations, and definitions; for this, a mixed-methodological approach is employed to achieve the following objectives:

1. Trace and evaluate the academic development and status of cyberterrorism and hacktivism through analysis of high-impact journal articles.
2. Identify key themes and distinctions within the academic literature and explore definitions of cyberterrorism and hacktivism using content analysis.

3. Recognize challenges in cyberterrorism and hacktivism research and suggest possible solutions to tackle these issues.

To answer the research questions and objectives, this study employs a mixed-methods approach, of which Creswell (2009) defines as a philosophically underpinned model of inquiry that integrates both qualitative and quantitative research approaches. The first method adopted in this study is bibliometric analysis (Donthu et al., 2021:287), of which is used to evaluate publication performance, and map the evolution of cyberterrorism and hacktivism research output, identifying crucial contributors, literature, journals, and academic definitions.

The second method, a taxonomic content analysis, is conducted to highlight recurring terms and concepts in the definitions of cyberterrorism and hacktivism, enabling a comprehensive comparative analysis (Al Mazari et al., 2015; Krippendorff, 2018; Plotnek and Slay, 2021). Taxonomies offer a valuable solution by providing linear classifications, thus establishing a common language for discussing these phenomena (Donalds and Osei-Bryson, 2019:415).

By integrating the empirical findings from both the bibliometric and quantitative content analysis into a taxonomic framework, this project seeks to provide valuable insights into the domain of cyberterrorism and hacktivism research, contributing to a clearer understanding of these complex phenomena and facilitating the classification and analysis of these phenomena for further research. Thus, for the purpose of this research project, mixed methods represent a philosophically oriented pragmatic research design that

embraces and integrates both quantitative and qualitative approaches to address the research objectives effectively (Jick, 1979). Further, subsequent sections will discuss justification and rationale towards this methodological structure.

4.1.1 Research Design and Methodological Justification

The methodological structure of this study follows a modified variation of the 'Triangulation Design: Data Transformation Model' proposed by Creswell and Plano Clark (2007:77). Triangulation, as a research design, aims to enhance the validity and reliability of research findings by combining multiple methods, data sources, and perspectives.

The decision to adopt the Triangulation Design: Data Transformation Model for this research project is grounded in several beneficial and practical considerations. Firstly, it enables the exploration and understanding of the research topic through a thorough literature review prior to data collection and analysis. This literature review allows the researcher to identify potential concepts for further analysis. For instance, the literature reviewed within this project frequently refers to the lack of empirical evidence-based research (Bossler and Berenblum; 2019) and the absence of a consensus on the definitions of cyberterrorism and hacktivism within academic literature (see Conway, 2011a, 2007; Jarvis and Macdonald, 2015; Macdonald et al., 2019) as significant issues within the research domain. This mercurial state has made it challenging to clearly distinguish these social phenomena as distinct fields separated from the broader domain of terrorism

studies. These circumstances are not unique to this research project, as similar observations were made by Von Lampe (2003) in his work on organised crime research. The initial qualitative review of the literature, therefore, aids the researcher in identifying a diverse range of research topics and addresses how individuals frame their understanding around a specific event or phenomenon, as suggested by Mihas (2019:3).

Furthermore, justification for the adopted methodological approach comes from review of existing literature which has frequently mentioned the necessity to comprehensively explore the current state of cyberterrorism and hacktivism research, with a focus on assessing both its strengths and weaknesses (see Landreth, 1985; Hollinger and Lanza-Kaduce, 1988; Rogers, 2006; Seebruck, 2015). This rationale draws a notable comparison to the field of terrorism studies, where Silke (2008) raised notable concerns regarding the research community's size, and limited constraints on data collection and analysis (Silke, 2004).

To address these considerations, the research project adopts a regression-based approach towards the identification of correlations and discrepancies within measurable variables related to cyberterrorism and hacktivism research, thereby providing essential data for interpretation. Through established quantitative methods, the concepts and health of the academic research field can be empirically mapped and catalogued along a time-linear overview.

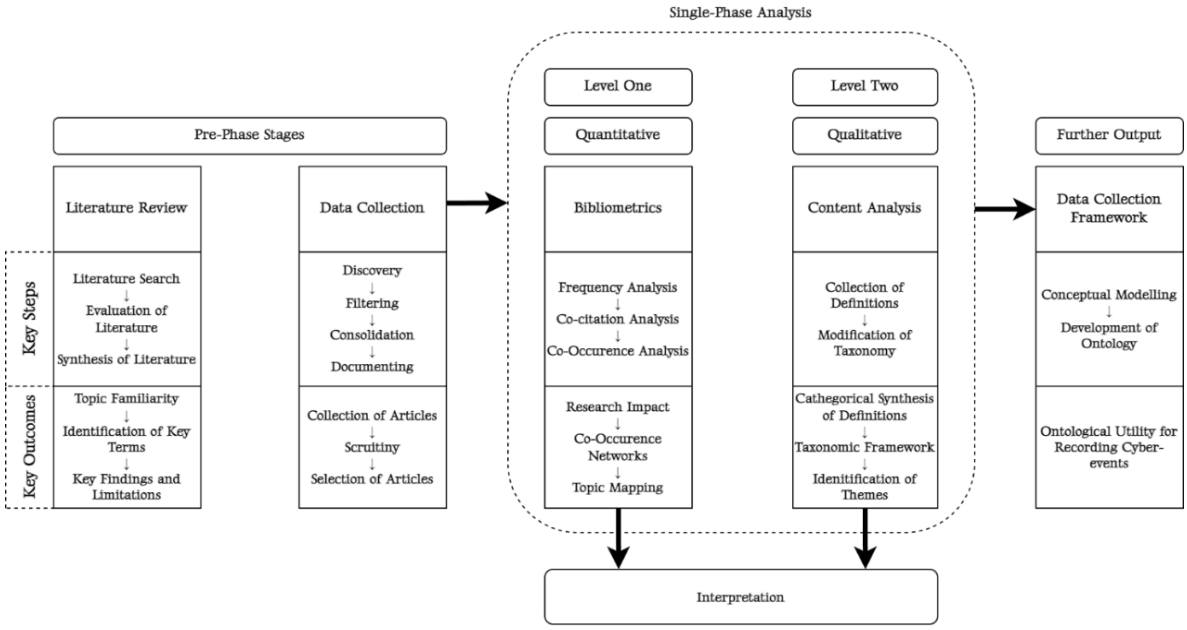


Figure 4.1 Single-Phase Triangulation Multilevel Research Design Structure

Illustrated in figure 4.1, the research project employs a modified single-phase multilevel triangulation approach (Tashakkori and Teddlie, 1998). This approach involves a series of key steps at each level of analysis, building upon the previous process. As highlighted by Creswell and Plano Clark, a multilevel triangulation approach makes use of diverse methodological approaches to address various levels of analysis within a single system (2007:153). In this context, the single system refers to the topic of analysis, specifically academic understandings of cyberterrorism and hacktivism research outputs.

The figure depicts the research project's structure, indicating that the literature review provides the foundational understanding and knowledge necessary to determine the required data for analysis and the research methods (known as the pre-phase). The single-phase analysis, indicated by dotted lines, consists of two levels: (i) the quantitative

bibliometric analysis on article output, and (ii) the quantitative content analysis on qualitative definitions of cyberterrorism and hacktivism. Data collected during the initial data collection phase is fed into the single-phase analysis, processed using their respective methodologies, and later merged for the interpretation of key findings. The following sections of this chapter will provide further details of the pre-phase data collection, and methodologies at each level of the single phase.

4.2 Pre-Phase Data Collection

The widespread adoption of the internet as a primary means of accessing scientific literature has led to an expansion of services that provide accumulative access to such literature. While this has opened scientific literature to a much larger and diverse audience, of which is of significant benefit of this study and its use of bibliometrics, it has also resulted in what can be considered an information overload (Roetzel, 2019) when it comes to identifying relevant literature of a consistent quality for analysis.

Roetzel (2019) defines information overload as the situation where decision-makers face a level of information that exceeds their information processing capacity. Shenk aptly describes this phenomenon as "data smog," or the "muck and druck of the information age" referring to the overwhelming and suffocating abundance of *information* accessible to researchers (Shenk, 1997:31). This data smog makes it increasingly difficult to sift through and identify pertinent scholarly publications for research and decision-making purposes.

Bibliometrics, as a means of quantitatively analysing scholarly publications, has been adapted to manage such copious quantities of bibliographic data. Software packages such as VosViewer (van Eck and Waltman, 2014), and Bibliometrix (Aria and Cuccurullo, 2017) which allow for the analysis of thousands of articles bibliographic details with relative ease and has seen increased adoption in more recent crime related research (see Bahoo et al., 2021; Luong, 2023; Unlu and Gurer, 2022), however. Most studies do not extend this analysis beyond surface level and limited overview of the publication's bibliographic details.

To address these limitations, PRISMA guidelines proposed by Page et al. (2023). Originally intended as a framework for Systematic and Meta-Analyses, PRISMA or "*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*," has been extended to provide guidance on conducting and reporting alternative studies such as scoping reviews (see Munn et.al, 2018), and has seen adoption for the collection of literature intended for bibliometric analysis (Maier et al., 2020). Such uses and adaptations of PRISMA aim to map the existing literature of a particular domain of study by assessing the volume, nature, and characteristics of the research available (Arksey and O'Malley, 2005). This feature of PRISMA is of particular use when the topic has not yet been extensively reviewed (Arksey and O'Malley, 2005:21), thus making its adoption suitable for the study of cyberterrorism and hacktivism research.

According to Page et al. (2023:337), the PRISMA approach indicates four phases in identifying and extracting the data for analysis; identification, screening, eligibility, and inclusion.

- **Identification**: Begins with the total number of records identified through one or more database searching, using the search criteria, and removal of duplicate entries.
- **Screening**: Involves the screening of titles and abstracts to identify relevant studies, and any necessary refinement.
- **Eligibility**: The records are reviewed in detail, and reasons defined for excluding studies at the full-text screening stage.
- **Inclusion**: The number of studies that met the eligibility criteria are specified for further analysis.

For this research project, the PRISMA data collection procedure is extended by facilitating a comparative approach to data collection, incorporating publications not only from third-party academic search engines (Scopus, Web of Science, BASE, JSTOR) of which are frequently used in bibliometric analysis and systematic reviews, but benefiting further from the inclusion of results identified directly from academic publishers (Sage, Taylor and Francis, Springer) through their respective services.

To discuss, the identification procedure of this section is divided into its two sources; 1. Academic search engines, and 2. Academic publishers with both using the same search criteria:

- Article Abstract, Title, or Keywords must include either cyberterrorism, hacktivism, or both.
- Articles must be sourced from peer-reviewed journals.
- Articles published between the years 1999 and 2021.
- Articles must be written entirely in English.

The provided criteria were adapted for Boolean searching and used to identify articles in the additional chosen databases and publisher repositories to ensure the later searches were as close to similarity as possible. For simplicity, the above identifies literature defined as "articles" for their availability within peer-reviewed journals, using the keywords: "cyberterrorism," "cyber-terrorism," "cyber terrorism," "hacktivism" within the title, abstract, and author keywords. A temporal range of peer-reviewed articles from 2000 to 2020 was chosen to capture any potential 'paradigm shifts' (see Kuhn, 1970; 1977) within the academic domain, and map the conceptual evolution of cyberterrorism and hacktivism over a significant period.

4.2.1 Literature Discovery by Academic Search Engines

A common approach to accumulate literature for scientific research is using third-party academic search engine providers such as Google Scholar, Scopus, and similar. In this study, seven academic search engines were initially identified based on the researchers'

own experience and popularity of these engines for researchers (Gusenbauer, 2019). These databases include Bielefeld Academic Search Engine (BASE), Google Scholar (GS), Scopus, Web of Science (WoS), JSTOR, Semantic Scholar, and Microsoft Academic (MS). The use of multiple academic search engines ensures a broader scope of scholarly coverage, increasing the chances of capturing relevant and authoritative articles for analysis.

During the literature review process, keywords and associated aliases (cyberterrorism, cyber-terrorism, cyber terrorism, hacktivism) relevant to the research were identified and used to do a broad search of the literature published between the years 2000 and 2020 in the previously mentioned academic search engines, providing a rough overview of the available literature for analysis:

Table 4.1 Academic Search Engine Results

Term	BASE	Google Scholar	Scopus	WoS	JSTOR	Semantic	Microsoft Academic
Cyberterrorism	1426	19800	216	195	650	2690	352
Hacktivism	457	7440	176	137	410	2020	205

As presented in Table 4.1, there are considerable variations in the number of available results generated by each search engine. These differences are due to the distinct methods used by these providers to process and catalogue scholarly information. Notably, Google Scholar (GS) stands out with significantly higher results compared to other search engines.

The higher the number of results in Google Scholar is a product of its web-crawling based algorithm, which retrieves academic literature from various sources, including journal websites, universities, and academics' personal websites (de Winter, Zadpoor, and Dodou, 2014). This approach, although contributing to many search results, can suffer from what some experts (Brophy and Bawden, 2005:499) identify as "infobesity" (Bell, 2004). This refers to the overwhelming abundance of information that may be less focused or relevant to the research question making the discerning of topical information difficult. A benefit of this approach, of which is later used to aid in identifying and filtering high-impact articles, is Google Scholar's citation score, which provides a general reflection of the cited impact of a scholarly article by identifying connections to a diverse array of sites, people, and objects linked by others (Wood et al., 1994:3).

4.2.1.1 Database Selection

The combined collection of literature from the general search of keywords exceeds 35,000 scholarly articles. Although as earlier mentioned, bibliometrics practices can readily analyse datasets in the thousands, these analyses are limited to articles bibliographic content, and not content topical for further analysis such as definitions and contextual interpretations. To mitigate the effects of the earlier mentioned "infobesity" when using academic search engines, a set of requirements for the search criteria was implemented. These requirements are based on three essential criteria intended to validate the literature as suitable for analysis: (i) adequate indexing of academic articles, (ii) accurate and

sufficient bibliographical information, and (iii) the use of a pre-inclusion review and editorial-like standards.

Adequate Indexing of Academic Articles: The selected search engine must index relevant peer-reviewed journal articles pertaining to the field of research, spanning across various publishers. This ensures that a comprehensive representation of the available literature is included in the search results.

Accurate and Sufficient Bibliographical Information: The indexed search results must provide accurate and comprehensive bibliographical information about the retrieved articles. This includes mandatory details such as author names, abstracts, keywords, publishers, and cited bibliography necessary for the bibliometric analysis.

Manual Review: To ensure the articles used for further bibliometric and content analysis were accurately identified as topic peer-reviewed journal articles, a degree of manual oversight is essential.[7] This process involves the search providers to manually review the submitted article in order to validate its quality and accuracy to the information provided via search results.

By adhering to these requirements, the research project aims to build a curated and high-quality dataset of peer-reviewed academic articles for analysis. By carefully filtering the

[7] An example of such editorial-like standards is available via Elsevier's 'Content policy and selection' at https://www.elsevier.com/products/scopus/content/content-policy-and-selection

literature, this research project can focus on relevant and credible sources that meet the specific criteria of the study, ensuring the accuracy and integrity of findings.

Table 4.2 Academic Search Engine Comparison

Search Engine	**No. of Articles**	**Bibliographic Details**	**Manual Review**
BASE	1883	Yes	Yes
Google Scholar	27240	No	No
Scopus	392	Yes	Yes
Web of Science	332	Yes	Yes
JSTOR	1060	Yes	Yes
Semantic Scholar	4710	Yes	No
Microsoft Academic	557	Yes	No

From the established requirements noted earlier; (i) adequate Indexing of Academic Article; (ii) accurate and sufficient bibliographical information, and manual review of publication, only four databases were found to fulfil these necessary requirements for data collection, shown in table 4.2; BASE, Scopus, JSTOR, and Web of Science. The chosen search engines adopt a more focused and concise approach, which reduces the available data for collection, but satisfy the necessary criteria for potential inclusion:

- Article Abstract, Title, or Keywords must include either cyberterrorism, hacktivism, or both.
- Articles must be sourced from peer-reviewed journals.
- Articles published between the years 1999 and 2021.
- Articles must be written entirely in english.

This approach offers a higher level of consistency in terms of data integrity as access to the source article and accurate bibliographic data is more likely. The decision to prioritise data integrity over volume addresses the issue of information overload and helps in managing the challenge of "infobesity" and focus on high-quality peer-reviewed articles that are most suited for the research objectives.

4.2.2 Literature Discovery by Academic Publishers

The second source of academic literature for this study comes in the form of academic publishers. Over the past two decades, publishers have contributed towards increasing the accessibility and availability of articles. It is common for most publishers to provide both physical and electronic versions of their journals, making scholarly content more widely accessible to researchers and readers (Tenopir and King, 2000).

The choice of publishers was determined through the examination of the initial literature review chapters with attention towards publishers associated with cited literature. This process aimed to identify publishers that align with the research project's focus and cover relevant academic areas related to the domain of cyberterrorism and hacktivism. Additionally, similar requirements established for third-party academic search engines were taken into consideration when selecting publishers. Thus, in aligning the selection process with the study's specific objectives and requirements, this study targets publishers that publish high-quality and credible academic content.

Table 4.3 Academic Publisher Comparison

Publisher	**Cyberterrorism**	**Hacktivism**	**Bibliographic Details**	**Peer Reviewed**
Sage	102	173	Yes	Yes
T & F	322	267	Yes	Yes
Springer	497	461	Yes	Yes

Based on the same key terms (cyberterrorism, cyber-terrorism, cyber terrorism, hacktivism) and search criteria, a search was conducted to gauge the available literature. This process included using the filtering options offered by each services website to refine the initial search query. The refinement involved restricting results to English language 'peer-reviewed academic articles' primarily addressing the topics of “cyberterrorism, cybert-terrorism, cyber terrorism,” and “hacktivism,” within a temporal range spanning 20 years (2000 to 2020). Given that each service provided unique variations on result, effort was made to achieve comparable results between the services by strictly enforcing the search criteria. Results from this refinement of the earlier general results were recorded for later comparison and review.

Table 4.3 demonstrates that all publishers offer a substantial collection of search results for each topic. Combining these with the previous results obtained from academic search engines, the total number of entries for cyberterrorism; are 3408 and hacktivism; 2081, resulting in a combined total of 5492 articles.

4.2.2.1 Refining the Search via Filtering

To evaluate the effectiveness of the search criteria, the results were subjected to scrutiny to ensure that only articles relevant for this study were collected where cyberterrorism and hacktivism were the primary focus of the publications. Through a preliminary manual review and reading of a random sample of the literature's collected abstracts, it became evident that much of the sample associated with the keywords: "cyber-terrorism", and "cyber terrorism" were ineffective in identifying literature topically specific to either domains of cyberterrorism, hacktivism, or both as a primary focus. Thus, the decision was made to limit the earlier search criteria to the following keywords: "cyberterrorism" and "hacktivism."

Table 4.4 Total Results Articles with "cyberterrorism" & "hacktivism" keywords

Topics	BASE	Scopus	WoS	JSTOR	Sage	T&F	Springer	Total
Cyberterrorism	96	63	64	10	4	33	26	296
Hacktivism	27	69	87	5	16	18	44	266

Table 4.4 demonstrates a substantial decrease in the number of results provided when the general search query is refined to studies with a primary focus on cyberterrorism, hacktivism, or both by limiting the keywords to; "cyberterrorism," and "hacktivism." This refinement resulted in the total number of relevant articles obtained for both keywords; "cyberterrorism" and "hacktivism," being 562. This reduction in the dataset size indicated the successful application of the filtering criteria to identify literature that aligns more closely with the research objective.

To compile the individual datasets from each search engine and publisher, the publications and relevant bibliographic data was collected from the respective service's web page using the provided download options. The downloaded articles were imported into Zotero, an open-source citation database management program for later manual review of the literature. Each article's bibliographic information and associated document was organised into folders based on the original source of retrieval.

4.2.3 Identifying and Removing Duplicates

Upon collection of the bibliographic information, an extensive review of the collected articles' bibliographic data was done to identify any missing data or potential duplications. An initial manual review was performed within Zotero, focusing on attributes such as title misspellings making the identification of duplicates difficult, a similar process was conducted concerning authors names, such as the inclusion of middle initials, or lack thereof leading to unidentified duplicates.

The database stored within Zotero was organised into two primary datasets: "cyberterrorism" and "hacktivism." A preliminary comparison was conducted based on the title and authors of each article, and upon initial review revealed the presence of duplicated data entries across the various sources. Due to the lack of duplication between publishers, articles identified from these publishers (Sage, Taylor and Francis, and Springer) were merged into a single Zotero folder titled 'Publishers' for more consistent comparison.

Within the *cyberterrorism* dataset, a total of 296 articles were collected, 63 of those articles are provided by publisher-based searches (Sage, Taylor and Francis, SpringerLink), with academic search engines (BASE, Scopus, Web of Science, JSTOR) providing 233 articles. When compared, a total of 71 duplicates were identified resulting in a dataset of 225 with 39 articles unique by publishers.

Within the hacktivism dataset, a total of 266 articles were collected, 78 articles were provided by publishers, while 188 articles were provided by search engines. When compared, a total of 100 duplicates were identified across the dataset resulting in a total of 166 individual publications with 40 publications unique to publishers.

4.2.3.1 Merging the Collected Datasets

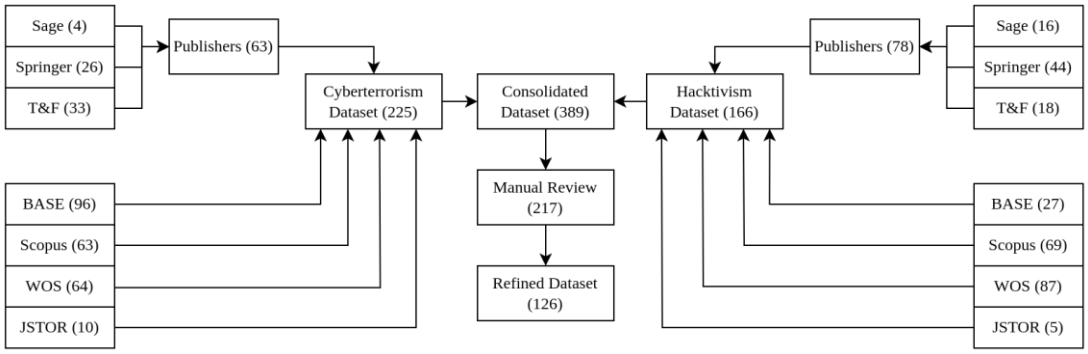


Figure 4.2 Dataset Consolidation Structure

The merging process of the cyberterrorism and hacktivism datasets was straightforward, following the same process introduced previously. The workflow diagram (see Figure 4.2 Dataset Consolidation Structure:156) illustrates the flow process in combining each

dataset into a unified collection for further review, alongside the number of articles present at each stage. When combined, the total number of articles from both datasets is 391, and after cross-referencing article title, year, and authorship, the resulting consolidated dataset comprised a total of 384 articles, with 7 duplicates removed.

4.2.4 Data Screening

After consolidating all the entries, a thorough manual screening of the collected literature was conducted to assess its overall quality of bibliographic information and identify any missing values pertaining to the articles data. This screening used a multi-level screening process that involved evaluating the accessibility and readability of each articles document, determining whether each article focused on cyberterrorism, hacktivism, or both as its main topic through manual review of the articles title and abstract, and if the included document was suitability for both bibliometric analysis (authors, affiliation, keywords, abstract, journal, list of cited references) and content analysis (has a primary focus on cyberterrorism and hacktivism, includes a definition of either phenomenon).

Table 4.5 Manual Review Stages

Review Stage	Stage Detail	Amount	Included	Excluded
First Level of Screening	Removal of Duplicates and access to the full text document of the article	562	389	173
Second Level of Screening	Relevant to the topics as primary or of significant relevance through the review of the articles title and abstract	389	313	76
Third Level of Screening	Has necessary bibliographic data required for analysis.	313	217	96
Data Refinement	Cited 10 or more times	217	126	91

After the final screening, a thorough comparison of basic bibliometric details of each article collection (authors, affiliation, keywords, abstract, journal, list of cited references) was conducted to ensure the databases accuracy and completeness. Any missing or incorrect information was manually rectified using the values obtained from the corresponding articles or their respective webpages and inputted into Zotero.

4.2.4.1 Defining High Impact Articles

To ensure that the dataset analysed consisted of only key research with significant impact in the domain of cyberterrorism and hacktivism, a data refinement process was employed. Only articles with a Google Scholar citation value of 10 or above were included in the study as a means of identifying highly impactful literature. Google Scholar was chosen

for its accessibility and reliable reflection of academic impact through traceable citation data, providing quantitative information for measuring impact within the database.

After collecting the data, the citation metric for each article was graphically plotted to illustrate the average distribution of citations across a yearly timeline. The observation revealed that 42% (91) of the total dataset (217) of manually reviewed literature consisted of articles with less than 10 citations, and 126 publications with a citation value of 10 or above, later defined as *'high-impact articles*.' This data refinement allowed for the identification of significant and impactful articles, ensuring that the analysis focused on research with notable influence in the field of cyberterrorism and hacktivism, providing a clearer reflection of its development.

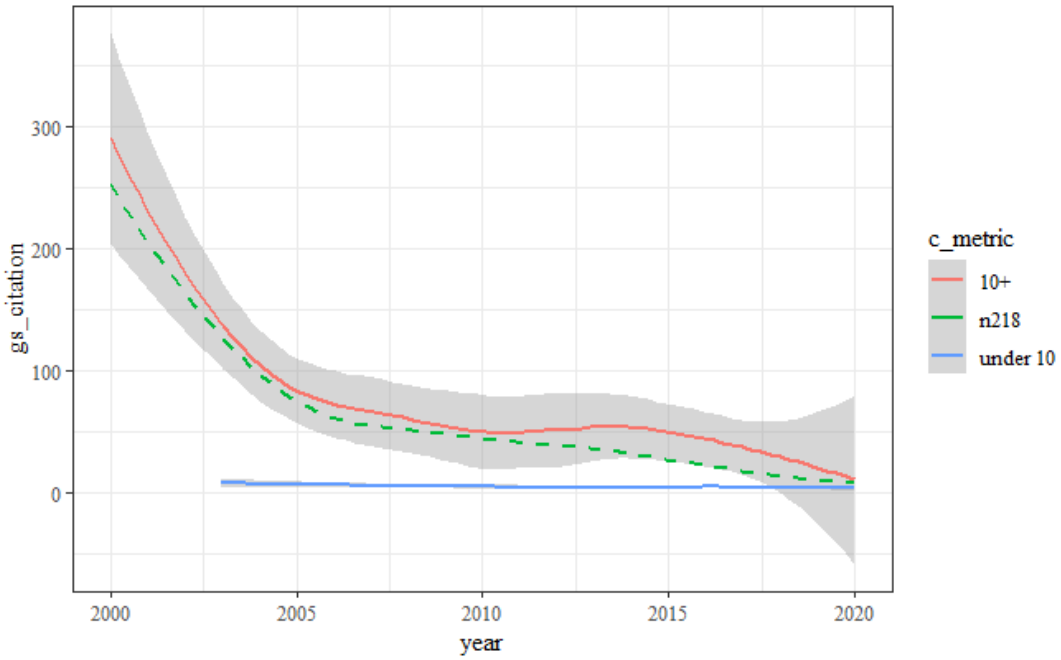


Figure 4.3 Average Distribution of Google Scholar citation score by year

Figure 4.3 illustrates the average distribution of Google Scholar citation metrics on a yearly axis (2000 to 2020). The red curved line represents articles with 10 or more citations. Articles with a citation metric of 9 or lower citations are shown in blue. The dashed line represents the average distribution of citation metrics for the (218) dataset for comparison.

Upon refinement of the collected articles, a manual assessment of the documents content was introduced to determine further eligibility for the inclusion in this research project. As this study conducts both a bibliometric and content analysis of peer-reviewed articles, each article's PDF document was reviewed from within Zotero, with attention placed on the document's inclusion of a definition of either cyberterrorism or hacktivism, and further discussion on the topic. Documents including definitions were highlighted and tagged appropriately marking the document eligible for inclusion in either the bibliometric analysis, the content analysis, or both.

In total, for inclusion in the bibliometric analysis, 126 articles were deemed eligible for inclusion having clearly detailed and accessible titles, abstracts, keywords, journal affiliations, and list of cited references. Further, 87 included high-impact articles were identified to meet the eligibility for inclusion within the content analysis of definitions. This included 55 articles that provide a definition for cyberterrorism, and 43 high-impact articles defining hacktivism.

4.3 Bibliometric Analysis

For this research project, bibliometric analysis methods based on citation analysis (see Wallin, 2005; van Eck and Waltman, 2014:37) are employed to extract and analyse data in which to map the domain of cyberterrorism and hacktivism research.

In advancing academic literature, the synthesis of previous research plays a crucial role. Traditionally, scholars have employed two main methods to consolidate earlier findings: qualitative approaches, such as literature reviews, and quantitative approaches, including meta-analysis and systematic reviews. However, Tranfield, Denyer, and Smart (2003) has highlighted the susceptibility of traditional literature reviews to researcher bias and the need for greater rigour. To address these concerns, bibliometric quantitative approaches, known as both performance analysis and science mapping emerged, offering a systematic, transparent, and reproducible review process that allows for descriptive and evaluative observation of published literature, enhancing the review process's quality (Donthu et al., 2021).

The rationale behind incorporating Bibliometric analysis lies in its ability to offer a comprehensive view beyond simple frequencies. Instead, bibliometrics provides a multi-dimensional perspective of the connections within a field, bridging current scholarship with its foundational articles (Harker and Saffer, 2018). Bibliometrics serves as a methodological technique with two primary uses. Firstly, it aims to evaluate the performance of articles and their authors through performance analysis (Donthu et al., 2021). Secondly, it functions as a mapping instrument to observe the structure and

dynamic evolution of a scientific field using scientific mapping (Cucari et al., 2023). Conceptualising the method, Shiffrin and Börner (2004) introduced the term "knowledge mapping" to encompass the synthesis of findings from a wide range of techniques used for charting, mining, analysing, sorting, facilitating navigation, and displaying knowledge. The application of knowledge mapping is not estranged within criminological research, and has seen use within terrorism studies (Gordon, 2004; Reid and Chen, 2006; Klona et al., 2021), thus was deemed a fitting framework for this study.

4.3.1 Knowledge Mapping Framework

Returning to the first research objective of tracing and evaluating the academic development and status of cyberterrorism and hacktivism research, this research project examines the production of knowledge in cyberterrorism and hacktivism research. To achieve this, the study adopts a modified variation of the 'integrated knowledge-mapping framework,' employed earlier by Reid and Chen (2006) in their study on contemporary terrorism research. Mapping the etymological and academic development of cyberterrorism and hacktivism, this section will describe the following framework:

Table 4.6 Modified Knowledge mapping framework

Type of analysis	**Unit of analysis**	**Measure**	**Research Question**
Basic analysis	Article, Authors, and Citations	Productivity, demographic, impact	What are the key articles, journals, authorship distribution, gender distribution, collaboration pattern, and the key articles by citation metric.

Citation analysis	Author citations	Linkage	What relationships exist between authors and their articles by their citations?
Centencis analysis	Key Cited Publications	Key concepts	What relationships exist between authors and the domains they cite from?

As table 4.6, based closely upon Reid and Chen's (2006) integrated knowledge-mapping framework as a guide for the bibliometric analysis of this research project, three types of analysis are conducted on the collected dataset of high-impact cyberterrorism and hacktivism research, of which to two are used from the pre-existing framework:

1. ***Basic frequency analysis*** of scientific output of articles from 2000 to 2020 (126) using bibliometric and social network analysis. This analysis identifies the most prolific authors, institutions, and countries contributing to the domain of cyberterrorism and hacktivism research.
2. ***Citation analysis*** by means of bibliometric coupling and co-citation analysis. This analysis maps the relationship between articles, authors, and their cited sources.

Notably, Reid and Chen's (2006) knowledge mapping framework incorporate an additional third 'topic mapping' analysis, of which they assess the correlations between various key terms within terrorism studies publication abstracts. Although originally included the decision to omit the use of topic mapping was partially due to the inclusion of a quantitative content analysis, and definitional focus. Further, as identified by Liu and Chen (2013:637) when discussing the accuracy of topic mapping, topics extracted from the abstracts of articles can be broader in scope than the topics arising from citation

contexts, suggesting that these ‘citences’ (see Nakov et al., 2004), i.e. the sentences that surround citations, offer more precisional context than abstracts, however. There is still value in adopting Reid and Chen’s integrated knowledge-mapping framework (2006) as a means of providing structure for mapping of the bibliographic findings.

For this study, several citation analysis techniques were adopted within the knowledge mapping framework, these methods can be summarised as performance analysis, and science mapping outlined and discussed in the following sections.

4.3.1.1 Performance Analysis via Bibliometrics

Noyons et al., (1999:592) regards performance analysis as the evaluation of scientific actors and the impact of their academic output based on bibliographic data. This impact is measured by assessing the number of times a particular article or author has been cited. This is a common metric used for evaluating the influence of a particular author (or group) and the significance of their research contributions (Donthu et al., 2021).

Citation Analysis

Citation analysis is commonly employed in bibliometric studies. This form of descriptive statistics uses citation counts to measure the influence and importance of academic literature (Osareh, 1996). Citations establish a relation among authors, serving as a measure of the extent to which they communicate indirectly through academic literature. Therefore, a highly cited piece of academic work indicates that the work of the highly

cited author is considered relevant and topical to scholars who cite their work (Osareh, 1996:152).

4.3.1.2 Science Mapping via Bibliometrics

Unlike performance analysis, which focuses on the contribution of individual researchers and often measures these contributions based on citation amount, science mapping focuses on the relationship between researchers, allowing for the evaluation of researchers and their institutional productivity (Cucari et al., 2023:2). For example; Noyons et al. describes science mapping as the monitoring of a scientific field in order to map its "cognitive" structure, of which in Noyon et al's., example, is achieved by identifying subdomains from keywords using co-word analysis (1999:592), and can similarly include; bibliographic coupling (Kessler, 1963), co-citation analysis (Osareh, 1996), and co-author analysis (Peters and Van Raan, 1991) to represent the structure and dynamics of a particular scientific field or research domain.

Bibliographic coupling

Introduced by Kessler (1963), bibliographic coupling is a science mapping method that uses the measurement of citation similarities to establish relationships between research documents (Jarneving, 2007; Habib and Afzal, 2019). This method focuses on the number of shared citations between research articles to determine the level of bibliographic coupling. Unlike co-citation analysis, which considers the cited references of the articles, bibliographic coupling focuses on the relationships between the cited articles themselves (Kessler, 1963:10).

One of the advantages of bibliographic coupling is its ability to recommend relevant papers based on shared citations, benefiting emerging and immediate research that may lack the considerable volume of citations associated with more established fields of research (Jarneving, 2007:289).

Co-citation analysis

Like bibliographic coupling, co-citation analysis is a method used to identify relationships between academic works. Co-citation analysis, introduced by Small (1973) measures the frequency at which two units (such as academic articles) are cited together (McCain, 1990)

According to Zupic and Čater (2015), co-citation analysis offers dynamic insights and can track changes in research focuses and schools of thought over time (Pasadeos, Phelps, and Kim, 1998). When multiple articles include shared cited sources, it indicates a level of similarity, leading to the emergence of clusters as the collection of citations grows. By examining co-citation counts, this technique assesses the similarity between two pieces of academic work. The underlying assumption is that when two items are frequently cited together, there is a higher likelihood of their content being related or interconnected.

Co-author Analysis

Co-author analysis is a method used to investigate the relationships between authors who collaborate on research papers. When two or more authors co-publish a paper, it

establishes a connection between them, surpassing other relatedness measures like co-citation (Zupic and Čater, 2015:435). As a result, co-author analysis is particularly well-suited for examining social networks within the academic community, focusing on the collaborative relationships and interactions between researchers rather than the intellectual structure of research fields. By conducting co-author analysis, researchers can observe and study the formation and development of scientific social networks among collaborating scholars (Acedo et al., 2006).

de Solla Price (1966) referred to this phenomenon as "invisible colleges," describing it as informal groups of researchers who frequently collaborate on projects (cited in Paisley, 1972:6). Co-author analysis enables the identification and exploration of these informal groups, shedding light on their dynamics. Moreover, co-author analysis allows for the examination of additional factors, such as "productivity," which involves assessing the number of individual and collaborative articles for a specific author. This analysis supports the identification of key figures within collaborative academic groups (Peters and Van Raan, 1991:239).

4.3.2 Analysis of Bibliographic Data

According to Reid and Chen, (2008:3), Creating a knowledge map entail extracting, examining, plotting, and illustrating a research field based on insights from experts, institutions, subjects, articles, and social networks. Thus, as part of the triangulation design discussed in the earlier (see Creswell and Plano Clark, 2007:77), the bibliometric

analysis conducted during this research project structurally mirrors Reid and Chen's integrated knowledge-mapping framework, but also introduces general restructuring of the findings presented. Modifications to the various techniques used, most notably, the introduction of gender as a component of measurement, like its usage in understanding organised crime research (Hosford et al., 2021), and the use of different, more modern software.

This study makes use of two distinct toolsets, firstly, for the basic analysis of article and author descriptive details using descriptive statistics, Rstudio is used to analyse a spreadsheet database of bibliographic details provided by Zotero's export database option. RStudio is an integrated development environment (IDE) for the *R* programming language and is intended for statistical computing and graphics.[8] Secondly, Vos-viewer is used for the analysis of author citations and abstract data. Developed by Nees Jan van Eck and Ludo Waltman (2014), Vos-viewer allows for the importing of spreadsheet-based bibliographic databases for the visualisation of bibliometric networks.

In preparation for the analysis, supporting documentation was provided by both Rstudio[9] and Vosviewer[10] and reviewed concerning how to correctly format the data for importing. This was manually configured and reviewed for all 126 articles to ensure any potential inconsistencies such as incorrect spelling and dates were corrected.

[8] See: Introduction to R, available at: https://www.r-project.org/about.html
[9] More recently rebranded as Posit, necessary resources are available at: https://posit.co/resources/
[10] Vosviewer: Getting Started, available at: https://www.vosviewer.com/getting-started

Similarly, as this research project reviewed the gender distribution of authors identified, and their primary research discipline at the time of their publication within the collected 126 articles. This thesis adopts the method used in Hosford et al., (2021:3) where authorship information was extracted from the published articles, with assessment of gender using web-based search for images and words indicating the specific authors gender and disciplines where needed, and recorded using a spreadsheet with each author of a article being given a unique identifying ID provided by Zotero, to link the author to their associated article. This web-based search included institutional profiles, online CVs, public social media accounts, academic database profiles (i.e. ResearchGate, Academia.edu), and other online material such as press releases and media presentations, adopting a similar method employed by Chesney-Lind and Chagnon (2016) in their study of gender and race pertaining to academic privilege in Criminology.

Liu and Chen (2013) note that the traditional means of extracting insight from the abstracts of articles provided only a broad context of the publications analysed, instead recommending that ‘citences’ (Nakov et al., 2004), or the sentences that surround citations, offer more precision and context than abstracts. Therefore, to map key themes, cited articles identified by the analysis and review of key authors' co-cited publications were used to identify leading themes discussed within the 126 high impact articles. leveraging Orange’s concordance feature, which acts similarly to a search engine, relevant citations referenced within the articles can be identified and catalogued. Doing so provides the analyst the ability to explore individual authors' citations within the wider collective list of citations more effectively.

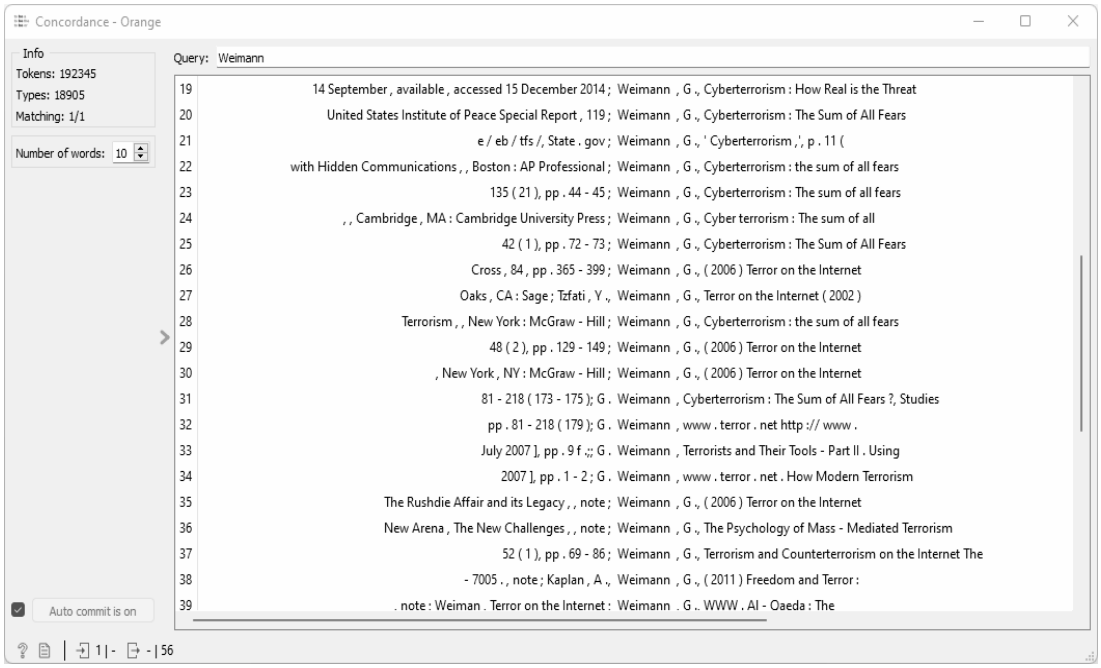


Figure 4.4 Orange Data Mining - Concordance View

Illustrated in Figure 4.4, Orange Data Mining was used to search the complete collection of citations cited within each of the 126 high-impact articles, offering an effective means to identify the citations from high-impact authors with significant contributions to the domain and identified in the co-citation analysis. With this information at hand, a thorough review of these cited works becomes feasible, enabling an examination of their overall themes and focus of discussion in relation to the works of other closely co-cited authors and their articles.

4.4 Taxonomic Content Analysis

The incorporation of bibliometric analysis facilitates the examination and emergence of numerical data within a literature collection, thereby offering valuable insights into the patterns and structures present in the scholarly domain (Schildt et al., 2006). However, it

is important to note that bibliometrics provides limited context regarding the specific utilisation of collected attributes, such as citations, within the literature text. Despite the advantages of employing a specialised dataset, which aids in mitigating noise in information discovery techniques like citation networks, citations in bibliometrics function as placeholders for the underlying concepts and discussions influencing the literature corpus.

To attain a deeper empirical understanding of the evolution of how cyberterrorism and hacktivism has been defined within academic research, content analysis is deployed as part of the Triangulation Design: Data Transformation Model (Creswell and Plano Clark, 2007:77). This content analysis aims to identify latent themes and concepts that underlie the scholarly discourse in the field. By combining these identified themes and concepts with the empirical bibliometric database through triangulation, a comprehensive timeline corresponding the the literature collected for analysis (2000 - 2020) can be constructed, offering a nuanced depiction of the developmental trajectory of cyberterrorism and hacktivism, as well as their respective definitional attributes.

4.4.1 Quantitative (Basic) Content Analysis

Content analysis is a systematic method employed to analyse textual data with the objective of uncovering underlying concepts, themes, and relationships within a collection of academic literature. By subjecting the data to rigorous scrutiny, content analysis seeks to reveal the inherent qualities of the information, leading to the generation

of valid and reliable inferences (Krippendorff, 1980, 1989, 2018). As a mode of unstructured ontological discovery, content analysis offers a systematic and objective means of exploring phenomena at a theoretical level (Elo and Kyngäs, 2008; Kyngäs et al., 2020:13). This enables researchers to gain detailed conceptual insights by delving beyond the surface level of authorship and citations to examine the actual texts employed by authors (Biesenthal & Wilden, 2014). Consequently, content analysis facilitates an objective and text-driven examination of the literature, allowing for a comprehensive and rigorous review of its content.

In this study, a quantitative content analysis method known as *basic content analysis* (Drisko and Maschi, 2016:21) is employed, coupled with a descriptive research design. Descriptive research design is a type of study aimed at providing a comprehensive account of the understandings and experiences related to a specific phenomenon (Delost and Nadder, 2014). Such research is particularly valuable when investigating topics that have not been extensively studied previously, or when establishing a foundational understanding of a subject before proceeding with further investigations (Siedlecki, 2020). By combining basic content analysis and a descriptive research design, this study endeavours to systematically examine the content of cyberterrorism and hacktivism definitions and offer an insightful portrayal of the phenomenon and issues under investigation.

It is essential to distinguish between quantitative content analysis (QCA) and deductive content analysis (DCA), as they differ in their approach and purpose. Deductive content

analysis is driven by a pre-existing theoretical framework or specific research questions (Kyngäs et al., 2020:23). On the other hand, quantitative content analysis employs a structured and systematic approach to analyse content (Janis and Fadner, 1943:106) and often uses descriptive statistics to empirically document a perceived social phenomenon, serving as a foundation for advocating change (Drisko and Maschi, 2016). While both methods share certain similarities, their distinctive characteristics underscore their unique roles in the analytical process.

Deductive content analysis encompasses both qualitative and quantitative approaches, while quantitative content analysis specifically employs numerical or statistical methods. Despite its primarily quantitative nature, quantitative content analysis incorporates qualitative components that are integral to its execution, blurring the strict boundary between the two (Lock and Seele, 2015:28). Krippendorff (2018) emphasises that content analysis integrates both qualitative and quantitative levels of analysis. Further, Krippendorff goes on to assert that content analysts, regardless of their approach, sample text to select relevant portions, unitize text by distinguishing words, propositions, or larger narrative units and using quotes or examples, contextualise the text within the circumstances surrounding it, and formulate specific research questions (Krippendorff, 2018:88). This convergence of qualitative and quantitative elements highlights the nuanced interplay between the two methodological paradigms in the context of content analysis.

4.4.2 Content Analysis and Epistemological Positioning

Epistemologically, quantitative content analysis is rooted in positivist and realist philosophies, as observed in studies conducted by Neuendorf (2002; 2011). Analysts typically adopt a scientific approach to the research task. In this paradigm, the analysts' beliefs, cultural experiences, social context, and research purposes are considered not to significantly influence the analysis of the data (Drisko and Maschi, 2016:28). Within a basic content analysis, data is regarded as objective and independent of interpretation, with Weber (1990) emphasising the importance of reliability and its consequential impact on the validity of the collected and analysed text. This objective stance aligns with the foundational tenets of positivism and realism, emphasising the empirical nature of the research endeavour in quantitative content analysis.

The epistemological stance and emphasis in quantitative content analysis significantly influence a crucial phase of the analysis, namely, the drawing of inferences. According to Krippendorff (1989), this phase involves determining how stable knowledge derived from the coded data pertains to the phenomenon under study. In the context of the current research, the purpose of quantitative content analysis is to map the degrees of conceptual themes and their trajectories within academic research related to cyberterrorism and hacktivism, thereby providing insights into the definitions, and understanding of these phenomena.

4.4.2.1 Validation and Reliability within Quantitative Content Analysis

As highlighted by Schwartz and colleagues (2001), quantitative content analysis plays a crucial role in the process of triangulation, which, as mentioned earlier, aims to enhance the validity and reliability of research findings through the integration of multiple methods, data sources, and perspectives (Creswell and Plano Clark, 2017). Transparency is a vital aspect associated with the content analysis process, as emphasised by Krippendorff (2018), and it contributes significantly to achieving validity and reliability in the research. The findings derived from quantitative content analysis are typically descriptive in nature and serve as evidence for making abductive inferences (Krippendorff, 2018). Abductive inferences involve linking an observation with a hypothesis that accounts for or explains the observed patterns and trends in the data (Drisko and Maschi, 2016; Reichertz, 2013). By employing quantitative content analysis, this research aims to provide valuable insights into the evolving landscape of cyberterrorism and hacktivism research, enriching our understanding through a combination of systematic analysis and triangulation of diverse data sources and methods.

This study aims at deepening current understandings towards the knowledge production and conceptual understandings of cyberterrorism and hacktivism research, therefore, the analysis operates within what Krippendorff terms “the conceptual environment” (2018:33). This means that the analysed text actively contributes to the larger conceptual context within which these social phenomena are situated. As this thesis explores these complex topics, the findings must be interpreted with thoughtful consideration of the broader conceptual academic landscape in which they exist.

Unlike deductive content analysis (DCA), quantitative content analysis does not rely on a pre-existing theoretical framework or set of research questions to guide the analysis (Kyngäs et al., 2020:23). Instead, it employs a structured and systematic approach to examine content (Janis and Fadner, 1943:106). Consequently, the validity of quantitative content analysis is not evaluated through the application of a pre-existing theory.

The use of content analysis without an overarching theory is not uncommon (see Potter and Levine-Donnerstein, 1999). In such cases, the primary objective of content analysis is to offer a comprehensive description of the analysed content through frequential and descriptive analysis, employing bivariate methods, including variable counts, leading to a univariate report. Potter and Levine-Donnerstein emphasise that when researchers begin reporting variables in a bivariate manner and identify relationships, they venture into the domain of providing empirical generalisations, marking the study as inductive (1999:264). However, it is crucial to emphasise, in accordance with Drisko and Maschi's perspective (2016), empirical findings alone do not inherently guarantee the validity of a conclusion.

In the absence of a subsequent inductive process, the study, as articulated by Potter and Levine-Donnerstein, would remain confined to the descriptive level (1999:264). To transcend this limitation, the analysis is extended to contextualise the findings within a broader framework, rather than relying on a direct comparison to existing theories. Consequently, while the validity of the analysis cannot be directly assessed against pre-

existing theory, it remains possible to assess the analysis and its findings for ecological validity.

Ecological validity, as defined by Lewkowicz (2001), pertains to the extent to which the results of a study can be applied to real-life settings. In the context of this research project, which primarily relies on data collected from academic literature, the scope of analysis encompasses disciplines related to cyberterrorism and hacktivism, and the dataset includes academic definitions of both social phenomena. Consequently, the context of this study centres on the academic research community exploring these domains. Considering ecological validity's focus on generalizability to naturalistic situations, such as experts in the research field of cyberterrorism and hacktivism, the reliability of findings becomes inherently linked to replicability (Krippendorff, 1980) within the academic research context.

4.4.4 Taxonomic Framework

To align with the deductive approach of the quantitative content analysis and to support replicability and practical utility for ecological validity, this research project incorporates a taxonomic framework for the systematic collection of terms identified during the quantitative content analysis process, with the intentions of being later implemented within the development of an ontological framework for data collection.

Taxonomy, as defined by Simpson (1961:11), entails the exploration of classification, encompassing its foundations, principles, procedures, and rules. In this context, adopting Bailey's interpretation (1994:6), a taxonomy is employed for the systematic classification of empirical entities. While taxonomies are commonly associated with the biological sciences, they have found relevance within the field of criminology, particularly in understanding various aspects of cybercrime. One such application is seen in the work of Rogers (2006), who employed a taxonomic approach to comprehend the development and mapping of hacker skill levels. Subsequently, Seebruck (2015) expanded on Rogers' work by incorporating motivation as a categorical entity within later typologies. Further, extending this line of inquiry, Hosford (2021) integrated cyberterrorism into the taxonomic framework.

Additionally, it is essential to clarify a common misunderstanding prevalent in the field concerning the interchangeable use of the term's "taxonomy" and "typology." As noted by Bailey (1994:6), there is a key distinction between the two concepts. Typologies are better suited for the conceptualization of entities, whereas taxonomies focus on empirical entities. Hence, while Rogers may have introduced a taxonomy in his work, it is more accurately described as a typology due to its conceptual nature. A different application of taxonomies was adopted by Akhgar and colleagues (2016) when consolidating understandings of various cybercrime entities. Their taxonomic framework facilitated the formulation of potential future research roadmaps by providing a rigid and topical structure for organising empirical entities related to cybercrime. Therefore, Taxonomies

serve as an ideal framework for conducting analysis, as their purpose is to identify the essential properties that distinguish one group of entities from others (Hodgson, 2019).

4.4.5 Analysis of Collected Definitions

To satisfy the second research question concerning the identification of key themes and distinctions within definitions of cyberterrorism and hacktivism, this research project adopted a quantitative content analysis (see Drisko and Maschi, 2016:21), supported by a taxonomic framework used to code, analyse, and categorise extracted terms. To achieve this, a taxonomy developed by Al Mazari et al. (2015) and extended by Plotnek and Slay (2021) was adopted for the analysis of 237 identified definitions of both cyberterrorism (162|68.3%) and hacktivism (75|31.6%) identified from 87 (69%) of the 126 academic articles analysed within the bibliometric analysis.

Table 4.7 Distribution of Collected Definitions

Definition	Cyberterrorism	Hacktivism
Quoted	89 (37.5%)	22 (9.27%)
Consolidated	18 (7.5%)	13 (5.4%)
Proposed	55 (23.2%)	40 (16.9%)
Total	162 (68.3%)	75 (31.6%)

Note: % valued from the total 237 definition appearances collected

During the collection of literature, definitions identified within the 87 articles were organised into three class types: *"Quoted"* definitions are those cited by authors of which

they have taken from earlier articles; "*Consolidated"* where the authors merge several earlier cited definitions together; and *"Proposed"* where authors introduce a new definition either as a product of their research or lacking any reference to earlier article.

4.4.5.1 Data Preparation

Data preparation for the content analysis was straightforward, adopting the same preparation process as seen in preparation for the bibliometric analysis (see section 6.3.1 Data Preparation and Analysis: 185). Upon the manual review of articles PDF's, identified definitions of cyberterrorism and hacktivism were highlighted within their articles document and extracted verbatim into a spreadsheet database.

Table 4.8 Example of Definition Database

Lit ID	Definition	Type	Source
8FEVV3S4	Broadly defined, cyber terrorism is the use of new communication technologies to attack computer systems with the objective of threatening and disruptive actions against computers, networks, and the Internet in order to cause harm or further ideological, political, or similar objectives, or to intimidate any person in furtherance of such objectives	Consolidated	Arquilla, Ronfeldt, & Zanini, 1999; Conway, 2002; Dunnigan, 2003
V2IBLYYC	Cyber-terrorism is "non-state actors' use of ICTs to attack and control critical information systems with political motivation and the intent to cause harm and spread fear to people or at least with the anticipation of changing domestic, national or international events"	Quoted	Beggs, 2005
6Q6NU89Y	In contrast to conventional terrorism, cyberterrorism employs malicious computer technology rather than kinetic force. But like conventional terrorism, cyberterrorism aims to further political, religious, or ideological goals by harming civilians physically or psychologically. & Despite its growth, cyberterrorism unlike conventional terrorism does not currently threaten life and limb.	Proposed	Gross, Daphna, & Vashdi, 2017

As table 4.8 shows, definitions were recorded in a spreadsheet database for easier organising and analysis, maintaining a reference link to the source article, and paired with articles unique ID code. This ID process facilitated the identification of key definitions

and provided access back to the source material where each definition was extracted if any further contextual or case-specific clarification was needed. Context to the following tabular columns is defined as follows:

- **Lit ID**: This column represents the unique identifier of the article from which the definition was extracted. Each definition is linked back to its respective source article through this identifier.
- **Definition**: This column contains the actual text of the definition as found in the article. It provides a clear representation of the meaning attributed to cyberterrorism and hacktivism in each case.
- **Type**: This column (illustrated in table 8.1) categorises the nature of the definition. Definitions are classified into three types:
    - **Quoted**: The definition is directly quoted from a single earlier source.
    - **Consolidated**: The definition is an amalgamation of multiple definitions taken from various sources, creating a unified and comprehensive understanding.
    - **Proposed**: The definition is unique to the specific article and is introduced as an original contribution by the authors.
- **Source**: The source column records the origin of the definition, allowing for the identification of key contributor articles that have played a significant role in shaping the understanding of cyberterrorism and hacktivism.

This structure facilitated additional observations, such as coding terms and categorization, to provide the analytical capabilities during subsequent research and exploration of the collected definitions.

4.4.5.2 Building the Taxonomy

Within the context of this research project, the taxonomy is used to systematically deconstruct and categorise the conceptualizations of cyberterrorism and hacktivism definitions, allowing for the identification of crucial attributes associated with each term. The use of taxonomies to extract fundamental traits from definitions has been a prominent approach in cyberterrorism research. For instance, Plotnek and Slay (2021) recently adopted a consolidated taxonomy of cyberterrorism definitions, building upon the groundwork laid by Al Mazari et al. (2015). The latter authors conducted a systematic analysis of identified cyberterrorism definitions and identified five key components that were frequently present in these definitions.

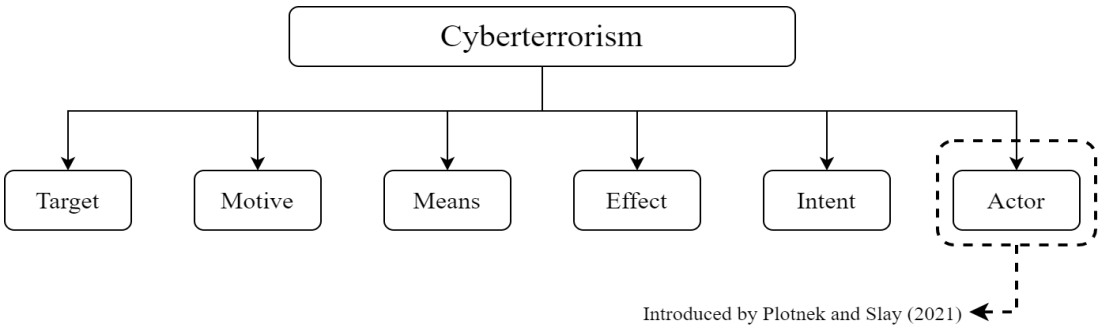


Figure 4.5 Definition taxonomy (Al Mazari et al., 2015; Plotnek and Slay, 2021)

Al Mazari et al. (2015: 12) developed a comprehensive taxonomy comprising five main classifications, each associated with specific traits, to analyse and categorise cyberterrorism phenomena:

Target: This classification encompasses various entities that could be subjected to cyberterrorist activities, including military forces, government cyber and physical

infrastructures, critical national infrastructures, social and national identity, as well as private industry or entities.

Motive: Within this classification, the taxonomy considers the diverse motivations driving cyberterrorist actions, such as social, cultural, religious, political, ideological, and others.

Means: This classification delves into the technological aspect of cyberterrorism, focusing on the use of computer and communication technologies and networks to execute attacks.

Effect: The effect classification analyses the outcomes and consequences of cyberterrorism, encompassing violence, destruction and/or disruption of services, infliction of physical, operational, and informational damages, as well as harm to individuals and groups.

Intention: The intention (intent) classification pertains to the desired outcomes sought by cyberterrorists, such as gaining political, social, military, or ideological advantages.

Furthermore, the original taxonomy has been expanded by Plotnek and Slay (2021) through the introduction of a sixth class, termed '*Actor*.' This addition was derived from an analysis of recent cyberterrorism articles that placed a greater emphasis on the *'Intent'*

of these threats (MacDonald et al., 2013; Plotnek and Slay, 2021; Yunos et al., 2015). This examination revealed a noteworthy dearth of understanding and attention directed towards the actors involved in cyberterrorism.

To achieve a conceptual merger of the provided taxonomies for use in guiding the quantitative content analysis, a comparative analysis was conducted between the classes of each taxonomy. In many instances, this comparison yielded straightforward correspondences (e.g., actor class in one taxonomy corresponded to actor class in the other). However, for certain classes that did not immediately appear related, slight variations in terminology were made to align and pair them effectively. For instance, the practice class was renamed as the means class, achieved by examining subclasses and identifying thematically similar terms. Through this process, thematic overlaps and similarities were identified, and harmonisation into a coherent and unified framework.

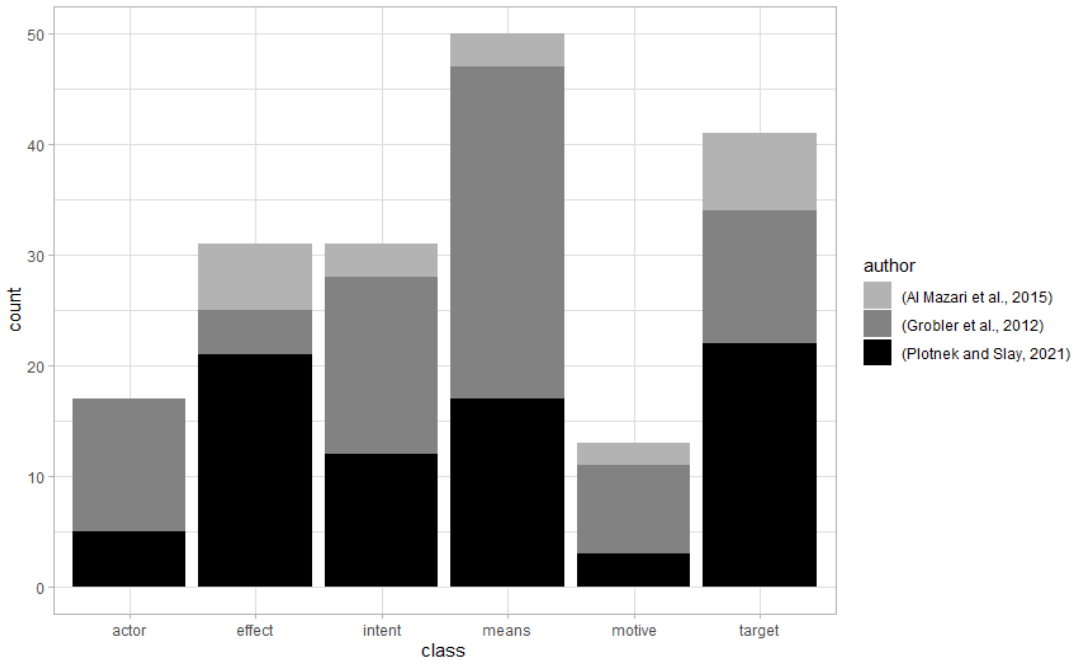


Figure 4.6 Merged Cyberterrorism Taxonomy Term Distribution

Figure 4.5 provides an overview of the sources from which the taxonomies' classes are derived, along with the count of individual terms present in each class. After the consolidation of the taxonomies, a total of 195 terms were distributed across six classes as follows: actor (17), effect (33), intent (32), means (50), motive (19), and target (44). However, the seventh class, 'cyber-event,' discussed by Veerasamy, Grobler, and Von Solms (2012), was excluded from this merging process as it was primarily used in the context of discriminating case studies related to cyberterrorism or cyber-enabled terror and not specifically on the definitions themselves.

Importantly, the terms present within the merged taxonomy are not exclusive to individual classes; they can appear in multiple classes as needed. This means that certain terms can establish 'relationships' between classes. The role of context in understanding the social

and situational meaning of terms is emphasised, and adopting a pragmatic approach ensures that the meanings and use cases of definitions and associated terms are considered when distributing them throughout the taxonomy (McTavish and Pirro, 1990:3). This approach was favoured over computer-centric methods like word-clouds and "bag of words" approaches, which focus solely on word frequencies without contextual comprehension.

4.5.4.3 Coding

Upon acquiring the datasets consisting of cyberterrorism and hacktivism definitions and developing the taxonomic framework in which to guide coding, the gathered definitions were imported into *RQDA*, an open-source qualitative analysis software application developed by Huang Ronggui (2014), specifically designed to facilitate the analysis of textual data. Leveraging RQDA's capabilities, the imported definitions were subjected to coding using both predefined codes and inductively identified codes. Coding involves the assignment of labels or tags to specific sections of the textual data to represent distinct themes, concepts, or categories.

The adoption of RQDA in this manner aided in the identification of shared patterns, distinctions, and subtleties within the definitions collected. This systematic approach provided a rigorous and comprehensive understanding of the concepts under investigation, thereby bolstering the research project's objectives and insights.

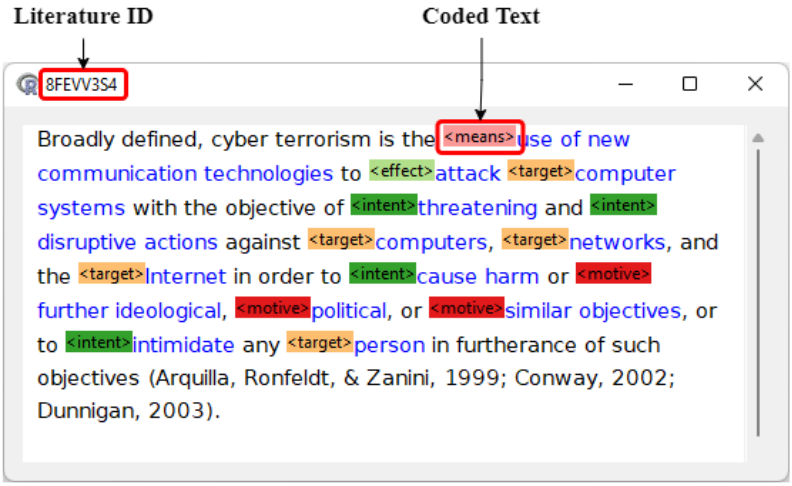


Figure 4.7 RQDA coding interface

In Figure 4.7, the collected definitions (237) underwent a meticulous coding process using the consolidated taxonomy and its classes as a guiding framework. Terms present in the definitions that aligned with the taxonomy were directly assigned the corresponding codes. Moreover, newly emerged terms in the definitions were coded using deductive reasoning, ensuring precise allocation into the appropriate class while thoughtfully considered with the context and position of each term within its respective definition referenced to aid interpretation.

The application of deductive reasoning when encountering novel terms in the definitions ensured comprehensive capture and classification of all pertinent information within the suitable classes. This methodological approach considered the context in which each term was used, thus contributing to a more precise and exhaustive coding process.

Table 4.9 Example Hacktivism Coding

id	**class**	**extract**	**code**
FAHGD2JL	effect	DoS attack	disruption
XIV8B6PR	effect	e-mail bombing	disruption
5KSFYQ58	effect	electronic disruptions	disruption

As presented in Table 4.9, three distinct terms were extracted from various definitions of "hacktivism" and were categorised under the "effect" class based on their contextual usage within each definition. These terms, namely "Dos attack," "e-mail bombing," and "electronic disruptions" all exemplify ways in which the effect of hacktivism leads to significant disruption. As a result, these terms were systematically coded under the overarching category of 'disruption,' as it aligns with the intended effect described in each definition.

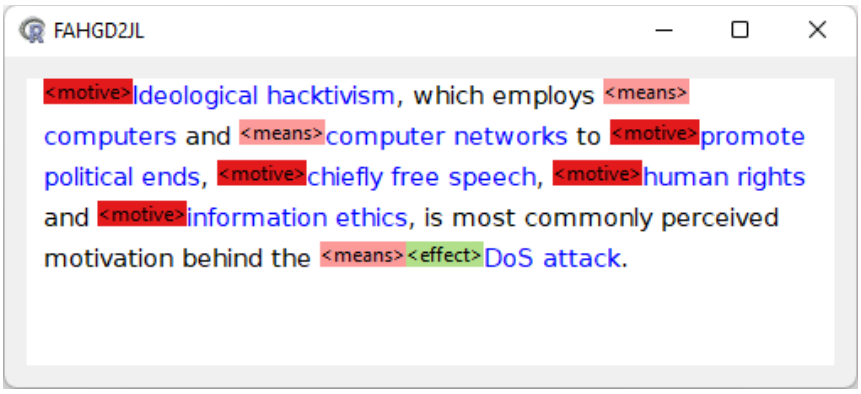


Figure 4.8 Example Hacktivism Definition

Moreover, it is worth mentioning that extracted terms may undergo multiple coding, as exemplified in Figure 4.8. This figure displays the term “Dos attack,” which has been coded under two distinct classifications: “means” and “effect.” Unlike previous taxonomic approaches used by Veerasamy et al., (2012); Al Mazari et al. (2015); Plotnek and Slay (2021), this method allows for a broader context to be considered, incorporating the coder’s observations and interpretations. Consequently, this approach expands the available information for later inferring and permits a rudimentary quantitative analysis of the extracted terms.

4.5 Methodological Limitations

Discussing limitations is vital for maintaining the credibility of the research, as it allows readers to better understand the extent to which the findings can be generalised to other contexts, or to avoid similar problems in future research (Price and Murnan, 2004; Sampson, 2012:59). This section of the research project is dedicated to articulating these

critical components, providing transparency and rigour in the research methodology, and setting clear expectations for the study's application and interpretation.

4.5.1 Peer Review Journal Articles

This project examines the domain of cyberterrorism and hacktivism academic research, centring on published research in peer-reviewed journals that aim to conceptualise and deepen our understanding of these phenomena. This emphasis on using peer-reviewed studies as a data source for bibliometric and content analysis introduces several limitations regarding the nature and utility of the analysis.

Kharasch et al. acknowledges that the peer-review process is the standard for the evaluation of a scientific research article's quality prior to publication and wider public access (2021). Their inclusion within academic journals is considered indicative that an article has been anonymously vetted by independent experts as to minimise potentially favourable bias and is deemed to contribute valuable knowledge to the field (De Vries et al., 2009). Though reasonable arguments challenging the need for anonymised reviews to exist (see Enslin and Hedge, 2018), at time of writing, the peer-review process remains an essential check and quality control prior to a publications release to the wider public (see Cohn and Farrington, 2014; Kharasch et al., 2021; Windle and Silke, 2019:398). Thus, the decision to limit this study to peer-reviewed journal publications as the standard for inclusion has a significant impact towards limiting this study's ability to include further non-peer-reviewed publications such as government, nonprofit and for-profit

reports (i.e; grey literature), therefore restricting interpretations to that of academic contexts alone (see Hosford et al., 2021:252). This may inadvertently exclude a variety of perspectives and types of knowledge that are typically found in grey literature or other non-academic sources. Consequently, while peer-reviewed sources ensure an elevated level of scholarly rigour and credibility, they may not fully represent the broader discourse surrounding cyberterrorism and hacktivism, potentially overlooking innovative approaches and practical applications that could enrich the academic discussion.

4.5.2 Citations as a Measurement of Impact

Citations and their cumulative metrics play a key role within this study. The distribution of citations within publications (via intext-citations, bibliographies, and similar use) are used to express the critical thinking of the researchers, representing their academic rigour, familiarity with the topic, and establishes epistemological relationships between mutually relevant publications (Iqbal et al., 2021). Further, the more widely cited a publication is, the higher its impact and influence are (Sharma, 2007: 873). The influence of citations and their use as a means of measuring impact has several important influences in shaping this study's methodological framework, in turn influencing the analysis and interpretation of findings.

Firstly, as noted by Ruscio et al., (2012:125), quantifying scholarly impact by numerical values inevitably results in a loss of information, such as context and variations between research fields. For example, Garfield (1972:476) emphasised the inappropriateness of

comparing citation counts across different research fields due to the varying citation behaviours inherent in each field. This potential reflects the different norms and practices of citations within various disciplines, making direct comparisons potentially misleading. Thus, evaluating the knowledge output and publications of various fields and domains that is comprised of various and distinct disciplines, requires a nuanced approach that accounts for these inherent differences. Citation metrics, while useful, should be supplemented with qualitative assessments to capture the full scope and impact of research and not as means of numerically evaluating the 'quality' of the research and researcher.

Secondly, the study limits the publications included within the bibliometric analysis to those with a minimum citation threshold of 10 citations. Justification for this decision stems from the need to focus the analysis towards high-impact publications that can be considered to hold significant impact in shaping the domain (see Iqbal et al., 2021; Sharma, 2007). However, this decision to include only publications with at least 10 citations could potentially exclude newer or less well-known works that may still offer valuable insights or novel perspectives. While prioritising high-impact publications helps to streamline the analysis and focus on influential research, it may overlook emerging trends and important contributions from smaller or more recent studies that haven't yet reached the citation threshold.

Further, this limited threshold may inadvertently prioritise publications with multiple authors introducing concerns of collaborative bias towards multi-author publications,

which tend to accumulate citations more quickly than those authored by individuals (see Hurley et al., 2013). This can skew the analysis towards recognizing works that, while potentially influential, may represent collaborative networks rather than the merits of the research itself. As a result, as research within a domain grows, single-author studies or research from less connected academics might become underrepresented, or misconstrued as being of lesser significance, a conclusion highlighted by Aulck et al., (2018) when compared to more collaborative researchers. Therefore, the potentially impact citation metrics can contribute to assumptions towards the effectiveness and impact of single-author publications within an emerging domain should be considered when evaluating findings.

4.5.3 Content Analysis of Academic Definitions

To mitigate an earlier recognised limitation associated with bibliometrics, i.e. the loss of information by quantifying literature impact (Ruscio et al., 2012), of which often does not consider publication context. This study incorporates the inclusion of a basic (quantitative) content analysis (Drisko and Maschi, 2016:21) to provide a thorough depiction of the examined academic definitions of cyberterrorism and hacktivism. This examination is typically accomplished through frequential and descriptive analysis of term words, employing bivariate methods such as variable counts, culminating in a univariate empirical report and generalisations (Potter and Levine-Donnerstein, 1999:262). However, it is crucial to underscore that empirical findings alone do not inherently ensure the validity of a conclusion, and that although researcher self-reflection

and reflexivity are not prohibited in basic content analysis, they are seldom acknowledged or discussed in published works (Drisko and Maschi, 2016:54).

This study attempts to alleviate these concerns by adopting a taxonomic framework developed from pre-existing taxonomies as a foundation to position coding within, and later use towards the development of an ontological framework for data collection and knowledge mapping. However, a notable limitation of taxonomies is that they do not adequately distinguish between words and concepts (Schmelzeisen and Staab, 2019), a similar concern for deductive coding where the "content features that could be categorised" are done so "with little or no interpretation by the coder" (Baxter, 1991:239). Thus, when collecting, coding, and categorising definitions and terms associated with cyberterrorism and hacktivism, effort was made to best capture the contextual usage of the terms, providing further context, and categorising these terms suitably.

Chapter 5. Findings

5.1 Introduction

This thesis examines how the development and conceptualisation of cyberterrorism and hacktivism has evolved throughout 2000 to 2020, with a focus on the academic output and the conceptualisation of both phenomena. Through the evaluation of high-impact journal articles and their associated definitions of cyberterrorism and hacktivism, this research project maps the conceptual and operational development of cyberterrorism and hacktivism research.

The following sections are divided into two parts. Firstly, "*Bibliometric Findings*" presents the analysis and presentation of the 126 high-impact articles applying several bibliometric techniques using a modified integrated knowledge-mapping framework, akin to the approach employed by Reid and Chen (2006; 2008). Second, "*Quantitative Content Analysis of Definitions*" presents the examination of 237 identified definitions of cyberterrorism and hacktivism, extracting a total of 1242 terms; cyberterrorism (823 terms) and hacktivism (419 terms), which are coded and classified into a pre-existing taxonomic framework developed by Al Mazari et al. (2015) and later extended by Plotnek and Slay (2021).

5.2 Part One: Bibliometric Findings

The bibliometric analysis in this research project focused on the bibliographic details of 126 high-impact peer-reviewed academic articles. Due to the lack of consistent output of research pertaining to cyberterrorism and hacktivism from any single journal, the study adopted a PRISMA-flow framework, manual review of publications, and cut-off metric of 10 citations to capture and assess high-impact academic articles pertinent to the research aim of tracing and evaluating the academic development and status of cyberterrorism and hacktivism research.

Findings from the analysis are organised in two parts, firstly the "*Basic Analysis*" presents the general distribution of articles based on temporal and frequential patterns, highlighting trends and fluctuations over time. Secondly, the '*Citation Analysis*' is used to present in order; a performance analysis (Noyons, Moed, and Van Raan, 1999) involving the assessment of scientific actors and their influence within the research domain (Donthu et al., 2021), and later; science mapping (Cucari et al., 2023; Noyons, Moed, and Van Raan, 1999) to identify networked relationships between researchers, their sources, allowing for the evaluation of researchers, their institutional productivity, and key conceptual contributions.

5.2.1: Basic Analysis

The temporal aspect of high-impact cyberterrorism and hacktivism articles was examined by analysing the distribution of these articles over a twenty-year period (2000-2020).

Secondly, the geographical affiliations of the authors and their distribution across different countries was identified, alongside their respective journal.

Moving forward, authorship is examined to identify the total number of author affiliations to understand the collaboration patterns among researchers. Next, the analysis focused on the gender distribution of authors and their specialised disciplines to gain insights into potential gender biases, and disciplinary distribution within the field. Finally, the positioning of individual authors within the co-authorship network was extracted to identify prominent contributors and their roles.

Frequency Distribution of Articles

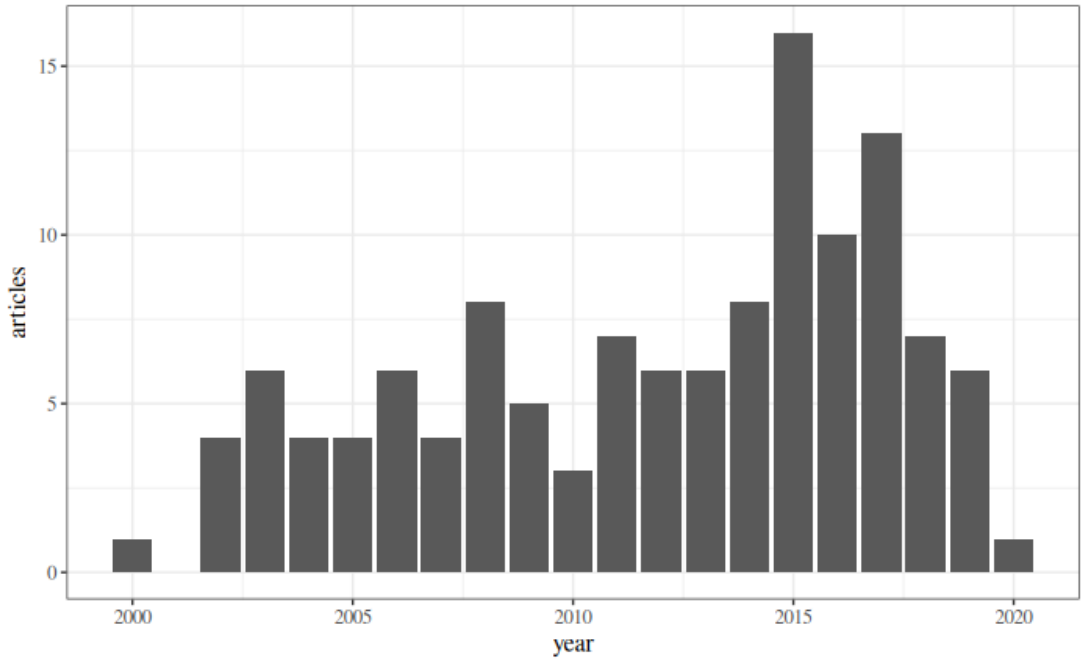


Figure 5.1 Sample Article (n126) Distribution by Year

Figure 5.1 illustrates the distribution of reviewed publications by publication year. When comparing cyberterrorism and hacktivism with well-established research areas such as terrorism studies and organised crime, it becomes evident that the former topics are new concepts that have emerged alongside the development of information communication technologies (ICT). This research project analysed academic literature spanning two decades (2000 - 2020), with Dorothy E. Denning's highly cited article "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy" (Denning, 2000a) being the earliest high-impact peer-reviewed article identified on the subject. Despite search engine results presented in chapter 6 (see able 4.3: Academic Search Engine Comparison:153) showing a substantial volume of literature associated with both topics, it is important to note that there is still a scarcity of topical and high-impact literature focusing primarily on cyberterrorism and hacktivism.

The gradual increase in the body of high-impact articles collected becomes evident when analysing the annual article trends (see Figure 5.1 Sample Article (n126) Distribution by Year:197). Following Denning's (2000a) article, within the dataset collected for this analysis, the topics of cyberterrorism and hacktivism experienced a relatively modest and stable output of four high-impact articles on average annually between 2002 and 2009, with a slight decline in 2010. Such a trend is to be expected in the initial stages of researching a novel phenomenon like cyberterrorism and hacktivism, especially when many authors contributing to this literature has a more transient status in the field. During the period from 2000 to 2010, a total of 45 articles were published, authored by a

collective of 51 individual authors. Notably, only five authors (representing 7.8% of the total 51 authors) contributed more than one article within this first decade.

In contrast, the academic growth post-2010 witnessed a remarkable surge in high-impact articles compared to previous years, with an average annual growth rate of 7.25% between 2011 and 2020, resulting in an average output of 8.2 articles per year. Throughout this decade, and encompassing the complete collection of publications analysed, the year 2015 exhibited the most significant growth, with a total of 16 high-impact articles published in 15 journals, produced by 19 (18.4%) independent authors out of the total 103 authors who published between 2011 and 2020. Overall, the literature has maintained an average annual growth rate of 22.42% between 2000 and 2020, although there is a noticeable decline in high-impact literature output after 2015.

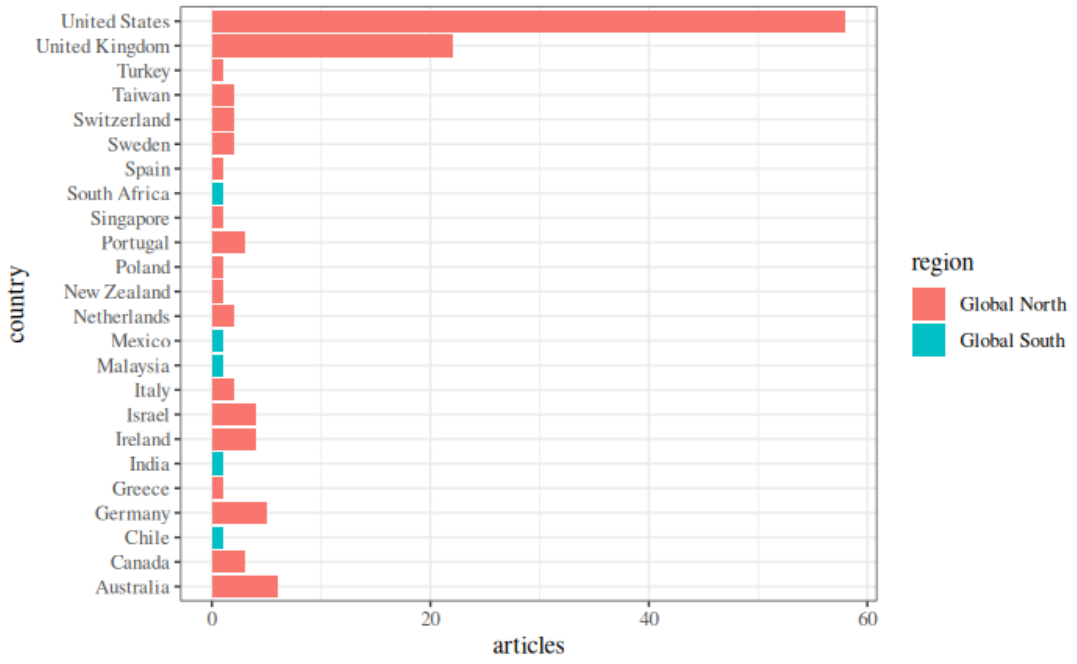


Figure 5.2 Distribution of Article Affiliation Organised by Country

The geographical distribution of literature is based on the affiliation of the first author. As depicted in figure 5.2, the bar chart representing the number of articles per country reveals that a majority of 122 (96%) publications stems from articles affiliated with institutions in the global north (illustrated in red). Notably, the United States emerged as the most prominent contributor, with a total of 58 (45.7%) articles, followed by the United Kingdom with 23 (18.1%) articles. In contrast, contributions from the global south (illustrated in blue) were limited, with only five single contributions per country: South Africa, Mexico, Malaysia, India, and Chile. This pattern aligns with similar findings from the examination of authorship trends in organised crime research (Hosford et al., 2021), which highlighted the dominance of the Global North in knowledge production in that domain.

Distribution of Articles by Journal

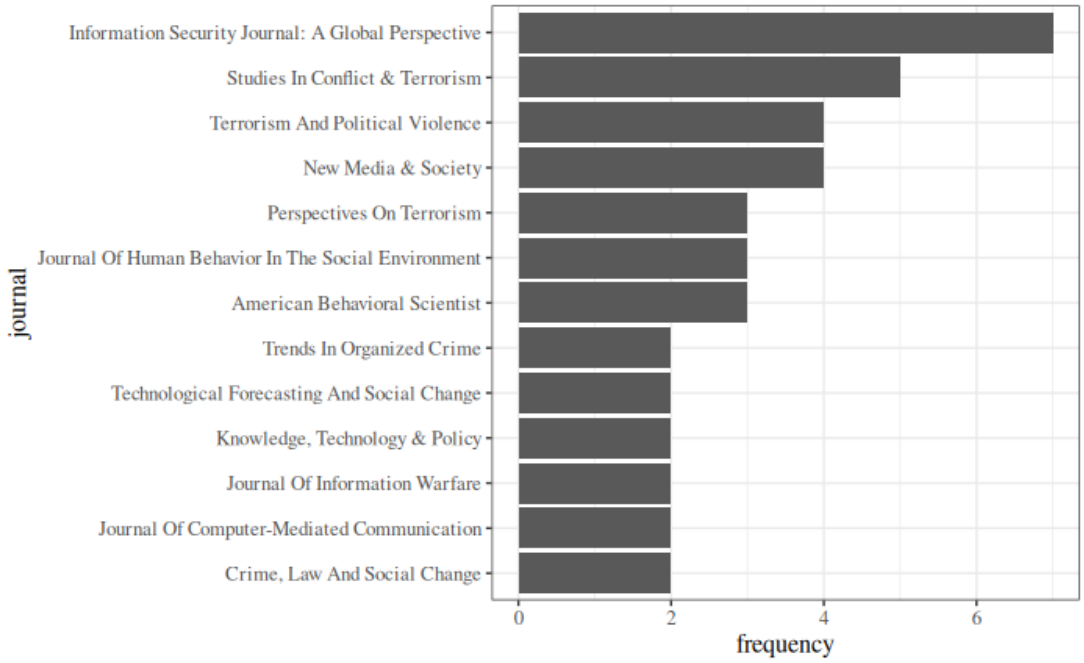


Figure 5.3 Journal Distribution

The total 126 high-impacted articles examined originated from 98 distinct journals. 13 of these journals published two or more articles as illustrated in figure 5.3. The bar chart illustrating the distribution of multiple publications within journals, shows the substantial number of unique journals reflects the absence of consistent and regular single-journal output focusing on the domains of cyberterrorism and hacktivism research, either as independent phenomena or as part of a shared body of work.

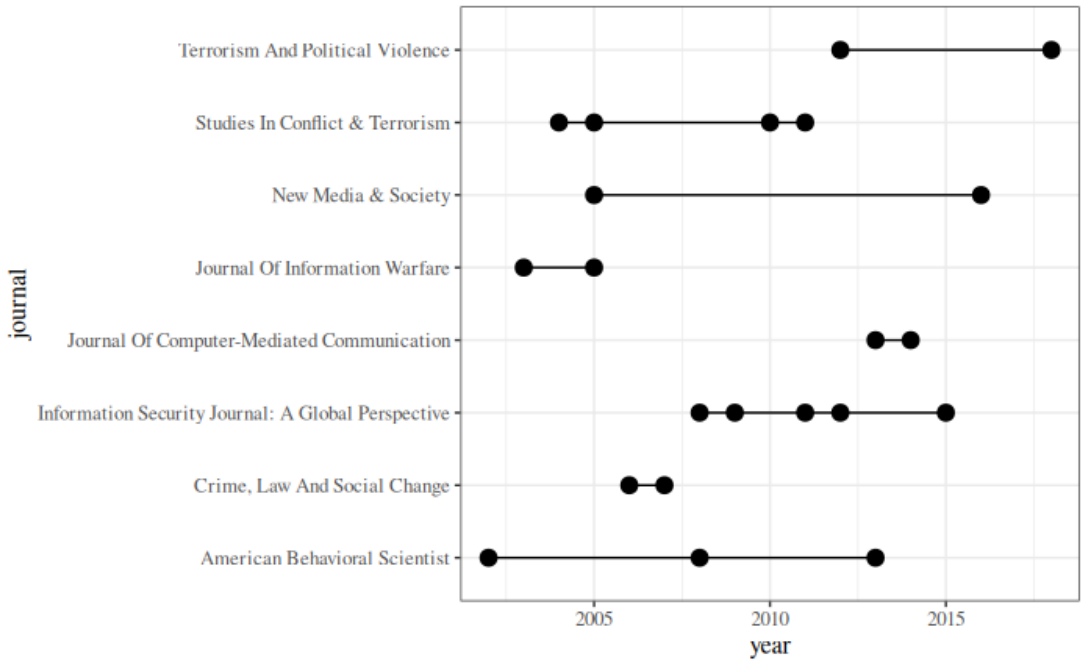


Figure 5.4 Annual Distribution of Journal Output

The scarcity of well-established and specialised journals on the topic of cyberterrorism and hacktivism becomes increasingly apparent when examining the level of productivity these journals exhibit towards cyberterrorism and hacktivism research. Figure 5.4 provides a visual representation of the annual distribution of journals via dot-points representing each article, linked to their affiliated article from the same journal which has produced two or more high-impact articles on cyberterrorism and hacktivism that, over a span of 20 years (2000-2020). Notably, during its peak, only four journals managed to publish four or more articles of considerable impact on these topics. Among them, two journals were focused on terrorism studies, one on media, and another on information security.

Moreover, the distribution of literature across these journals appears scattered, suggesting that while editorial calls for submissions might have been open, there may not have been explicit interest to actively solicit contributions specifically related to cyberterrorism or hacktivism. However, it is worth mentioning that a noteworthy surge in interest occurred between 2010 and 2015, wherein there was a significant increase in submissions and editorial attention towards research on cyberterrorism and hacktivism. During this period, six out of the 13 journals in question produced two or more high-impact articles on these subjects. Interestingly, this trend aligns with the annual distribution of the overall literature collection of high-impact articles, which observed a gradual rise in article volumes, reaching its peak in 2015. The analysis reveals that only a limited number of journals have produced multiple high-impact articles on these topics, and that their distribution is scattered. While the data analysed for this study presents an increase in submissions regarding cyberterrorism and hacktivism between 2010 and 2015, overall, there is a dearth of consistent and annual journal articles dedicated to these subjects producing high-impact studies.

Descriptive Analysis of Authorship Distributions

In the following section, the data pertaining to authorship patterns will be presented. The dataset of 126 high-impact articles is composed of 145 individual authors, having a total of 185 author appearances (individual authors can attribute multiple publications). The primary focus of this section centres on investigating the distribution of authorship regarding country of affiliation, gender, and collaborative efforts.

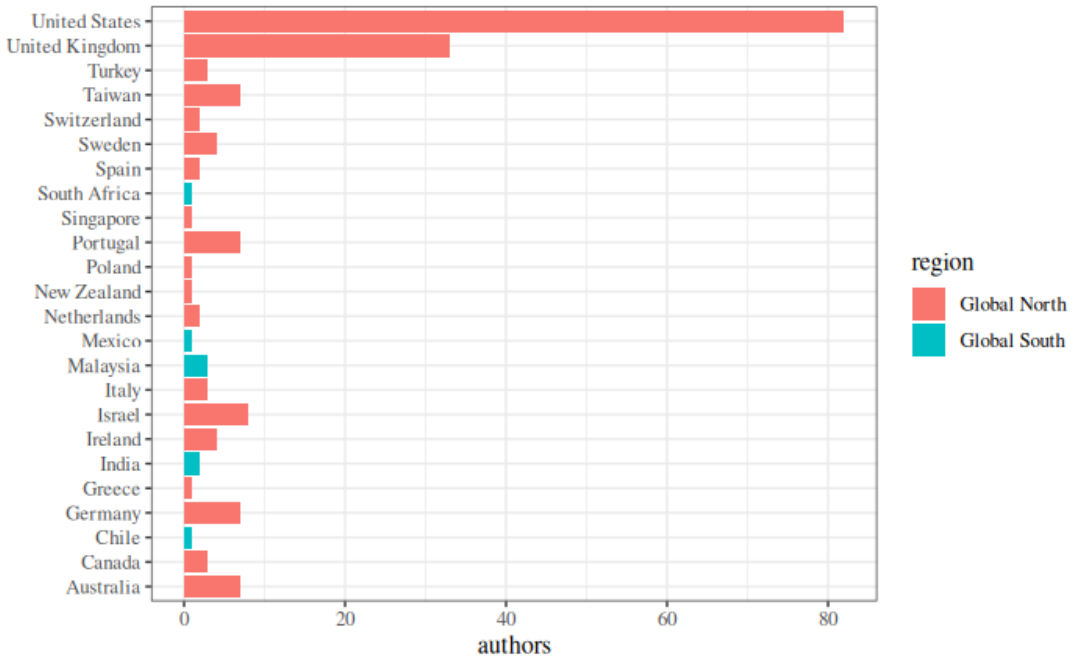


Figure 5.5 Authorship by Country Affiliation

Like figure 5.2, figure 5.5 reveals certain patterns in geographical affiliation. Authors affiliated with institutions in the global north accounted for 97.3% (180) of total appearances, while only 4.3% (8) of authors had affiliation based in the global south. Specifically, the United States represents the largest number of authors affiliated with the global north, with a total of 82 (44.3%) author appearances, followed by the United Kingdom with 33 (17.8%) appearances. Combined, the United States and the United Kingdom dominate a sizeable portion, amounting to 62.2% of the total author appearances.



Figure 5.6 Distribution of Author Appearance by Continent

When examining author affiliations grouped by continent, as depicted in figure 5.6, a noticeable dominance becomes apparent for authors within North American (86) and European (66) institutions including the United Kingdom. Notably, both Africa and South America exhibit the weakest representation, each with only a single high-impact article represented from their respective continents.

The disparity between authors affiliated within the global north and global south has been extensively explored by scholars. Chakrabarty (2008) critiqued prevailing world history narratives and scientific progress accounts, which have been biassed towards Euro-centric perspectives, portraying non-Western regions as passive recipients of European advancements that unfold over time and disseminate unidirectionally from core to peripheral countries. Conversely, Raj (2007:7) argues that science often emerges within

the context of colonialism and imperialism, arising from intricate interactions and negotiations between colonists and the colonised. This viewpoint posits science as a product of co-production, reflecting not only imperial dominance but also the influence of imperial science itself.

In the context of Africa and its research and publishing landscape, it is evident the continent's scientific contributions make up only 1% of the global research output (Collyer, 2018). Asare et al. (2021) further highlights the weaknesses in Africa's publishing industry, characterised by a lack of distribution hubs and intra-Africa book trade, alongside educational curricula, pedagogy, and learning processes that remain rooted in the colonial legacy. Additionally, the absence of a robust scholarship culture presents challenges to the advancement of academic endeavours in the region (Asare et al., 2021; Amutuhaire, 2022).

Moreover, it has been suggested that knowledge production does not follow a single, unified stream, but rather operates through diverse circuits regional and transregional, often emerging in response to global publishing inequalities (Collyer, 2018:66). The presence of these diverse circuits poses difficulties in both disseminating knowledge and findings across borders and in capturing and evaluating such knowledge.

Distribution of Author Gender

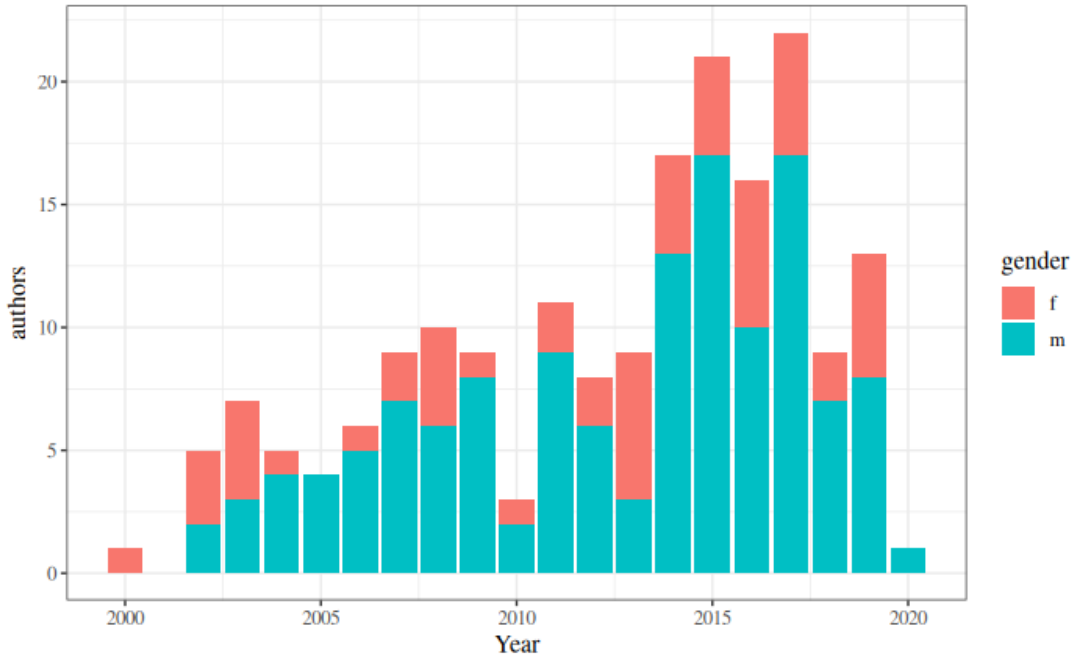


Figure 5.7 Distribution of Gender by Year

When examining the distribution of authors' appearances by gender, it becomes evident that male authors (blue | 132) significantly outnumber female authors (red | 54). Notably, none of the authors recorded in this research project made explicit within the 126 publications reviewed, that they self-identified outside a classical dual-binary gender system, and there were no distinct self-identifications as non-binary or other genders. The data on gender was meticulously collected, relying on authors' self-descriptions or third-person descriptions of the authors and their work at the temporal point of publication if self-descriptions were unavailable. In cases where information on authors was scarce, particularly with single authors who often only contributed a single high-impact article to the dataset, extensive efforts were made to ascertain gender confirmation based on further

publications associated with the author, or if these options are exhausted, the geographical origin of their names and its associated gender.

Figure 5.7 visually represents this gender distribution over the 20-year period. Interestingly, the first three years of articles (2000, 2002, and 2003) witnessed most female authors as contributors of high-impact articles. However, there was a significant decline in 2004, with a female-to-male author ratio of 1:4. Subsequently, the ratio remained relatively static until 2013, when the female-to-male ratio reached 2:1. Nevertheless, the ratio returned to pre-2013 levels shortly thereafter, with fluctuations that leaned more towards male authors in the years that followed.

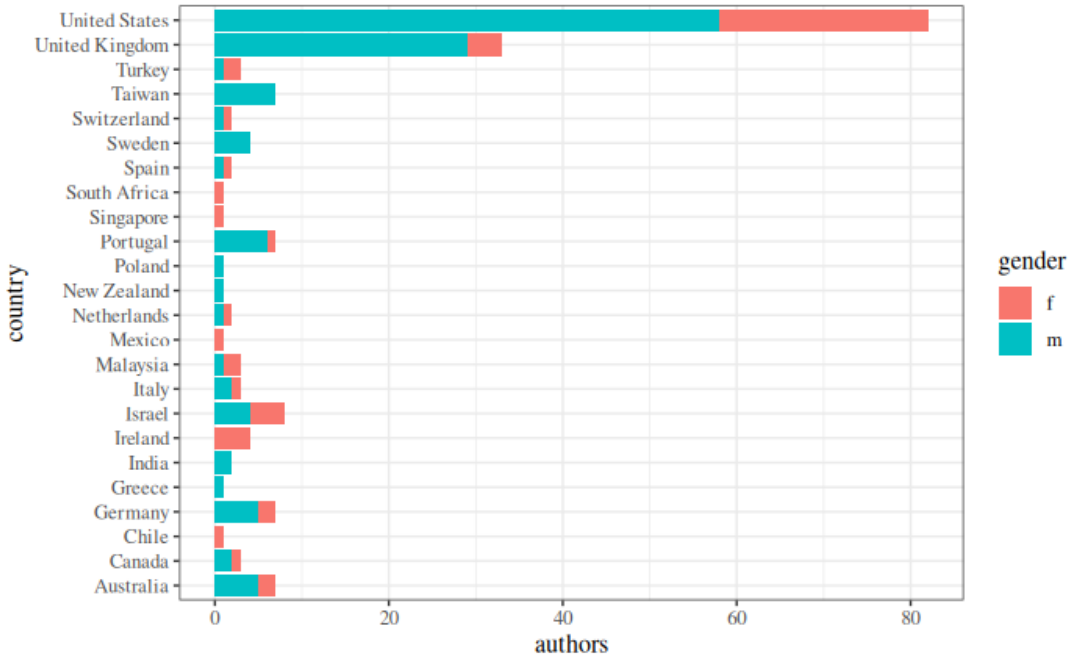


Figure 5.8 Distribution of Gender by Country Affiliation

The geographical analysis of the literature reveals a significant gender disparity, with male authors from the global north dominating the representation. Among the total 185

author appearances which includes authors with multiple high-impact publications, only 27.2% (red | 54) are female. Specifically, within the United States, there are 24 female contributors compared to 58 male contributors (visualised as blue). The gender contrast is more pronounced in the United Kingdom, with only four female contributors as opposed to 29 male contributors. Outside the United States and the United Kingdom, no consistent gender contrast is apparent. For instance, in the global south, there are 5 female contributors and three male contributors representing five countries (South Africa, Mexico, Malaysia, India, and Chile).

Within the global north, excluding contributors from the United States and the United Kingdom, there are 21 female contributors and 42 male contributors among the 63 total contributors. As shown in figure 5.8, this distribution does not provide enough observable data points to make any meaningful comparisons. The evident gender disparity in authorship within the global north amongst high-impact articles is disheartening, but not unexpected. Fahmy and Young (2017) observed a gender-based stratification in co-authorship patterns within criminology and criminal justice journals. Their findings indicate a tendency for males to collaborate predominantly with other males, while females are more inclined to co-author articles with males (Fahmy and Young, 2017:285), later quoting Fisher et al., (1998) who stated that gender formation of research alliances has potential consequences for inequality in scholarly production and attribution." Therefore, "women are more likely to be excluded from research collaboration" (Fisher et al., 1998:21).

Distribution of Author Position

The significance of collaborative work in scientific research is widely acknowledged (see Fisher et al., 1998; Hosford et al., 2021, Smith et al., 2023). The increasing specialisation and complexity of research questions, coupled with the excessive costs of conducting research, often exceed the feasible means of many academic researchers, making collaboration essential. Moreover, fostering collaborative endeavours is advantageous on several fronts. Collaborations provide researchers with broader and easier access to public funding, while affiliating with well-established research groups enhances visibility and facilitates higher productivity (Lee and Bozeman, 2005). Additionally, collaborative efforts promote the inclusion of multidisciplinary and transnational perspectives, enriching the research process with diverse insights and expertise.

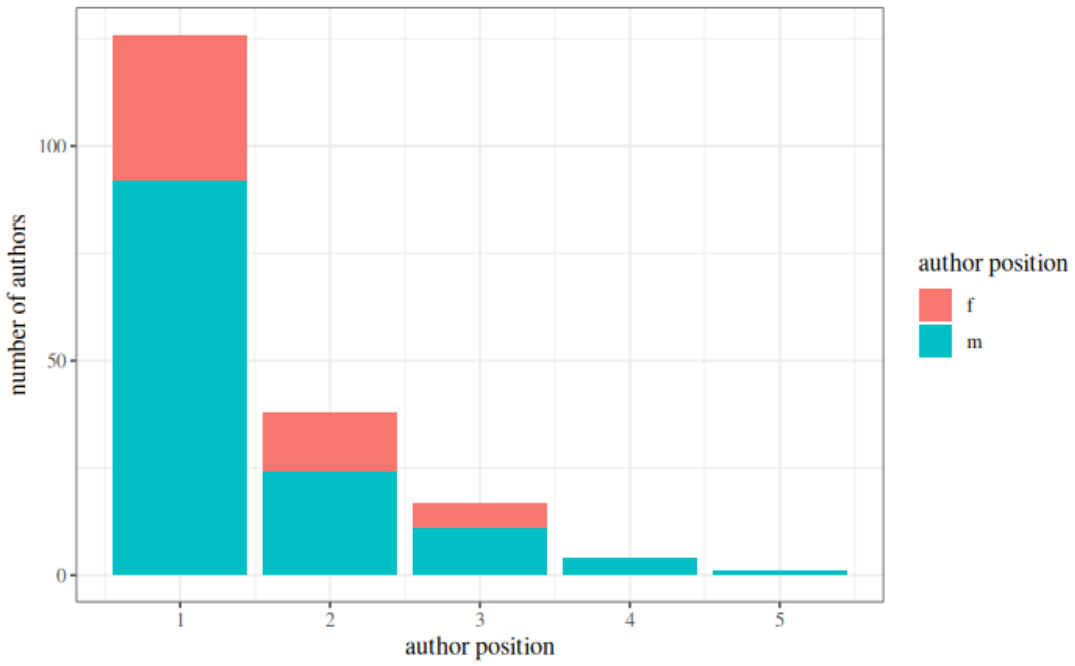


Figure 5.9 Distribution of Gender by Author Position

Figure 5.9 presents the distribution of authors based on their acknowledged position within the publications list of authors (1 being first author cited, 2 being second author cited, and so on), with author gender distinguished by colour shade (red = female, blue = male). A significant portion of the articles collected for this study consisted of single-authored articles (67.3% | 88). Of the 145 individual authors included in this study 11% (16) have contributed more than one high-impact article, and 4.1% (6) have contributed three or more articles. Similar low retention rates can be observed in related criminological topics, such as terrorism and organised crime. In the case of organised crime research, von Lampe (2015; 2017) attributes the low retention of frequent authors to the lack of specialisation.

Limited specialisation leads to fewer opportunities for collaborative work and focused discussions within research communities, hindering the development of common conceptual frameworks and data collection approaches involving external data-holders (Hosford et al., 2021). Consequently, the potential for significant advancements and comprehensive insights within the field is constrained, thus warranting an evaluation of the discipline distribution amongst authors.

Distribution of Author Discipline

The academic background and discipline of researchers play a critical role towards the development of a domain, and its' establishment of 'normal science,' where the domain's paradigm is established, leading to key theories and conceptual frameworks to be established (Kuhn, 1970:180).

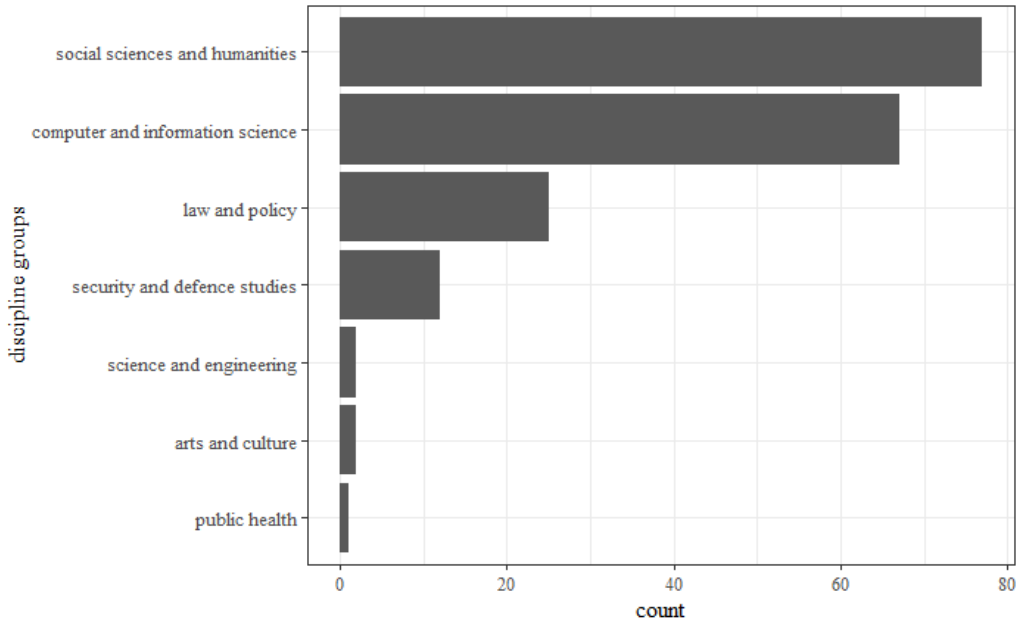


Figure 5.10 Distribution of Discipline Groups by Author count

Having mapped the disciplinary primary degrees and focus of authors identified within the dataset (alias; *disciplines*) using both in-document descriptions, and/or available information online with attention towards the date of the publication, figure 5.10 illustrates two notable key groups of disciplines; 'social sciences and humanities' (77), and 'computer and information science' (67). This is unsurprising, with Payne and Hadzhidimova (2020:86) noting that researchers have increasingly recognised the interdisciplinary nature of cybercrime research. This vibrant interdisciplinary distribution is further solidified by the nuanced distribution of disciplines associated with individual authors.

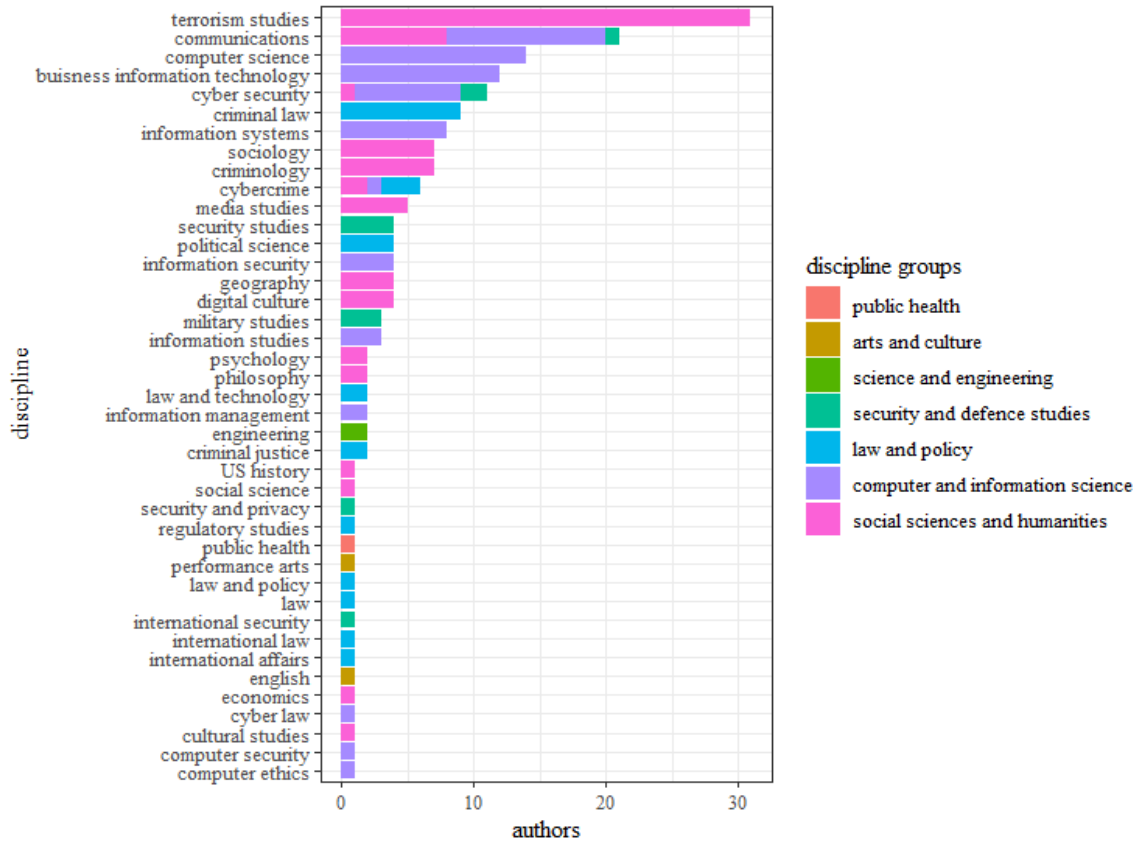


Figure 5.11 Distribution of Author Discipline by Gender

Figure 5.11 shows a vertical bar graph that displays the number of authors across various academic disciplines (grouped and coloured by their overarching 'discipline groups'). Each bar represents a different discipline, listed on the y-axis, with the count of authors shown on the x-axis. As demonstrated in figure 5.11, the interdisciplinary nature of cyberterrorism and hacktivism research mirrors that of cybercrime research. Cybercrime is frequently employed as a comprehensive term, covering a variety of illicit activities occurring through the internet or within computer systems, exploiting vulnerabilities in intricate information systems or infrastructures (Finklea & Theohary, 2012, Wu et al.,

2023), with these activities attracting researchers of various disciplines. The variety of disciplines within publications focusing on cyberterrorism and hacktivism demonstrates the same complex and multifaceted domain seen in cybercrime research, requiring diverse perspectives and expertise to fully understand and identify the broad implications across different fields of study. Yet, as later findings suggest, coinciding with similar bibliometric findings by Wu et al., (2023), contemporary research on cyberterrorism and hacktivism is highly fragmented with limited collaboration, leading to separate investigations by social scientists, mainly terrorism studies experts (31), and computational scientists (14), communication scientists (21), and business information scientists' technology scientists (12).

Collaboration by Affiliation

The literature examined in this study did not reveal any evidence of transnational collaboration among authors. However, at a national level, there were 24 (19%) co-authored articles within the sample of 126 articles with collaboration between authors from different institutions.

For authors with internal affiliation (authors who collaborate within the same institution), a total of 13 articles: 9 written by two authors, 3 by three authors, and a single article by five authors were identified. Notably, none of the authors within this group contributed more than one high-impact article, suggesting a potential lack of repeated collaboration among them. The absence of transnational collaboration and limited internal affiliations underscores a potential need for fostering collaborative efforts and interdisciplinary

engagements to enrich the research landscape and promote wider knowledge communication and exchange.

Within the external affiliation group (authors who collaborated with individuals outside their institution), a total of 23 high-impact articles composed by 35 authors were identified. Among these authors, 22 (62.8%) contributed only one article each, while 13 (37.1%) authors made two or more contributions to different articles. Notably, the external affiliation group exhibits multiple collaboration networks, wherein authors have collaborated with both frequent collaborators and new authors from external institutions. To note, all collaborations captured were within the same country of the first author's affiliation.

The observation underscores the common occurrence in many fields, where single-authored articles outnumber co-authored works (see Del Carmen and Bing, 2000; Lemke et al., 2015). However, co-authored articles that involve contributors from external institutions tend to yield notable advantages (Freshwater et al., 2006). Firstly, they often result in multiple contributions to the research topic, leading to a series of related articles, further bolstering a concise network of knowledge, especially when in the initial stages of development. Secondly, such collaborations often encourage further cooperative efforts with external contributors, resulting in additional articles, further expanding the interconnected network of articles, cohesive language, and domain norms and assumptions, thus furthering the likelihood of ‘normative science.’ Lastly, these collaborations aid towards establishing and legitimising key contributors as active

participants within the research field (Freshwater et al., 2006), allowing key theories and assumptions concerning the domain to be solidified.

Thus, when comparing the earlier findings concerning the distribution of disciplines, and the high number of single authors. The domain of cyberterrorism and hacktivism research is ripe for a rich and collaborative network of multi-disciplinary researchers that could add further contributions towards the domain, and thus expand towards a concise paradigm. However, as noted with the earlier dispersion of journals, efforts towards consolidating this rich group of disciplinary interest may prove difficult.

Identifying Core Contributors

To identify core contributors in the cyberterrorism and hacktivism literature, citation counts are used (see Cohn and Farrington, 2014). In this study, citation data was collected using Google Scholar, and only articles with a minimum threshold of 10 citations were included in the analyses.

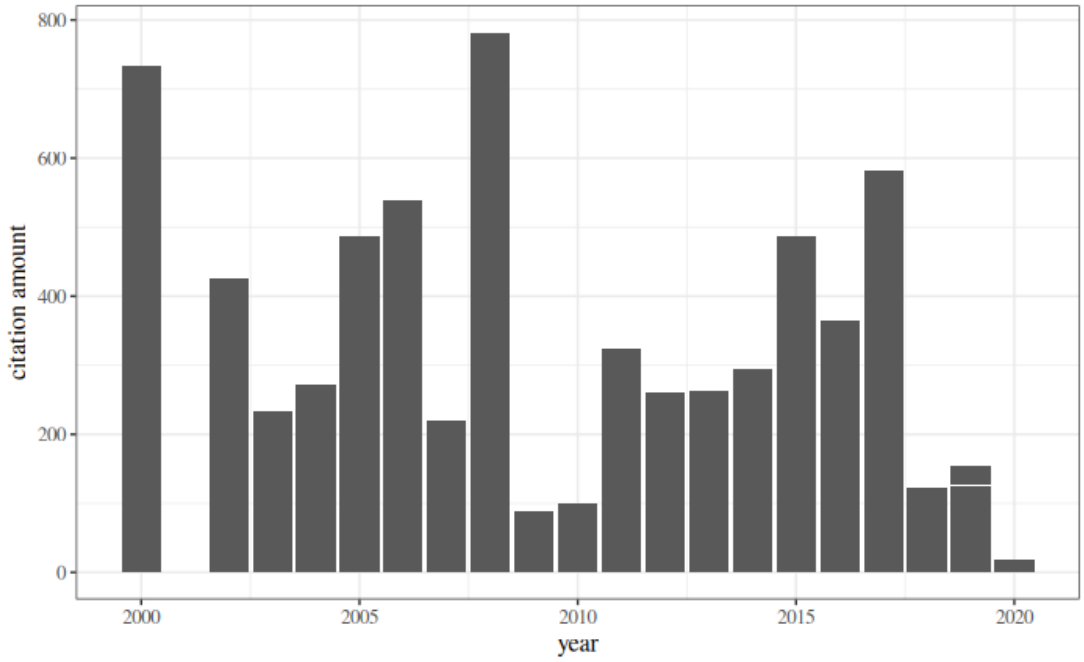


Figure 5.12 Citation Distribution per Year

The citation distribution, as depicted in figure 5.12 bar chart, presents the annual distribution of citation metrics across the 126 high-impact articles analysed, with table 5.1 below presenting a list of articles with the highest citation impact.

Table 5.1 Ten Highest Cited Articles

author	title	citations
D.E. Denning	Activism, hacktivism, and cyberterrorism	734
V. Carducci	Culture Jamming: A Sociological Perspective	251
G. Weimann	Cyberterrorism: The sum of all fears?	231
M.D. Cavelty	Cyber-Terror: Looming Threat or Phantom Menace?	179
KK.R. Choo	Organised crime groups in cyberspace: a typology	167
G. Weimann	The Psychology of Mass-Mediated Terrorism	167
P.A. Taylor	From hackers to hacktivists: speed bumps on the global superhighway?	151
A.R. Shrock	Civic hacking as data activism and advocacy	147
M. Stohl	Cyber terrorism: a clear and present danger	141
M. Conway	Reality bytes: cyberterrorism and terrorist ‘use’ of the Internet	126

When examining individual articles, we can isolate 10 of the most highly cited articles as shown in table 5.1, representing the key authors cited names, publication title, and the total number of citations captured during the data collection process (dated 2021). Denning's (2000a) study titled “Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy,” first published in Computer Security Journal in 2000, stands out as both the earliest seminal work in the field. It has garnered a total of 734 citations at the time of analysis and can be considered one of the most impactful overviews about cyberterrorism and hacktivism.

Denning's work is significant as it contributed towards introducing the concepts of cyberterrorism and hacktivism into the academic literature. It achieved this by gathering various testimonials from key event speakers, incorporating case studies from diverse sources like news articles and technology blogs, and incorporating operational definitions provided by US state agencies. The study also hypothesised potential examples and comparisons of each phenomenon. Through this literature review, Denning established a comparable framework for further research, providing academics with a baseline from which to advance their investigations in this domain.

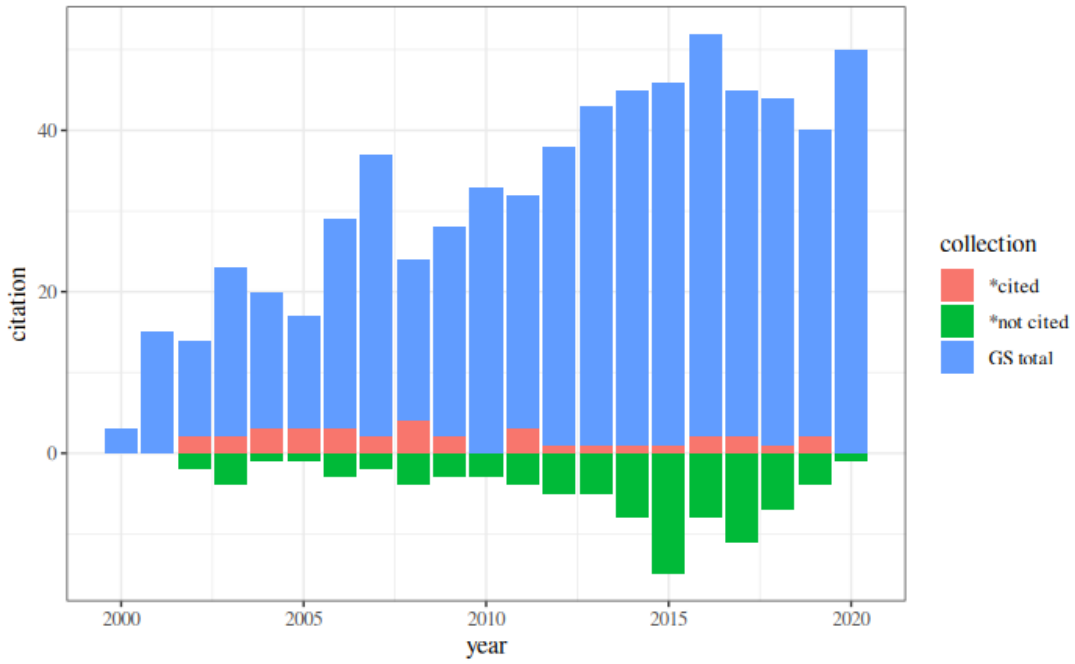


Figure 5.13 Denning (2000a) citation distribution over time

Within the 126 high-impact articles collected for this research project, Denning's (2000a) article is cited 27.4% (37) times, as represented in figure 5.13 under the label "*cited." The high citation count for Denning (2000a) is in large part since the article has been

available and cited for over twenty years, however, the sustained interest in the article is demonstrated by the fact that there were 50 citations in 2020.

In addition, the increase in citation can be primarily attributed to Denning's well-regarded approach in defining the phenomenon of cyberterrorism. Stohl (2007:230) argues that no compelling theoretical or practical arguments have been put forward to reject Denning's approach to defining cyberterrorism. This recognition of Denning's work has contributed to its enduring impact and continuous growth in citations over time, making it a cornerstone contribution within the field of cyberterrorism and hacktivism research.

Core Contributors by Article Volume

Within this thesis, a core contributor is characterised as an author who makes substantial and repeated contributions to a specific field over a meaningful timeframe. To discern this core group of researchers within the dataset, a standard frequency analysis was conducted to identify authors who have published two or more articles. Despite the notable prevalence of authors who have produced single articles, a proportion of 13.1% (19) among the 145 individual authors have actively produced two or more articles recorded within the dataset. Remarkably, the highest number of articles attributed to a single author within the dataset amounts to nine articles.

Table 5.2 Core Researchers within the Collection of Articles

author	no. of articles*	year coverage*	total citation*
J. Matusitz	9	2008-2014	158
S. Macdonald	6	2014-2018	171
L. Jarvis	6	2014-2017	171
M. Conway	4	2002-2011	242
A. Whiting.	3	2015-2017	62
T. Holt	3	2012-2019	158
J. Hua	3	2012-2018	151
E. Minei	3	2011-2012	34
G. Weimann	3	2005-2012	474
S.M. Chermak	2	2017-2019	69
J.D. Freilich	2	2017-2019	69
D. Canetti	2	2016-2017	99
M.L. Gross	2	2016-2017	99
D.R. Vashdi	2	2016-2017	99
S. Bapna	2	2012-2013	126
H.C. Chao	2	2009-2011	23
H.C. Chu	2	2009-2011	23
D.J. Deng	2	2009-2011	23
F. Papadimitriou	2	2006-2009	35
KK.R Choo	2	2008	295

Note: (*) pertains to research articles collected and analysed within the bibliometric dataset

Table 5.2 presents a list of 20 core contributors in the cyberterrorism and hacktivism literature, based on the number of high-impact articles contributed to the dataset collected, the number of times their research appears within the dataset, the year of coverage, and the total citation amount of the articles. Among these contributors, the median of articles from authors with multiple contributions is 3.16, with most authors (11) having contributed two articles.

All these core contributors are affiliated with academic institutions located within the global north. The United States has the highest representation with seven contributors, followed by Israel with four, the United Kingdom and Taiwan with three each, and Australia, Greece, and Ireland with one each. This geographical distribution highlights the dominant presence of contributors from the global north in the research field of cyberterrorism and hacktivism.

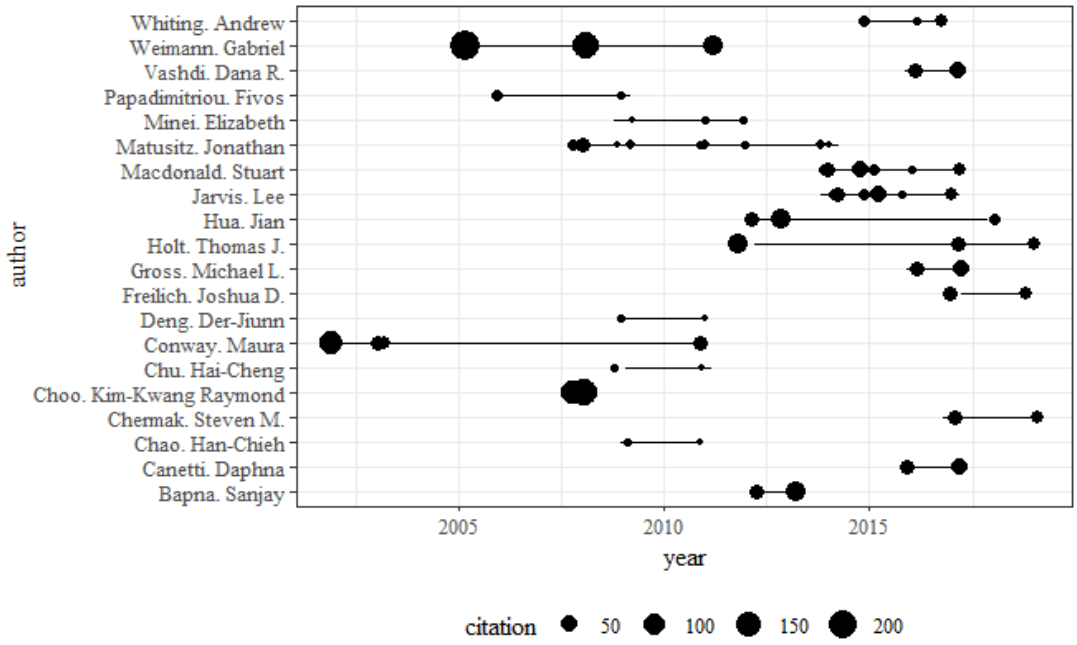


Figure 5.14 Distribution of Author Contribution by Year

Figure 5.14 provides a visual dot-chart representation of the distribution of core contributors identified in table 5.2, presented along a yearly linear timeline with points representing their publications included in this study, and the sizes representing their citation amount at time of collection. In this visualisation, the size of each data point corresponds to the number of citations received by the respective article. By mapping author contributions of high-impact articles along this yearly timeline, we gain valuable insights into the citation performance and frequency of the identified core authors' contributions over the years.

Analysing the data points on the timeline enables us to identify and compare the yearly outputs of these core authors in terms of both citation performance and article frequency. Larger data points indicate articles that have received a higher number of citations,

suggesting their significant impact within the field. Conversely, smaller data points represent articles that have garnered fewer citations, implying lower impact.

Summary of Basic Analysis

To summarise, part one of the bibliometric analysis of cyberterrorism and hacktivism literature examines various aspects of the research such as their temporal distribution, geographical affiliations of authors, associated journals, authorship patterns, and gender representation. It reveals that cyberterrorism and hacktivism are recent concepts that have emerged with the development of information communication technologies (ICT). Over the past two decades, the academic growth in this field has seen a significant surge, especially after 2010, reaching its peak in 2015. Despite this growth, there remains a scarcity of dedicated journals, which poses challenges in obtaining comprehensive and specialised information.

The geographical distribution of the literature reveals a noticeable dominance of contributions from the global north, particularly from the United States and the United Kingdom. This concentration accentuates the need to foster more representation and inclusivity from researchers based in the global south to ensure a more diverse and holistic understanding of cyberterrorism and hacktivism. Further, gender representation among authors displays a substantial disparity, with male authors significantly outnumbering female authors. This finding emphasises the urgency to address gender imbalances within the field and promote greater gender equality in research and scholarship.

Lastly, collaborative efforts in scientific research are vital, although researchers identified within the study present an array of disciplines that all play a substantial and beneficial role in better understanding cyberterrorism and hacktivism from a multi-dimensional and holistic perspective, the study identified a lack of transnational collaboration among authors. Most collaborations occur at the national level, indicating the potential for increased international cooperation to enrich the research landscape with sharing of data, and contributions by diverse perspectives and expertise.

5.2.2 Citation Analysis

The present research project adopts a comprehensive approach that integrates the cyberterrorism and hacktivism literature, justifying this decision based on several reasons. Firstly, as demonstrated in previous sections, Denning's (2000a) seminal work provides a fundamental framework for discussing these emergent topics as interconnected yet distinct phenomena. Secondly, a significant portion of the literature examined during the early stages of the research frequently employs both terms (Hampson, 2012; Drmola et al., 2015; Beck, 2016; Mezei, 2018), either following Denning's approach (Stohl, 2007; Hua et al., 2018) or using the terms interchangeably without clear differentiation (see Krapp, 2005).

Furthermore, both cyberterrorism and hacktivism share noteworthy similarities, primarily in their use of political and ideological motivations, similar operational tactics, and potential impacts. If we were to merely analyse the terms independently, deconstructing them into "cyber" and "terrorism" and then "hacking" and "activism," this would identify

clear distinctions between the phenomena. However, such an approach would neglect the existing relationship between cyberterrorism and hacktivism research, which holds value in comprehending and accurately understanding both phenomena through rigorous scientific analysis, rather than basing the distinction solely on the terminology, which poses definitional challenges in their respective contexts.

Hence, to establish the necessity of delineating cyberterrorism and hacktivism as distinct entities, it becomes imperative to recognize and acknowledge the interconnectedness of research articles in these fields, which underscores the significance of defining each phenomenon separately.

This section employs bibliometric coupling as the primary method for identifying distinct clusters of academic literature and potential connections to related concepts. In contrast to Reid and Chen's (2006) approach, which uses co-citation analysis to visualise the frequency of citations among multiple articles (Griffith, 1974; Small & Griffith, 1974), this section introduces bibliographic coupling as the initial measurement and classification method. Rather than relying on how often articles are cited together by other works, bibliographic coupling examines the presence of a third article cited by both articles (Kessler, 1963). The greater the number of shared citations between articles, the stronger the bibliographic coupling.

While bibliographic coupling has received criticism, notably from Martyn (1964), who questioned its validity as a measure due to the potential variance in the context of citation

usage, it is important to consider the circumstances under which this criticism was raised. Particularly, when dealing with a vast dataset comprising tens of thousands of articles with limited knowledge of their context, Martyn's critique holds significance. However, in the case of smaller, more well-defined datasets where the context of articles is better understood within the general discipline, bibliographic coupling can prove to be a valuable tool for identifying groupings of articles based on the similarity of their citation patterns. In such contexts, bibliographic coupling can be leveraged effectively for the purpose of discerning meaningful relationships among academic works.

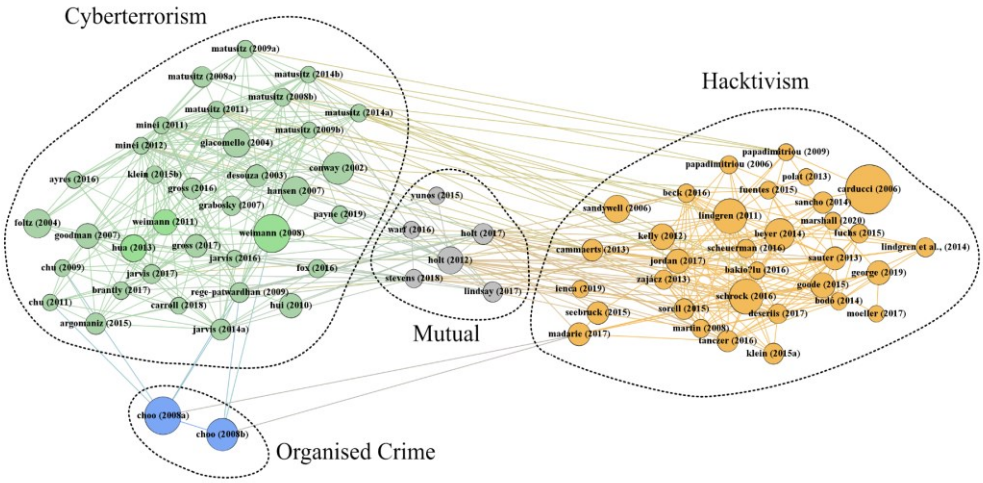


Figure 5.15 Group Clustering via Bibliographic Coupling

Figure 5.15 presents a network graph that visually depicts the interconnections among the collected articles in the dataset. Notably, two distinct and prominent clusters of articles, represented by circular nodes, are observable at opposite ends of the network graph. The spatial proximity of nodes reflects the similarity in citation patterns, while the size of each node is proportional to the number of citations specific articles have received. To ascertain

the primary focus of each individual node within the clusters, a comprehensive review was conducted, classifying them as pertaining to cyberterrorism, hacktivism, or both, with these clusters demarcated by dashed boundaries.

The formation of groupings in this manner facilitates the clustering of articles sharing common citation patterns and thematic concerns. Following a thorough analysis of the node clusters, four discernible groups emerged:

- **Cyberterrorism:** Comprising primarily literature centred on cyberterrorism as its primary focus.
- **Hacktivism:** Consisting of literature centred on hacktivism.
- **Mutual:** Encompassing literature that addresses both cyberterrorism and hacktivism in a balanced manner, without a specific primary focus on either.
- **Organised Crime:** Comprising two articles authored by Choo (2008), also collaborating with Smith (Choo and Smith, 2008), concentrating on the exploitation of online systems by organised crime groups.

The interrelationships among these groups are indicated by "strings" or, more appropriately, "links" connecting the nodes. The density of these links between grouped clusters signifies the strength of the relationships shared among the clusters. While the precise intricacies of these linkages may be challenging to discern directly from a static figure, they effectively illustrate the extent of shared citations between individual articles and contribute to our understanding of their interconnectedness.

With reference to figure 5.15 (page 229), the application of bibliographic coupling demonstrates that a strong association between the two main topics (cyberterrorism; hacktivism) exists as they frequently cite similar sources in conjunction with each other.

Co-citation Analysis of Key Sources

The study identified a total of 3,346 unique citations, including journals, news agencies, conferences, reports, and others, within the 126 high-impact articles by employing co-citation analysis via VOSviewer. However, when considering citations that appear 10 or more times within the collection, this number decreased significantly, representing a mere 0.68% (23) of the entire set of unique sources. It was observed that six of these sources were duplicate pairs, arising from minor variations in their titles, such as the inclusion of "the" at the beginning or the substitution of "and" with an ampersand ("&"). These duplicate pairs were appropriately merged, resulting in a total of 20 distinct sources that appeared 10 or more times within the collection of articles, or 0.59% of the total number of unique sources identified.

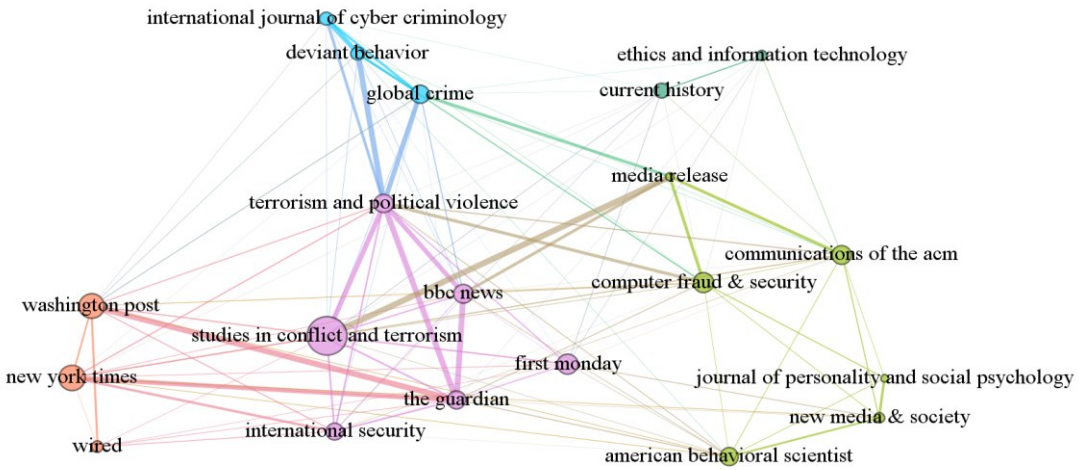


Figure 5.16 Co-citation of Article Sources

The network file extracted from VOSviewer was further analysed using the open-source network analysis tool, Gephi, to achieve more detailed and customizable visualisation. Figure 5.16 presents the resulting network, showcasing the interrelationships among the top 20 information sources identified within the article dataset. These sources can be broadly categorised into four types: journals (14 | 70%), news media (4 | 20%), magazines (1 | 5%), and state media (1 | 5%).

Table 5.3 Top Information Sources

no.	**source**	**citation**	**type**
1.	Studies in Conflict and Terrorism	44	journal
2.	New York Times	31	news agency
3.	Terrorism and Political Violence	29	journal
4.	The Guardian	26	news agency
5.	Washington Post	23	news agency
6.	Media Release	17	state agency
7.	Wired	15	magazine
8.	New Media & Society	14	journal
7.	First Monday	13	journal
10.	American behavioural Scientist	12	journal
11.	Computer Fraud & Security	12	journal
12.	International Security	12	journal
13.	Global Crime	11	journal
17.	Deviant Behaviour	10	journal
20.	Journal of Personality and Social Psychology	10	journal
15.	Communications of the ACM	10	journal
18.	Ethics and Information Technology	10	journal
17.	International Journal of Cyber Criminology	10	journal
14.	BBC News	10	news agency
16.	Current History	10	journal

Table 5.3 presents the core sources of information in the order of their appearance in citations within the collection of articles. The primary source, 'Studies in Conflict and Terrorism' (SICAT), accounts for 13.4% (44) of the total citation count. Figure 5.16 further illustrates that SICAT shares a robust citational relationship with 'Terrorism and Political Violence' (TPV), which ranks third in terms of total citations, constituting 8.8% (29) of the collective citation count. Both SICAT and TPV are specialised journals primarily focusing on the topic of terrorism, enjoying a well-established reputation within the field of terrorism studies.

Previously, these journals were instrumental in providing an accurate gauge of the state of terrorism research from 1990 to 2007, as highlighted in Silke's contribution titled; *Contemporary terrorism studies: Issues in Research* (Jackson et al., 2009; Jackson, 2012). Silke observed a shift in focus from opinion-based reviews to more rigorous methodologies and analyses, including statistical and inferential approaches. Moreover, both journals have shown a growing receptiveness to diverse areas of research, as noted in an anecdote about an early editor's exasperation at receiving "yet another article on the IRA" (Jackson et al., 2009:47). This research project aligns with Silke's observations, as evidenced in figure 5.3 depiction of the annual distribution of journal output. In this figure, both "Terrorism and Political Violence" (2) and "Studies in Conflict and Terrorism" (4) have made significant contributions concerning the topics of cyberterrorism and hacktivism, with a particular emphasis on cyberterrorism. This reflects the journals' openness to accommodating non-traditional perspectives on terrorism.

Beyond academic journals, three of the top five sources of information, each with a citation value of 20 or above, belong to news media outlets. Leading this group is the New York Times, contributing 7.4% (31) of the collective citation count. Among the four cited news agencies, the UK-based news agency, The Guardian, stands out with the strongest linkage to its neighbouring news sources and shares a robust co-citation relationship with the journal "Terrorism and Political Violence."

The prevalent reliance on media-based information is a recurring theme in criminological research of this nature, often conducted within hyperbolic channels (Brantly, 2020; Neufeld, 2020; Shandler and Gomez, 2022) of "cyber-doom" like scenarios (Lawson, 2013; Lawson et al., 2016). For instance, in a systematic analysis of organised crime research output, news and media emerged as the third top data source (Windle and Silke, 2019). Historically, a sizeable portion of pre-9/11 terrorism research heavily relied on data gathered from media outlets and media-derived databases (Silke, 2006:80). This reliance on secondary sources of limited detail and uncertain accuracy, such as news articles, has been a matter of concern in terrorism research, as highlighted by Schuurman (2018). In their study, Schuurman noted that such methodologies can potentially compromise the precision and reliability of findings.

This emphasis on media sources within the present study's criminological research aligns with broader trends in the field and reflects the ongoing challenge of striking a balance between accessibility and accuracy in source selection, alongside an over-reliance

towards secondary data sources (Woodward et al., 2016), with Nelson et al. (2014) concluding that there exists an over-reliance towards pre-existing data even as criminology moves towards more quantitative approaches of analysis compared to qualitative approaches.

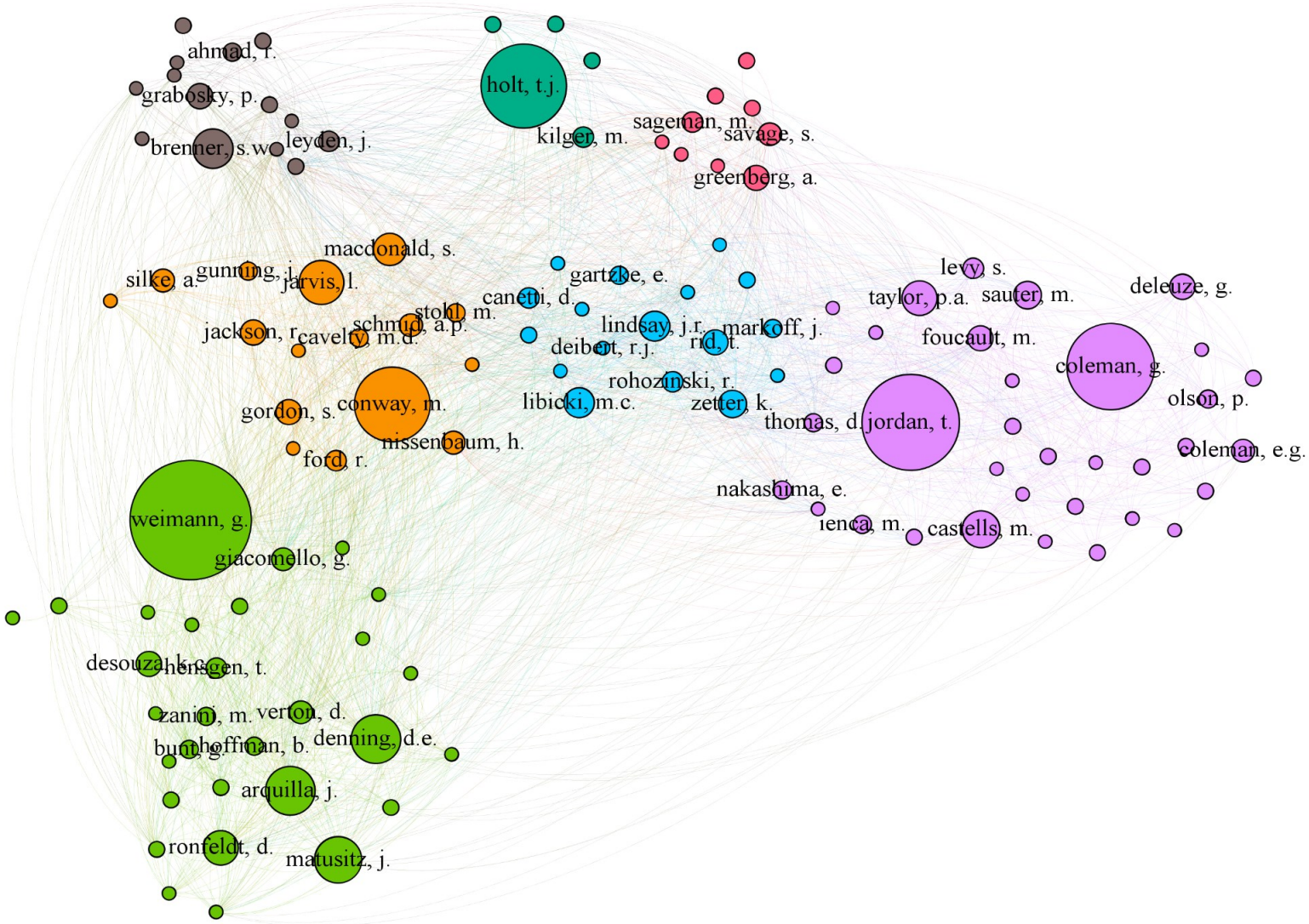


Figure 5.17 Co-citation of Cited Authors with a minimum of 5 appearances

Co-citation Analysis of Key Authors

A total of 4,586 authors were identified to have been cited within the collected dataset. Figure 5.17 presents authors who have been cited at least five times within the collection of articles. Among these authors, 2.8% (128) emerged within the co-citation analysis, contributing to several distinctive clusters. However, despite providing an appealing and robust visualisation, this approach adds little additional value in determining core authors' co-citation patterns and groupings.

To focus on identifying the most significant authors and their co-citation patterns, the analysis was restricted similarly to the previous co-citation analysis of key sources of information. Specifically, the examination was narrowed to authors who appeared 10 or more times within the collected articles, accounting for 0.61% (28) of the total author pool. Out of these entries, four were identified as duplicates, arising from minor variations in spelling, which were appropriately merged. As a result, a total of 26 core authors were identified, with their works collectively garnering 505 citations.

Limiting the appearance value to 10 helps to avoid over-complexity when interpreting the network graph of co-citations among authors. By focusing on this select group, the research gains valuable insights into the most influential authors and their interconnectedness within the domain of cyberterrorism and hacktivism research.

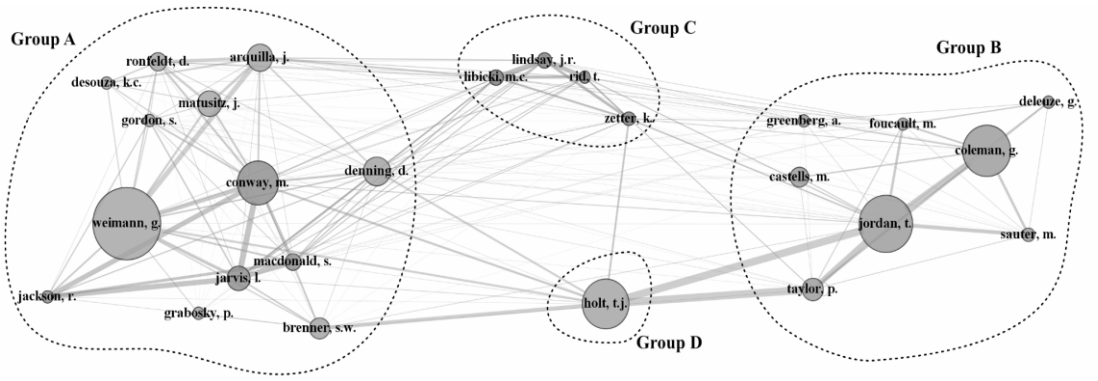


Figure 5.18 Co-citation of Cited Authors with a minimum of 10 appearances

Figure 5.18 presents the relationship between authors cited within the collection of articles, where linkage density is represented visually, and the node size reflects the citation count associated with each author. The co-citation analysis of these authors yielded four distinct groupings, depicted by dotted boundaries encompassing clusters of author nodes. These groupings, akin to an approach earlier adopted by Reid and Chen (2006:51), allow for the clustering of authors who share shared areas of interest.

Subsequently, unlike topic-mapping which focuses on the keywords and abstracts of a publication, the cited works of authors mentioned within figure 5.18 depiction of co-cited authors, were subject to manual review of the publications content to identify their areas of interest. This involved examining the high-impact articles alongside collection of definitions for the later quantitative content analysis and summarising these publications into key terms and labelled as distinct *'area*' in the co-citation analysis.

Table 5.4 Top Cited Authors

author	citation	group	area
weimann, g.	50	A	cyberterrorism; cyber enabled terrorism
denning, d.	41	A	cyberterrorism; hacktivism
jordan, t.	40	B	hacktivism; sociology
coleman, g.	36	B	hacktivism
holt, t.j.	35	D	cyber; criminology
conway, m.	31	A	cyberterrorism; cyber-enabled terrorism
taylor:a.	31	B	hacktivism; cyber-enabled terrorism
arquilla, j.	20	A	cyberwar
matusitz, j.	19	A	cyberterrorism
jarvis, l.	18	A	cyberterrorism; terrorism
brenner, s.w.	16	A	law; cyberthreats
castells, m.	15	B	ICT; sociology
ronfeldt, d.	14	A	cyberwar
macdonald, s.	13	A	cyberterrorism
libicki, m.c.	12	C	cybersecurity; cyberwar
lindsay, j.r.	12	C	cybersecurity; cyberwar
sauter, m.	11	B	hacktivism; civil disobedience
zetter, k.	11	C	hacktivism
desouza, k.c.	10	A	ICT
gordon, s.	10	A	cyberterrorism
grabosky:	10	A	law; cybercrime
jackson, r.	10	A	terrorism; cybercrime

deleuze, g.	10	B	philosophy
foucault, m.	10	B	sociology; security; politics
greenberg, a.	10	B	ICT; security
rid, t.	10	C	cyberwar; cybersecurity

Table 5.4 reveals a diverse array of areas of interest and focus within articles cited from high-impact authors. Notably, these areas of interest are both varied and shared among the authors. By examining the co-citational relationships depicted in figure 5.18, the areas of interest within author groups become apparent. This observation allows for the determination of focused research areas for each group, which are composed of frequently cited authors and sheds light on the interconnections between authors, highlighting their collective research interests and thematic foci.

By discerning the shared areas of interest within these groups, the research can ascertain the dominant research topics pursued by key authors in the domain of cyberterrorism and hacktivism. Such insights contribute towards understanding the research landscape and the collaborative networks that emerge within this field of study.

Identifying Key Themes from Co-citation Authors.

When grouped, figure 5.18 presents a list of 26 authors with a minimum of 10 referenced citations cited within the collection of 126 high-impact articles (see Table 5.4 Top Cited Authors:238). To precisely identify specific citations for review, the open-source data mining software; Orange was employed. Using the concordance feature, this software

enables the search for query terms (such as author names) within a substantial volume of citation text, illustrating the term in relation to neighbouring words and punctuation.

By exploring the context, or "citences" (Nakov et al., 2004) in which these citations are used, the research gains valuable insights into the interconnectedness of ideas and research themes within the collection of high-impact articles of cyberterrorism and hacktivism. These findings from the analysis of co-citation authors publications have been reviewed to identify four key groups shared within these publications (Cyberterrorism, Hacktivism, ICT Security and Infrastructure, and Cyber-criminology) and presented as follows:

Group A: Cyberterrorism

Key areas: cyberterrorism (7), cybercrime (2), law (2), terrorism (2), cyber-enabled terrorism (2), cyberwar (2), hacktivism (1), cyberthreats (1), cybercrime (1).

When limiting the analysis to the 20 most cited authors within the collection, Group A includes four of the eight most cited authors listed in table 5.4. The most cited author, Weimann, garners a significant citation score of 50. Much of Weimann's work included in this analysis contributes to discussions on cyberterrorism and the use of internet technologies (ICTs) by terrorists to orchestrate attacks, commonly referred to as cyber-enabled terrorism. Weimann's research also includes the third most cited article; Cyberterrorism: The sum of all fears? (2005), which delves into the concept of "cyberangst" and explores the reality of terrorist use of ICTs for cyberterrorism, such as

disrupting banks and disabling power grids, water treatment facilities, and other critical infrastructures.

This is followed by the second highest cited author; Denning (cited 41 times) appearing in the co-citation analysis. Denning made significant contributions to the field through her testimony on cyberterrorism and hacktivism before the congressional House Armed Services Committee, later being published as an article (Denning, 2000a). Her work played a pivotal role in establishing the definition of cyberterrorism and coining and defining hacktivism within academic discourse.

Conway is the third most cited author in the analysis, with 31 citations. Her work strongly correlates with Weimann's research, particularly around the pragmatism of research into cyberterrorism and cyber-enabled terrorism. Conway's article 'Reality bytes: cyberterrorism and terrorist 'use' of the Internet' (2002), cited 126 times, along with her other works (Conway, 2003a; 2003b; 2011a), delves into the conceptualising cyberterrorism alongside terrorist communication and propaganda—a major area of study within her early PhD thesis. Conway also explores the representation of cyberterrorism within media and political discourse, while highlighting the lack of evidence to suggest that terrorist organisations view the value vs. costs as a motivating factor for investing in and conducting acts of cyberterrorism.

Lastly, Arquilla (200), cited 20 times, is frequently referenced within the collection of articles due to his RAND article, 'Screensaver: Preparing for cyberterrorism-badly.' This

work is a compilation of contributed chapters, including one of many variations of Denning's (2000a) "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." These chapters offer descriptive discussions on the topic of internet technologies for use in conflict, terrorism, and political violence.

Group A can be characterised by its descriptive approach to discussing cyberterrorism and its frequent reliance on secondary sources. These sources include thematically specialised websites and blogs, online news sources, literature review articles, and agency media releases that emphasise the potential threat posed by cyberterrorists. Notably, core authors in "Group A" rarely rely on empirical studies when discussing cyberterrorism as a viable and potential threat.

Subsequent research within Group A contextualises cyberterrorism in relation to terrorism and explores its potential adoption as a tactic. This research has given rise to a subgroup that specifically focuses on the concept of cyber-enabled terrorism. Figure 5.18 (page: 239) highlights Conway's strong co-citation linkage with notable terrorism researchers such as Andrew Silke, Lee Jarvis, and Richard Jackson.

Overall, the research within Group A sheds light on the potential threat posed by cyberterrorism and its relationship to conventional forms of terrorism. Although empirical research is limited in this group, there is a growing body of literature that examines cyber-enabled terrorism and its implications for national security. The descriptive approach taken by these authors contributed valuable insights into the conceptualization and

potential ramifications of cyberterrorism, offering a foundation for further empirical investigations in the field.

Group B: Hacktivism

Key areas: hacktivism (4), sociology (3), security (2), philosophy (1), civil disobedience (1), politics (1), cyber-enabled terrorism (1).

Group B comprises three of the top eight authors, with a focus on the phenomenon of hacktivism and its sociological implications as a form of activism. The highest cited author in this group is Tim Jordan, with 40 citations. A sizeable portion of Jordan's citations are attributed to his article, "Hacktivism and Cyberwars: Rebels with a Cause?" published in 2004. In this work, Jordan maps out the emergence of digital activism and explores the societal impact of emerging technologies like ICT, drawing frequent references to Marxism. Jordan views hacktivism as akin to anti-capitalist and Marxist-inspired movements of the 1970s (Jordan and Taylor, 2004:51).

The second highest cited author in Group B is Coleman, cited 36 times. Her research introduces the political motivations within hacker communities, specifically focusing on the decentralised hacker collective Anonymous and open-source groups like WikiLeaks. In her 2011 article, "Hacker Politics and Public," she identifies those engaging in online political protest as "hackers and geeks" (Coleman, 2011:512). In her later published book "Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous," published in 2015, Coleman applies the term "hacktivist" while comparing online hacker groups to

RedHack, a Turkey-based Marxist-Leninist computer hacker group founded in 1997 (Coleman, 2015:156), who were the first to face terrorism charges for encouraging criminal activities through social media postings.

Lastly, in Group B, Paul Taylor, cited 31 times, focuses on hacktivism through his co-authored article "Hacktivism and Cyberwars: Rebels with a Cause," (Jordan and Taylor, 2004) alongside Tim Jordan. Taylor's separate research delves into hacker subtypes, particularly "Hackers: Cyberpunks or Microserfs," originally published in 1998. This work discusses the concepts of "cyberpunks," denoting a lawless subculture dominated by technology, and "Microserfs," describing computer coders who work within corporate organisations, such as Microsoft, often in conflict with core hacker ideologies (Taylor, 1998).

Group B's core themes revolve around ideology, philosophy, and anti-capitalist motivations, with a strong focus on human rights-focused virtual action. A sizeable portion of our understanding of this group comes from dedicated books on hackers, allowing for in-depth exploration of complex political and social ideologies. Group B's research is particularly descriptive in understanding societal motivations, as evidenced by the close co-citation reference to the works of Castells (cited 15 times), who heavily focuses on understanding the motivations of hacker groups and their societal movements (Castells, 2014).

Group C: ICT Security and Infrastructure

Key areas: cybersecurity (3), cyberwar (3), hacktivism (1)

In Group C, no authors were identified with 20 or more citations. However, three leading academics in this group primarily discuss two key areas: cybersecurity and cyberwar. The literature cited from these authors centres around the potential risks to cyber-dependent infrastructure, such as ICT, and the importance of defence and deterrence against potential sub-national or state-operated cyberattacks. Much of this understanding is derived from the works of Martin Libicki, particularly "Cyberdeterrence and Cyberwar" (2009) and "Crisis and Escalation in Cyberspace" (2012), which heavily focus on implementing and using deterrents to protect national air forces.

Risk to state agencies from state groups is a recurrent theme in Group C, also reflected in the works of Jon R. Lindsay, whose contributions concentrate on international security as a global concern. Lindsay's research primarily focuses on cybersecurity experiences in non-western contexts, particularly in China and other East Asian countries, exploring the myths and factual issues faced by these states (Lindsay, 2014; Cheung et al., 2015; Lindsay, 2015). Thomas Rid contributes to these discussions by challenging the concept of cyberwar itself, arguing that no cyberattack or offence has yet constituted a true cyberwar, with motivational cyberattacks instead being instances of sabotage, espionage, and subversion (Rid, 2013).

The areas discussed within Group C can be found in literature that examines the security focus of ICT, particularly in literature on securitization theory. This theory argues that political issues are labelled as extreme security concerns by a "securitizing actor" who possesses the social and institutional power to move the issue "beyond politics" when they have been branded as "dangerous," "menacing," "threatening," "alarming," etc. (Eroukhmanoff, 2017:104). This is evident in the often polarised and extreme descriptions of hypothetical scenarios in cybersecurity literature, such as potential interception and silencing of a surface-to-air missile system (Libicki, 2009:XV) or the hacking and controlling of UAVs used for weather reporting (Libicki, 2015:4). These hypothetical scenarios, although lacking empirical evidence, contribute to the securitization of cybersecurity issues.

Similar behaviours were acknowledged and explored by Fierke, who describes concepts surrounding hypothetical scenarios as generating debates that cannot be resolved by reference to empirical evidence due to their ideological or moral elements (Fierke, 2015:35). In the context of cyberterrorism and hacktivism, such hypothetical scenarios can be used to promote concepts and methods of securitization, as seen in the works of Denning (2001) and the absence of empirical evidence to support the need for reactive measures, as seen in the works of Conway (2014a). These insights contribute to a better understanding of how cybersecurity issues are framed and debated within academic discourse, highlighting the influence of securitization and hypothetical scenarios in shaping perceptions and responses to potential cyber threats.

Group D: Cyber-Criminology

Key areas: cyber (1), criminology (1)

In Group D, there is only one author with 10 or more citations and that is Thomas J. Holt (35). Holt's work is frequently cited by authors in this study for his application of criminological and related theories to understand cybercrime phenomena. His contributions (Holt, 2007; Holt, 2010; Holt et al., 2010) cover areas such as subcultures, routine activity theory, and social learning to gain insights into cybercrime actors.

Expanding on co-citations frequently cited alongside Holt's contributions, it becomes apparent that Holt and the associated co-cited works form an isolated collection. This suggests that within cyberterrorism and hacktivism research articles, the application of criminological theories and related disciplines such as sociology, psychology, and law is limited. However, the literature closely cited with Holt delves into areas such as the social impact and influence of emerging technologies on the criminal behaviour of "cyber-terrorists" (Kilger, 2015). Kilger himself later co-authored an article with Holt, further examining the social networks of hacker groups and their willingness to engage in cyberattacks (Holt et al., 2016; Holt and Kilger, 2012).

Holt also shares strong co-citation linkage with the works of Tim Jordan and Paul Taylor, two authors identified in Group B. They collaborate closely and co-cite each other in their contributions to the sociological discussion of ICT and deviant behaviours. Therefore, from the observation of co-citations, it can be determined that Group D primarily focuses

on the societal impact of ICT and theoretical understanding of cybercrime and cyber-deviant actions online, as evidenced by the strong citation value of Holt and his associated co-authored articles. Furthermore, Group D's focus is broad, with strong co-citation linkages spanning topics such as hacktivist motivations (Jordan and Taylor, 2004), terrorist networking (Sageman, 2004; Kilger, 2014), and legal aspects of cybercrime (Brenner, 2006). The group's research explores diverse aspects of cyber-related deviance and its social implications, encompassing both theoretical and empirical investigations.

5.2.3 Summary of Bibliometric Findings

The academic journey of cyberterrorism and hacktivism research output has been challenging due to the lack of dedicated active and annual platforms, such as academic journals and conferences, which has hindered consistent research output, especially in terms of empirical research. In comparison to more established fields like terrorism studies and organised crime studies, cyberterrorism and hacktivism research are still relatively new phenomena within academic discourse. They lack the dedicated journals, conferences, college classes, and wider discussions that are common in terrorism and organised crime studies. However, despite these challenges, cyberterrorism and hacktivism research share common issues found in terrorism and organised crime research, such as the lack of empirical quantitative research and the ongoing definitional debate (Silke, 2004; Windle and Silke, 2019; Schmid, 2004a; Von Lampe, 2015; Symeonidou-Kastanidou, 2007).

Given the new and unstructured state of research in this area, conducting a bibliometric review becomes crucial to map the intellectual structure of cyberterrorism and hacktivism research. Through the mapping of 126 high-impact articles, the findings suggest that despite being transnational phenomena, much of the research output is male-dominated and confined to the global north, particularly the United States and the United Kingdom. This limited perspective poses a challenge for understanding such a global issue comprehensively. Moreover, a considerable number of the contributed articles come from single authors, with only a small percentage of authors having provided multiple contributions, and although many of these authors come from a rich collection of disciplines, the domain is only limited by the lack of collaboration research outputs.

Authors identified within the collected data demonstrate an array of multidisciplinary contributions, with strong contributions from both the social sciences, and the computer sciences. This multi-disciplinary structure of the domain provides unique perspectives towards a topical issue. However, as noted by Bossler (2017), without effective collaboration between scientists of different disciplines, these distinctions in disciplines risk compartmentalising research efforts. In this study, out of the 146 unique individual authors identified, only 11% (16) provided more than one contribution. While no transnational author collaboration was identified, 24% (35) of authors had collaborated in at least one article with another author outside their immediate institution at the national level. The lack of transnational collaboration is concerning, as international perspectives on a transnational phenomenon can significantly enrich national understandings. By sharing knowledge, methods, and resources, collaborative efforts can break down

research barriers and lead to a more comprehensive understanding of the subject, challenging issues raised by Holt, Freilich, and Chermak (2017), who suggests that the lack of a 'common language' establishes barriers towards fully understanding these complex phenomena.

In the final section of the bibliometric analysis, themes associated with cyberterrorism primarily focused on the reality of cyberterrorism as a method of terrorism, encompassing both traditional terrorist groups labelled as "cyber-enabled terrorism" within this research project, and emerging forms such as 'pure' or 'cyber-dependent' cyberterrorism (Gordon and Ford, 2002; Jarvis and Macdonald, 2015). Strong criticism was raised regarding the actual existence of such phenomena and the challenges faced in conducting empirical research (Conway, 2002; Berner, 2003; Foltz, 2004; Gorge, 2007; Smith, 2015).

Publications related to hacktivism delved into the complex variety of sociological and ideological motivations behind hacking, contributing towards causes more strongly associated with traditional activism (Carducci, 2006; Sorell, 2015; McCarthy, 2015). Particularly, the focus was on freedom of information and knowledge, as government and private services have become more invasive and secretive with individuals' data, privacy, and civil liberties (Züger, 2013; Stoehrel and Lindgren, 2014; McKelvey, 2015). The means to mitigate these invasions of personal liberties were a major concern within hacktivism discourse (Lindgren and Lundstrom, 2011; Merck, 2015; Asenbaum, 2018; Coleman, 2019; Coleman and Jandrić, 2019).

Finally, the theme of ICT Security and Infrastructure centred on the risk of ICT being used as an offensive means by state or non-state actors to impact critical infrastructures, with potential consequences for national (Matusitz and Breen, 2011), international security (Sieber, 2006), and enterprise operations (Giacomello, 2004). Much of the research in this area focused on the need to develop approaches to mitigate and manage such events when they occur. However, it is important to note that much of the securitization discourse is built upon hypothetical "what if" scenarios with similar risks and effects, which can make interpretations and measurements of these threats and the effectiveness of securitization challenging and open to loosened interpretation (Jarvis et al., 2016; Mott, 2016; Shad, 2019).

5.3 Part Two: Quantitative Content Analysis of Definitions

The second objective of this research project is focused on identifying key terms and distinctions within academic definitions of cyberterrorism and hacktivism. This section of the thesis focuses on the findings of the quantitative content analysis of 237 identified definitions of both cyberterrorism (162 definitions) and hacktivism (75 definitions). These definitions, identified from 87 (69%) of the 126 high-impact academic articles, were broken down into six categorical classifications (actor, effect, intent, means, motive, and target) based on a taxonomic model adapted from both Al Mazari et al. (2015) and Plotnek and Slay (2021) and discussed earlier (see section 6.4.2 Building the Taxonomy: 192). This taxonomic model, using terms identified within the earlier taxonomies as a guide, was used to code and organise 1242 extracted terms found between definitions of cyberterrorism and hacktivism for further analysis.

Findings of the content analysis are firstly grouped by their definitions, cyberterrorism, and hacktivism. The results of both analyses are then presented in three sections: the "*Overview of Analysis*" presents the general distribution of extracted terms across the taxonomy, classifying raw terms concerning cyberterrorism into the taxonomy for comparison to terms identified in earlier cyberterrorism taxonomies by both Al Mazari et al. (2015) and Plotnek and Slay (2021), and later between both cyberterrorism and hacktivism groups. Due to the number of collected definitions of cyberterrorism and hacktivism being different, and the quantitative number of coded terms from both groups

being equally different, both groups are later normalised to allow for further comparative analysis using a general min-max normalisation formula which assigns the frequency of each coded term a value between 0 to 1.

The next section: "Comparison of Distributions by Definitions" compares the normalised distribution of classifications between both cyberterrorism and hacktivism across the temporal axis of 20 years (2000 to 2020), allowing for the distributional nuances of each six classifications to be observed and compared. This is later broken down into each classification for further evaluation and review of the findings with key terms and associated high-impact articles presented.

Lastly, within the "Synthesising the Taxonomy," findings from both sections are synthesised and merged with the earlier taxonomies to develop an extended taxonomy incorporating new findings from the analysis of cyberterrorism definitions, and further extended by the inclusion of findings from the analysis of hacktivism definitions.

5.3.1 Overview of Analysis

Distribution of Raw Terms

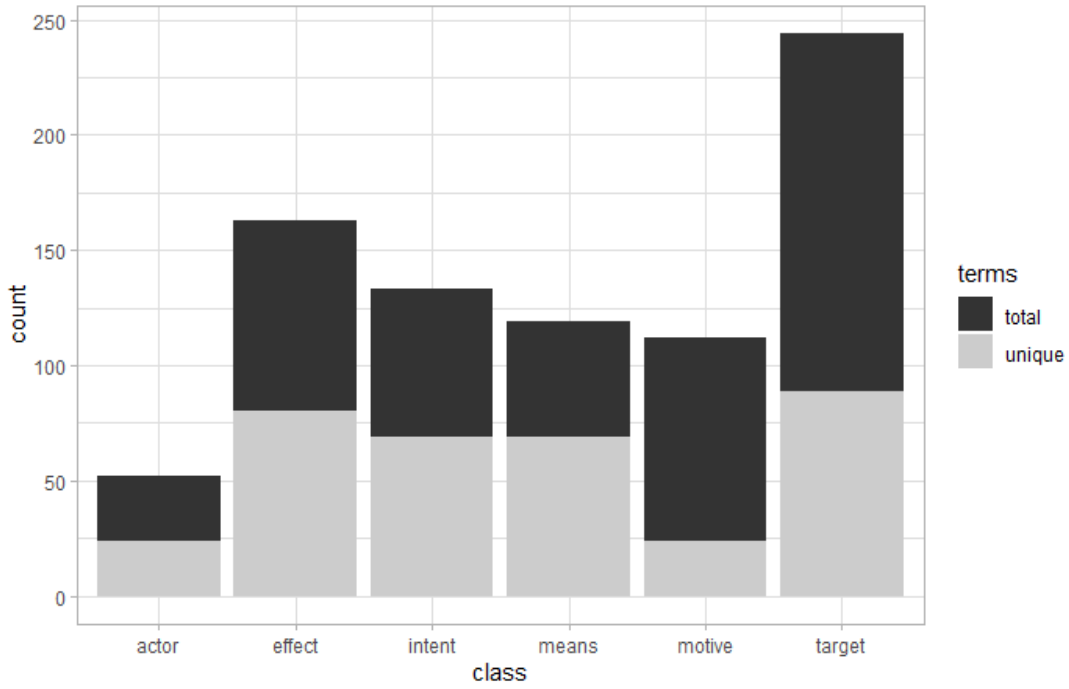


Figure 5.19 Cyberterrorism Term Distribution

Following the data collection and content analysis, shown in figure 5.19 representing a bar-chart of terms collected, a total of 823 raw terms were identified from definitions specifically related to cyberterrorism. Raw terms are words taken verbatim from the definitions during the initial breakdown. In comparison to the earlier merged taxonomy (195), a total of 355 unique raw terms were identified (represented as grey) and extracted from definitions of cyberterrorism, which is an 82% (160) increase in terms from the previously mentioned merged taxonomy (Al Mazari et al., 2015; Plotnek and Slay, 2021). The distribution of these extracted raw terms is represented in figure 5.19 which illustrates

how these terms are allocated to their respective classifications and the proportion of unique terms not found in earlier typologies within each classification.

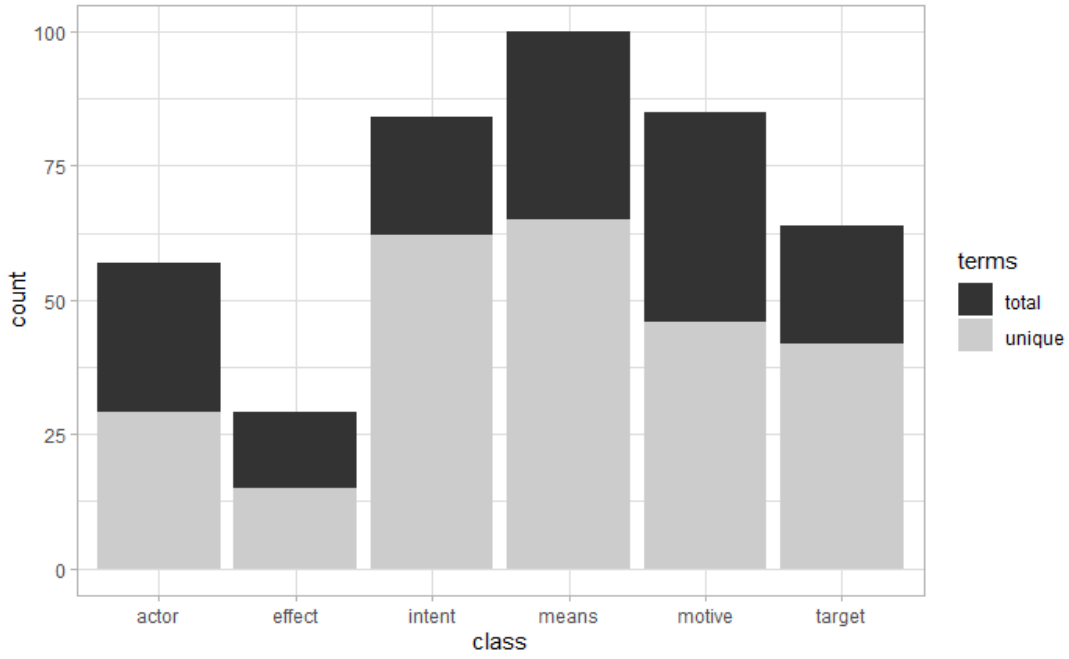


Figure 5.20 Hacktivism Term Distribution

When evaluating hacktivism definitions alongside the earlier typology, figure 5.20 illustrates a comprehensive total of 419 raw terms identified and extracted from definitions of hacktivism. Among these terms, there were 259 (61.8%) unique terms, signifying the distinct vocabulary encompassed within the context of hacktivism.

Distributional Analysis

Following the completion of coding the definitions within the taxonomic framework, this section focuses on presenting the distribution of coded terms based on their classifications, both in total and yearly distribution. The discussion will encompass both cyberterrorism

and hacktivism as aggregates, allowing for a comprehensive comparison between the two phenomena. Later, a detailed examination will be conducted at the individual term level, comparing cyberterrorism and hacktivism side by side to identify commonalities and unique terms associated with each.

Table 5.5 Distribution Count of Total Terms by Definition

Terms	Actor	Effect	Intent	Means	Motive	Target
Cyberterrorism: Total	52	163	133	119	112	244
Cyberterrorism: Unique	24	80	69	69	24	89
Hacktivism: Total	57	29	84	100	85	64
Hacktivism: Unique	29	15	62	65	46	42

In total, the content analysis yielded 1242 extracted terms from definitions pertaining to both cyberterrorism (823 terms) and hacktivism (419 terms). Upon examination of table 5.5, it is evident that the total number of terms within the ‘actor’ classification for both cyberterrorism (52) and hacktivism (57) are similar, with hacktivism displaying only a slight increase of 8.8%. A significant difference emerges in the ‘effect’ classification, where cyberterrorism (163) surpasses hacktivism by a substantial 82.2% (134) in terms of count. The distribution of ‘intent’ also demonstrates a notable increase, with cyberterrorism (133) and hacktivism (84) showing a one-third higher count, representing a 33.8% (43) increase in usage. Within the ‘means’ classification, cyberterrorism (119) exhibits a 19% increase compared to hacktivism (100). As for the ‘motive’ classification, cyberterrorism (112) and hacktivism (85) have a separation of 24% (27).

Lastly, the ‘target’ classification exhibits a stark contrast, with cyberterrorism (244) significantly outweighing hacktivism (64) in terms of usage, representing a difference of 73.8%.

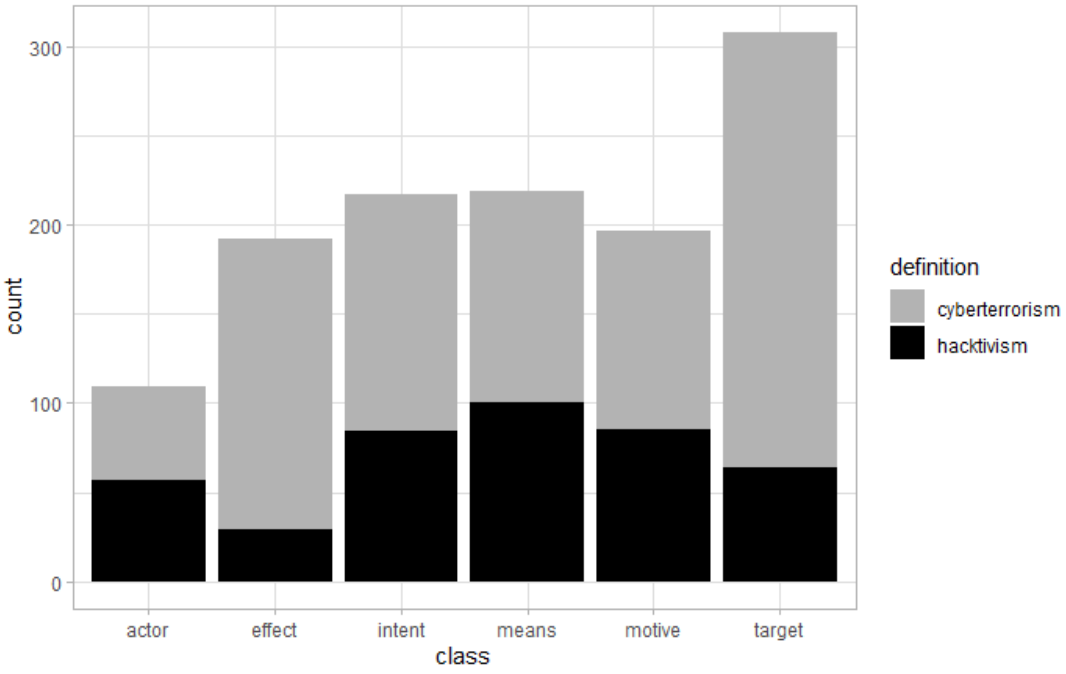


Figure 5.21 Distribution of Total Terms by Definition

After breaking down all definitions into their appropriate classifications, the quantity of terms distributed between both cyberterrorism and hacktivism definitions was summarised and visually represented in a bar chart, as depicted in figure 5.21. Both figure 5.21 and table 5.5 provide an overview of the overall distribution of classifications for cyberterrorism and hacktivism, showcasing the composition of extracted terms within each classification. While this approach offers a useful means of observing the key focuses of these classifications across the board, it does not capture the evolution of these classifications over time.

To address this limitation and incorporate the dimension of time into the analysis, each raw code was assigned a unique ID value that corresponds to the collection of 126 high-impact articles in which the term originated from. By applying a unique article-specific ID, the ability to associate the publication year (time) of that article with the frequency (usage) of the coded terms was achieved, allowing for a more dynamic and comprehensive perspective on how the various classifications and terms associated with cyberterrorism and hacktivism definitions have evolved.

Distribution of Classifications Over Time

Using the bibliographic data collected from the bibliometric analysis, the publication year associated with each high-impact article which provided the definitions (86 articles) was linked to each extracted term and its classification. This enables the mapping of the term's usage over a linear timeline of two decades (2000 - 2020). This approach allows for the observation of how the taxonomic classifications have fluctuated in frequency over time. Moreover, it provides the capability to isolate term usage for any specific year within the collection of high-impact articles.

In this section of the analysis, the yearly distribution of the taxonomic classifications for both cyberterrorism and hacktivism will be presented. This presentation will offer insights into how the usage of different classifications has evolved over the years. Additionally,

the distributions for both cyberterrorism and hacktivism will be normalised to facilitate a more direct and fair comparison between the two definitions.

By normalising the distributions, these findings account for any variations in the number of publications or terms between different years, thereby enabling a more accurate and meaningful comparison. This normalisation process ensures that the comparison is based on proportional usage rather than absolute counts, making it easier to identify trends and patterns in the term usage over time.

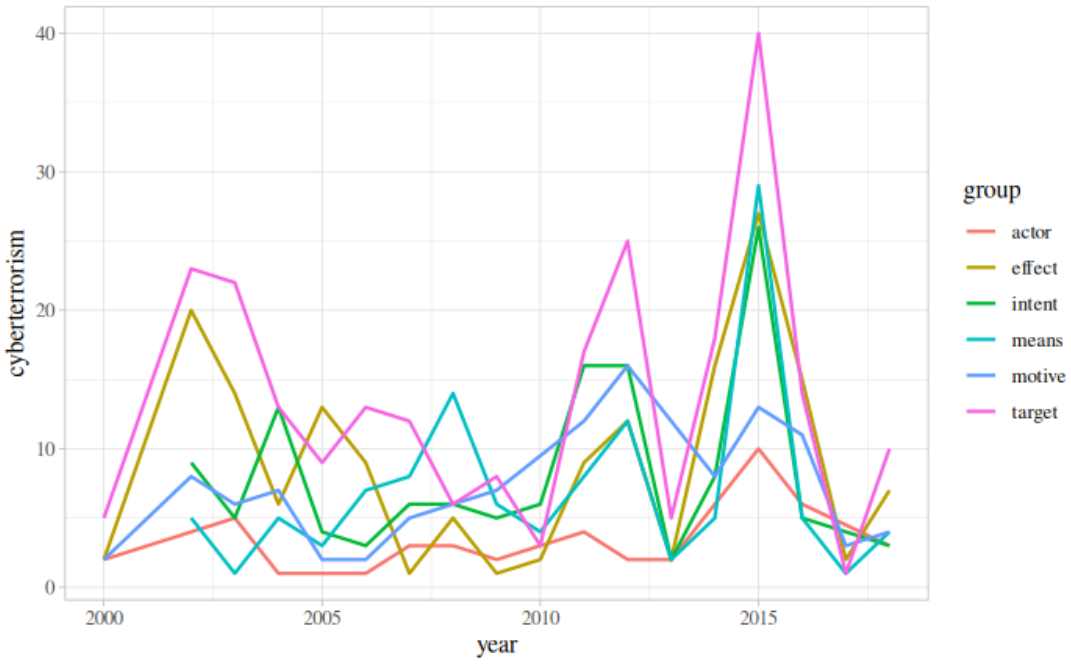


Figure 5.22 Cyberterrorism Distribution of Classifications by Year

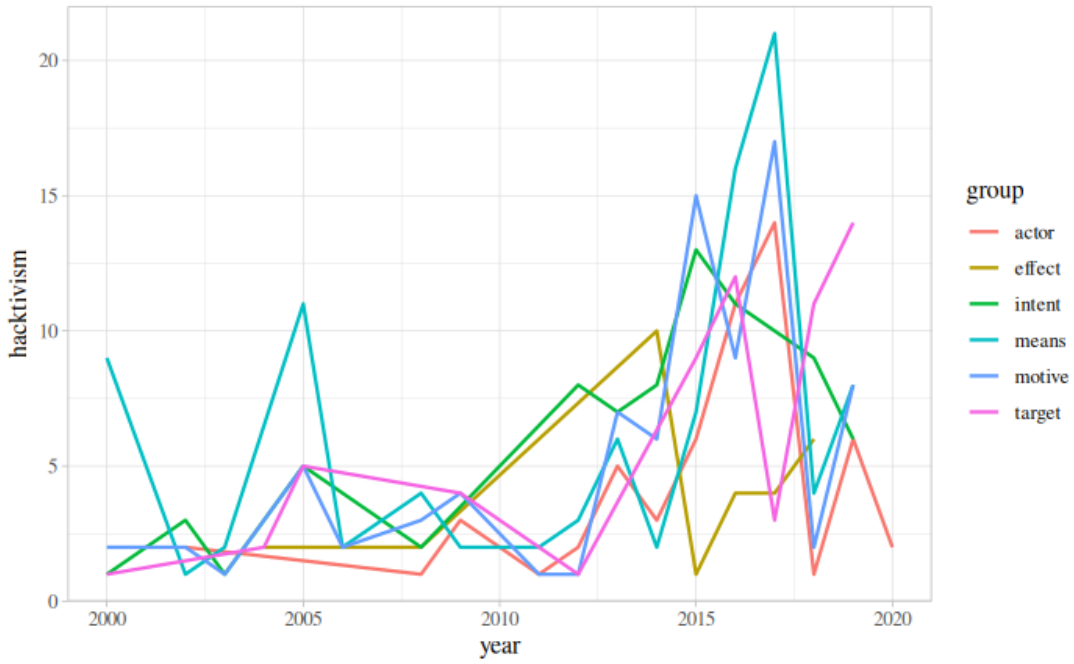


Figure 5.23 Hacktivism Distribution of Classifications by Year

Figure 5.22 displays the yearly distribution of term usage within definitions of cyberterrorism. Notably, the analysis did not identify any definitions of cyberterrorism from publications collected for the years 2019 to 2020. On the other hand, figure 5.23 depicts the yearly distribution of term usage within definitions of hacktivism from 2000 to 2020.

The classification distribution, as illustrated in the graphs, can be considered as the conceptual focus of the overall academic discourse surrounding both social phenomena, cyberterrorism, and hacktivism. This allows for the identification of key classification focuses within each yearly period and facilitates a meaningful comparison between the research discourses of cyberterrorism and hacktivism.

Both figures, 5.22 and 5.23, present a clear overview of the distribution of each classification's term usage over their respective timelines. To enable a fair and comparable analysis, each phenomenon's distribution is normalised to establish a consistent base for comparison. This normalisation process eliminates the impact of frequency distribution on the overall classification distribution, ensuring that the comparison is based on proportional usage.

Normalisation of Distribution

Normalisation of variables is crucial when conducting an analysis involving multiple variables (classifications) measured on different scales (frequencies). In this case, both the cyberterrorism and hacktivism taxonomies have different values, making a direct comparison difficult based on frequencies alone. To facilitate a more meaningful comparison between the two phenomena and their distribution among the coded taxonomy, a method of normalisation known as 'feature scaling' or 'Min-Max Normalisation' is employed:

$$N = (x - min(x)) / (max(x) - min(x))$$

In this formula, 'x' represents the value (term frequency), 'min' denotes the minimum frequency present, and 'max' indicates the maximum frequency present. The total term frequency for each year within the dataset was normalised on a per-classification basis.

To avoid potential human errors, the normalisation process was conducted within RStudio, a software environment for statistical computing and graphics.

This normalisation technique scales each dataset within a range of zero and one. Here, zero represents the minimum value present within the dataset, and one corresponds to the maximum value within each dataset, ensuring that each feature within the scale holds equal importance (Saranya and Manik, 2013: 2702). By doing so, it prevents any single variable from exerting excessive influence, thereby preventing skewed comparisons.

By normalising both the cyberterrorism and hacktivism datasets, it becomes possible to compare each of the six classifications (actor, effect, intent, means, motive, target) independently and more effectively. This normalisation process provides clarity and allows for a more focused discussion, enabling the researcher a means to analyse and interpret the distribution of each classification within the context of both phenomena. The generated line-charts from the normalised data aid in visualising and understanding the trends and patterns of each classification over time for cyberterrorism and hacktivism.

5.3.2 Comparison of Distribution by Definitions

After normalising both datasets using the method described by Patro and Sahu (2015), each individual classification was paired across both definition datasets (cyberterrorism and hacktivism). This pairing resulted in each classification existing as its own independent dataset. These six datasets are now more suitable for visualising and comparing the values and codes associated with each classification.

The discussion of the following findings from the quantitative content analysis provides insights into the distinct characteristics and focuses of cyberterrorism and hacktivism, as represented by their taxonomic classifications, and allows meaningful conclusions to be drawn from these comparisons, supporting a more comprehensive understanding of the nuances and conceptual differences between the two social phenomena.

Actor Classification

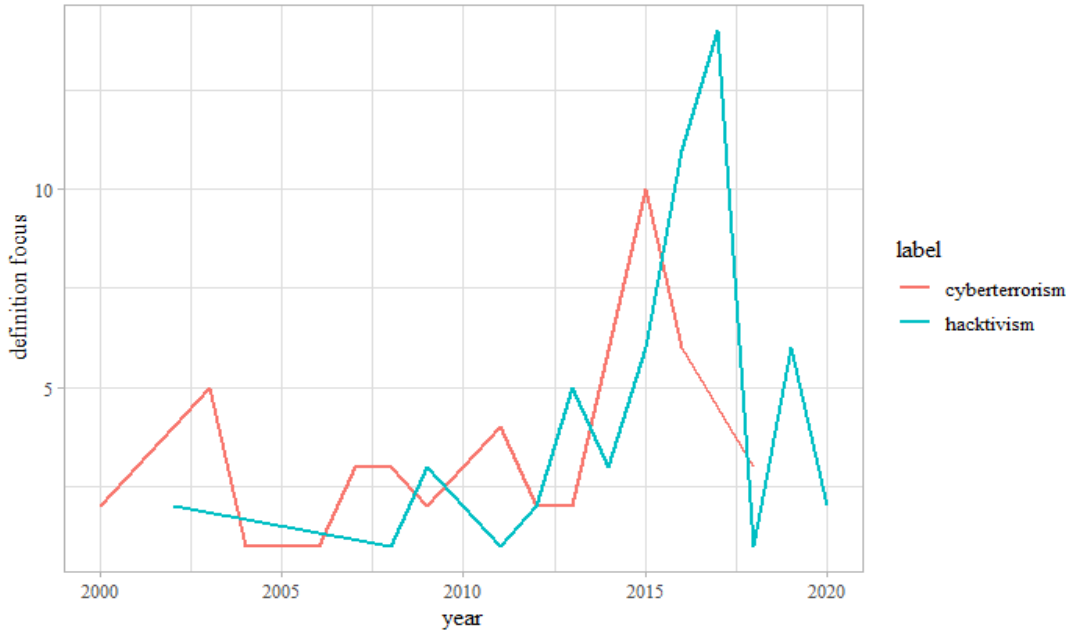


Figure 5.24 Yearly Distribution of Actor Classification

Findings illustrated above describe the normalised distribution of term usage within definitions of both cyberterrorism (represented by the red line) and hacktivism (represented by the blue line) in figure 5.24. This graph illustrates the distribution of term

usage over a yearly period spanning 20 years (from 2000 to 2020). Peaks in the graph indicate significant usage of terms, while valleys represent dips in usage.

The actor classification, as explained by van Heerden et al. (2012) and Veerasamy et al. (2012), typically focuses on highly skilled individuals or groups using computer coding and hacking for various motivated activities that exploit or counter the intended purpose of the target. Observing the graph, we can see that initially, the usage distribution within cyberterrorism fluctuated, while in hacktivism, the usage was limited, primarily featuring terms used when discussing actors within a terrorism context, such as 'terrorist,' 'clandestine agents,' and 'subnational groups.' Early definitions of hacktivism centred around terms like 'hackers' or 'hacktivists.' However, starting from 2009 onwards, researchers expanded the inclusion of terms associated with actors in both cyberterrorism and hacktivism. For hacktivism, this expansion involved incorporating terms commonly associated with more traditional forms of activism, such as 'activists' and 'freedom fighters.'

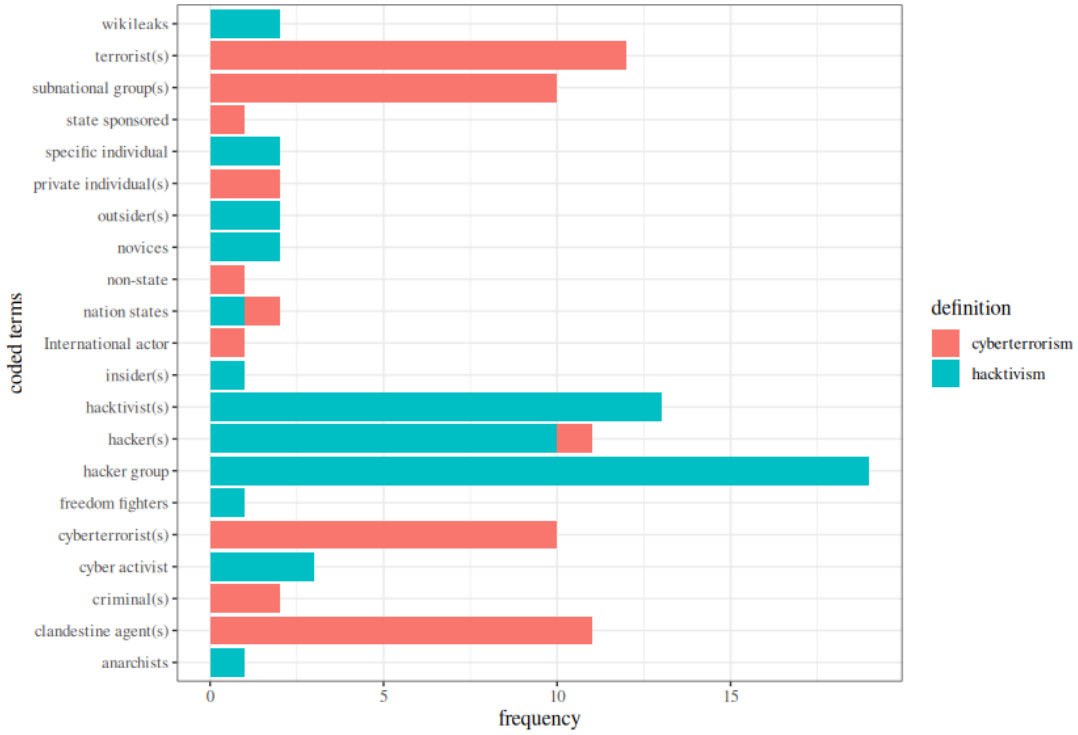


Figure 5.25 Total Frequency Distribution of Coded Actor Terms

Figure 5.25 illustrates the frequency distribution of coded terms between definitions of cyberterrorism and hacktivism. Within the actor class of cyberterrorism definitions, the focus is on key 'actors' such as terrorists (12), clandestine agents (11), subnational groups (10), and cyberterrorists (10). In contrast, the definitions of hacktivism highlight key actors identified as hacker groups (19), hacktivists (13), and hackers (10). Only two coded terms, nation-state, and hackers, are shared between both cyberterrorism and hacktivism definitions.

Upon observation, clear distinctions emerge between the definitions of cyberterrorism and hacktivism in terms of their actor classification. The coded terms within hacktivism definitions denote a high degree of ICT skills associated with the actors engaging in

hacktivism. This is evident from the significant focus on terms related to hacking or other related skill sets (e.g., insiders, outsiders, novices, cyber activists, wikileaks). The emphasis on high-level ICT skills underscores the technological nature of hacktivism.

In contrast, the actor classification in cyberterrorism definitions exhibits a greater opaqueness. The terms often revolve around the association of actors with states or the lack thereof (e.g., state-sponsored, private individual, subnational group, criminal...), and there is a significant association with terrorism itself, a field with its own challenges of opaqueness and lack of consensus within a singular framework of understanding. This lack of clarity in the cyberterrorism actor classification leaves much to the interpretation of researchers and contributes to the complexity in defining and understanding cyberterrorism.

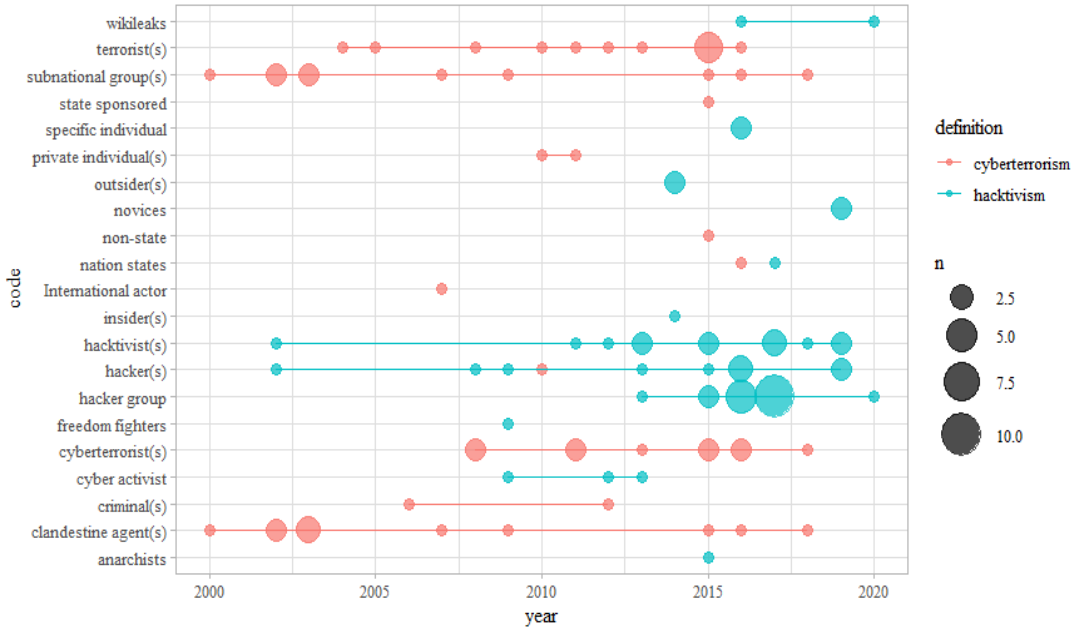


Figure 5.26 Actor Code Distribution by Year & Frequency

Figure 5.26 presents the distribution of coded terms over the 20-year period, where each 'n' size is represented as a circle taken from the frequency of the term in that particular year. In the early years, the term distribution is scarce, which is expected in the emerging academic discourse surrounding social phenomena such as cyberterrorism and hacktivism.

Within the first five years, only five coded terms associated with cyberterrorism (3) and hacktivism (2) were identified amongst definitions, largely stemming from the works of key contributors such as Berner (2003), Conway (2002), Denning (2000a), Embar-Seddon (2002) and Emery (2005), Foltz (2004), and Milone (2002). This limited variety of terms in the early years reflects the initial stages of research and exploration into these new concepts.

As technology evolved and became more accessible, there is a significant increase in the variety of terms used within the later 15 years. Cyberterrorism definitions underwent a transformation, adopting a more nuanced approach to describing actors, such as criminals, state-sponsored entities, and private individuals, while retaining a focus on the association with states or the lack thereof, as seen in the earlier years. This evolution in the language used to describe actors in cyberterrorism reflects the growing understanding and depth of research in this field.

Similarly, hacktivism also experienced an increase in added terms over time, although more localised in nature. The focus shifted towards specific individuals, whistleblowers,

or non-state and decentralised groups, becoming more prominent within the hacktivism discourse. This localised emphasis suggests a specialisation and refinement of research interests within hacktivism.

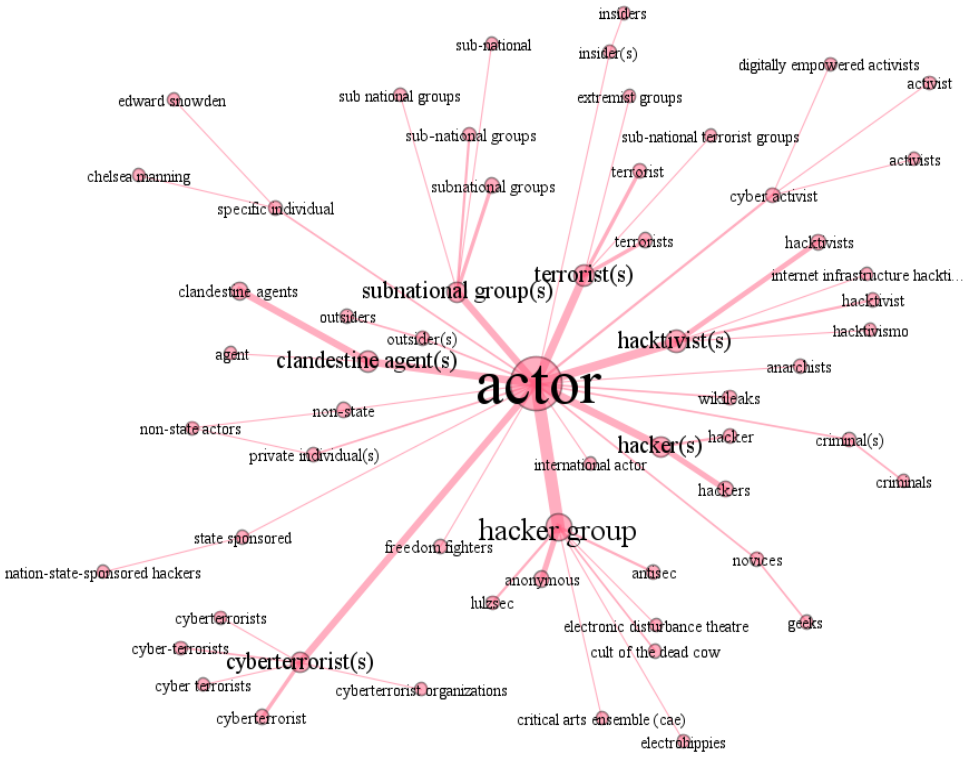


Figure 5.27 Network Distribution of Extracted Actor Terms

Figure 5.27 depicts the distribution of terms extracted from definitions of both cyberterrorism and hacktivism that are connected to the coded terms within the actor classification. The graph shows a diverse range of terms, including alternative spellings and more specific terms.

As expected, within the ‘cyberterrorist(s)’ code, various alternative spellings are present, such as cyberterrorist, cyber-terrorist, and cyber terrorist. This variability in spelling highlights the linguistic nuances and differences in terminology used to describe actors engaged in cyberterrorism.

Moreover, within the ‘hacker group’ code, specific group names are identified, including lulzsec, antisec, cult of dead cow, electrohippies, and anonymous, to name a few. These specific group names underscore the distinct and varied identities of hacker groups involved in hacktivism.

Effect Classification

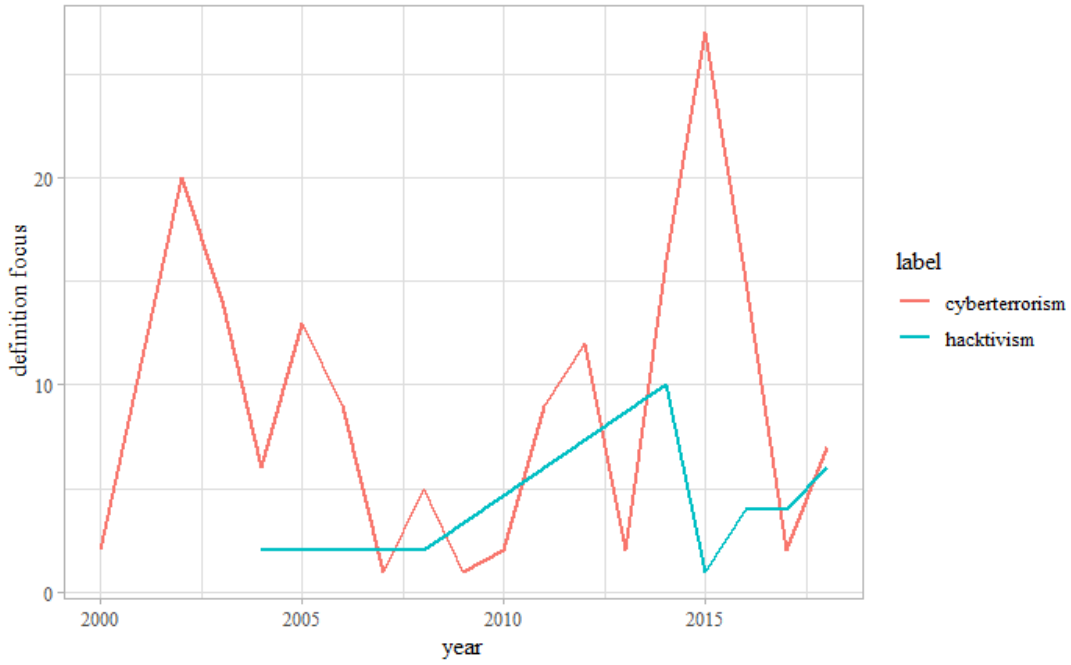


Figure 5.28 Yearly Distribution of Effect Classification

Figure 5.28 illustrates the distribution of the effect classification. It is worth noting that terms coded under the effect classification did not emerge through content analysis of identified definitions of hacktivism (blue line) until 2004.

The effect classification, as defined by Veerasamy, et al. (2012), is associated with causing damage to the target. Al Mazari et al. (2015) further associates the effect classification with violence, destruction, disruption, physical damage, and harm to an individual or group. While the analysis is limited to cyberterrorism, insights from hacktivism can offer further understanding into the intended effect of hacktivism, which includes civic hacking (Schrock, 2016), patriotic hacking (Lokot, 2017), and other

associated effects, such as what George and Leidner (2019) refer to as 'digital gladiatorial activities.'

The term distribution of the effect classification exhibits significant differences between cyberterrorism and hacktivism. In cyberterrorism, there are several notable peaks in usage, occurring both earlier and later in its usage timeline. In contrast, hacktivism shows a more gradual incline from 2008 to 2014, followed by a significant drop immediately after in 2015.

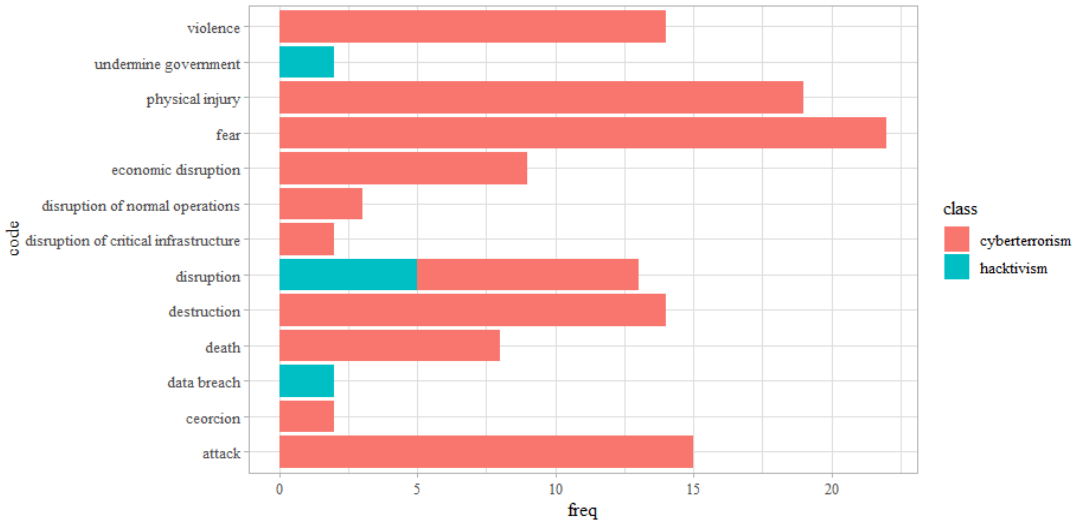


Figure 5.29 Total Frequency Distribution of Coded Effect Terms

Due to limited space, figure 5.29 presents the distribution of coded terms within the effect classification with a value of 2 or more frequencies.[11] This figure reveals significant contrasts between cyberterrorism and hacktivism. In the analysis, definitions of

[11] A complete bar chart is included within the appendix

hacktivism contributed a total of 7 coded terms, with 4 of them being unique to hacktivism (undermine government, non-violence, data breach, communication) and 3 shared with cyberterrorism (economic disruption, disruption of critical infrastructure, disruption).

On the other hand, cyberterrorism definitions contributed a total of 17 coded terms, with 14 of them being unique to cyberterrorism and 3 shared with hacktivism, as previously noted. Coded definitions of cyberterrorism feature the most highly frequent codes within the effect classification. These prominent codes include terms such as violence, physical injury, fear, destruction, and attack, indicating a more detrimental tone associated with the effects of cyberterrorism.

When comparing the coded terms associated with cyberterrorism and hacktivism within the effect classification, distinct patterns emerge. Codes associated with cyberterrorism tend to adopt a more harmful and severe tone, often describing effects that cause physical and emotional harm, such as violence, physical injury, and fear. These terms suggest a focus on aggressive and harmful actions towards individuals and society.

In contrast, hacktivism codes demonstrate a more subdued set of effects, centred around actions intended to cause disruption, such as data breach, economic disruption, and significant but temporary disruption of critical infrastructure. Additionally, communication-based effects like undermining government and communication are highlighted, emphasising the use of information dissemination and communication as a means of achieving objectives.



Figure 5.30 Effect Code Distribution by Year & Frequency

Figure 5.30 provides the distribution of coded terms within the effect classification over a 20-year period, extending the significant contrast identified in figure 5.29. The graph shows that the distribution of terms associated with hacktivism was initially minimal, with most term usage occurring in 2014. The coded terms identified within definitions of hacktivism (disruption, data breach, non-violence) were later adopted by only a handful of researchers (Fernandes et al., 2014; Fuentes, 2015; Tanczer, 2016; Deseriis, 2017; Scheuerman, 2016; Gupta and Badve, 2017; Hua et al., 2018).

In contrast, term distribution within definitions of cyberterrorism remained consistent in their usage, with a relative dip between 2006 and 2010. However, post-2010 shows a significant re-adoption of these terms, with steady or, in certain cases (such as physical injury, fear, violence), increased term usage.

The fluctuations in term usage within the effect classification of cyberterrorism and hacktivism definitions can be attributed to numerous factors. For example, global focus on the terrorist attacks of 2001 led to speculations and concerns about extreme scenarios of how internet-based technologies and ICT could be used to terrorise and cause harm (Gomez and Whyte, 2021; Lawson, 2013, Lawson et al., 2016; Weimann, 2005; 2008), potentially affecting the choice and frequency of certain terms associated with cyberterrorism. Another factor may have been tied to understanding and interest towards the adoption of technologies, specifically in the increased development of web technologies. The dot-com bubble crash of the early 2000s, which led to a significant economic downturn for internet-based companies, may have contributed to a sense of distrust towards internet technology as a viable product (Abramson, 2005).

Further, Jaishankar (2018), writing about "digital-native" criminologists pursuing cyber-based research, that as these technologies develop, researchers will emerge with better understanding of this technology in comparison to earlier researchers, which Jaishankar terms "digital-immigrants" as people born before 1985 and have adopted digital technology later (Jaishankar, 2018:6), introducing new technical terminology, and potentially retiring or further explaining earlier terms.

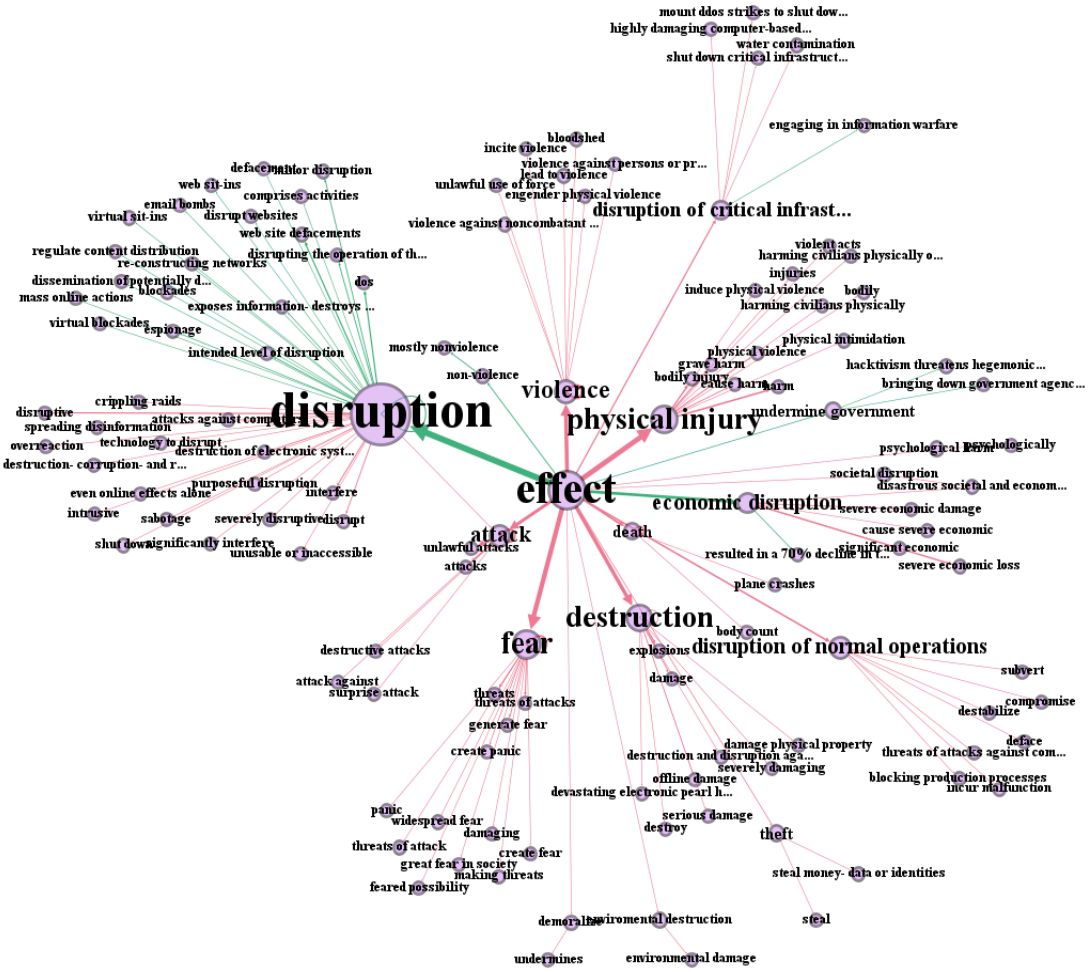


Figure 5.31 Network Distribution of Extracted Effect Terms

Figure 5.31 displays the distribution of terms within the ‘effect’ classification, represented by circles and extracted from definitions of both cyberterrorism (red lines) and hacktivism (green lines). The graph shows a wide variety of extracted terms associated with key coded terms.

The most notable code found within the ‘effect’ classification is ‘disruption,’ which has a total frequency of 32 extracted terms, with cyberterrorism contributing 15 terms and

hacktivism attributing 17 terms. This indicates that the concept of disruption is a significant aspect within the definitions of both cyberterrorism and hacktivism.

Overall, the extracted terms associated with the 'effect' classification are associated with definitions of cyberterrorism, with a total of 163 extracted terms, compared to hacktivism's 29 extracted terms, as shown in table 5.5 (page: 259).

Intent Classification

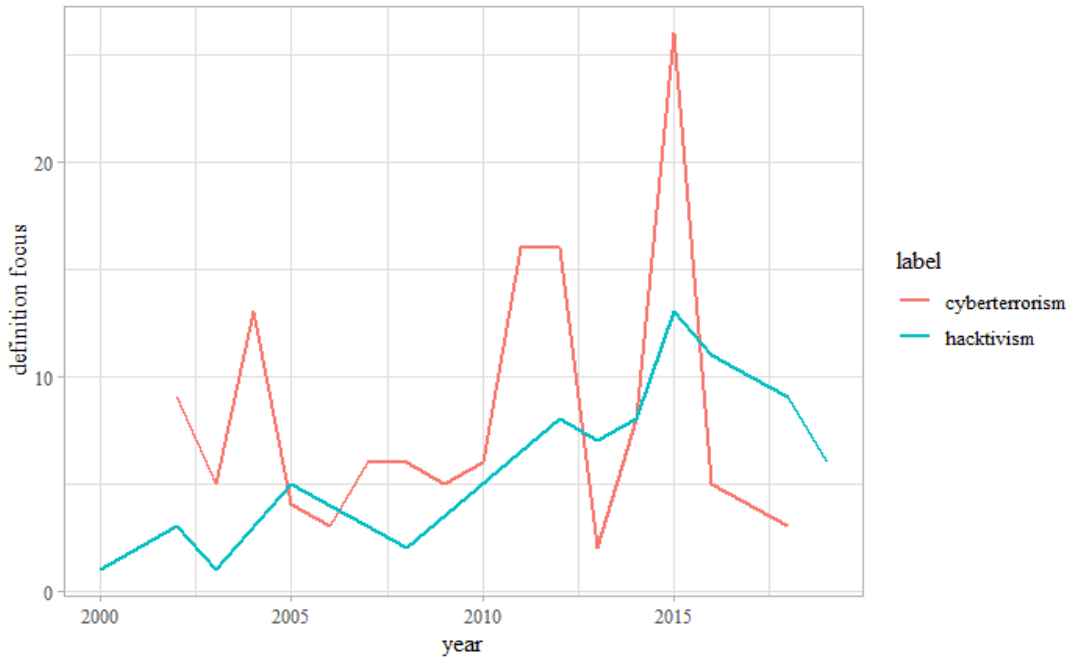


Figure 5.32 Yearly Distribution of Intent Classification

Figure 5.32 illustrates the distribution of coded extracts over a range of 19 years (2000 to 2019) for the intent classification of cyberterrorism (red line) and hacktivism (blue line) definitions. It is worth noting that the range of intent codes within cyberterrorism

definitions is evident between 2002 and 2018, while hacktivism definitions have a broader range spanning from 2000 to 2019.

As mentioned in the earlier discussion on taxonomies, Veerasamy et al. (2012) describe the objectives' classification, later referred to as 'intent,' as the desired outcome of an act. Subsequent work by Al Mazari et al. (2015) expands on this definition, proposing that the intent of cyberterrorism and hacktivism includes gaining political, social, military, or ideological advantages.

Comparing both phenomena, it becomes evident that cyberterrorism exhibits more prominent intent peaks (indicating significant term usage) and valleys (representing dips in usage) compared to the more gradual incline and decline of term usage within hacktivism definitions. Both cyberterrorism and hacktivism intent classifications reached their highest peaks in 2015, with cyberterrorism contributing the most coded terms (26) compared to hacktivism (13).

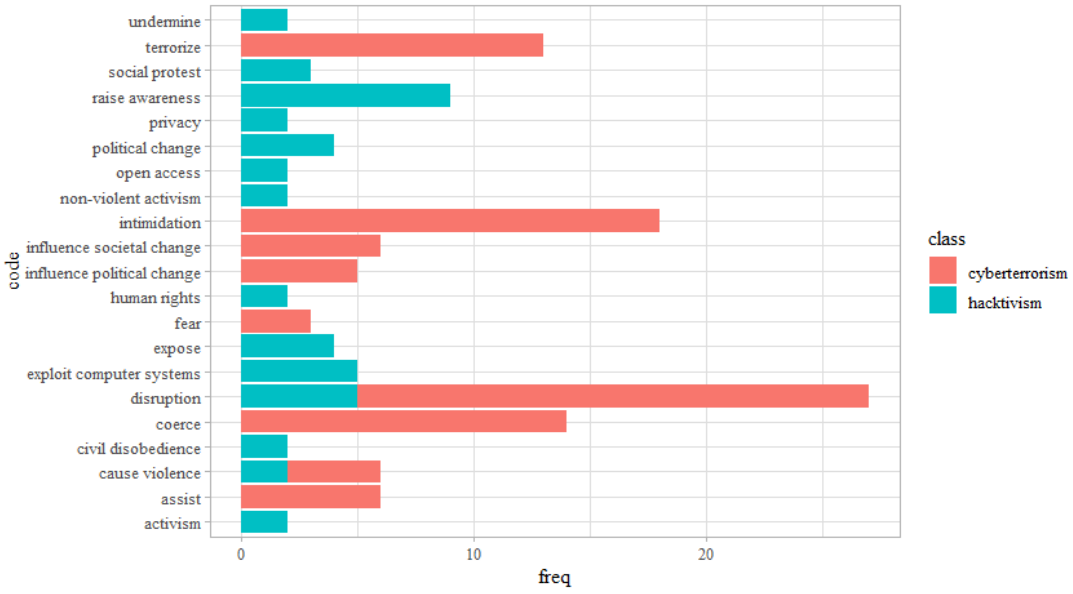


Figure 5.33 Total Frequency Distribution of Coded Intent Terms

Figure 5.33 displays the coded terms within the intent classification. Most coded terms (21) are associated with hacktivism, while cyberterrorism has fewer but more frequently used coded terms (11). Three coded terms (disruption, cause violence, influence political change) are shared between both cyberterrorism and hacktivism definitions.

Coded terms identified within cyberterrorism definitions attribute critical and severe intents, often seen in traditional terrorism research (e.g., Sánchez-Cuenca and De la Calle, 2009; Abrahms, 2012). These terms include “terrorize” (16), “intimidation” (29), “coercion” (24), “attack” (15), and “fear” (5). On the other hand, hacktivism contributes more nuanced coded terms, reflecting less frequently used terms such as “raise awareness” (12), “civil disobedience” (8), “non-violent activism” (7), “expose” (5), “exploit computer systems” (5), and “social protest” (5). These terms align with the more traditional

intentions of hacktivism, aiming to bring attention to certain issues, as seen in political activism literature (e.g., Norris, 2007).

The shared terms identified within the coded intent classification between cyberterrorism and hacktivism include both harm-inducing focus (cause violence) observed in cyberterrorism and the attention-focused intent (influence political change) characteristic of hacktivism. Additionally, both phenomena share a cyber-based means of causing disruption, which is significantly apparent in both cyberterrorism (17) and hacktivism (8).



Figure 5.34 Intent Code Distribution by Year & Frequency

Figure 5.34 depicts the distribution of coded terms within the intent classification, highlighting the wide variety of terms associated with hacktivism, particularly

accumulated towards the later years between 2012 and 2019. In contrast, cyberterrorism exhibits a more even distribution of terms with less variation between individual codes. As mentioned earlier, this pattern may be attributed to the increased adoption of information and communication technologies (ICTs) in both cyberterrorism and hacktivism.

The significant variety of terms within hacktivism definitions, especially in the later years, can be linked to the emergence and advancement of new and more accessible technologies. As these technologies continue to evolve, they bring forth novel ideas and use cases for actors involved in cyberterrorism and hacktivism, shaping their expected intentions and strategies.

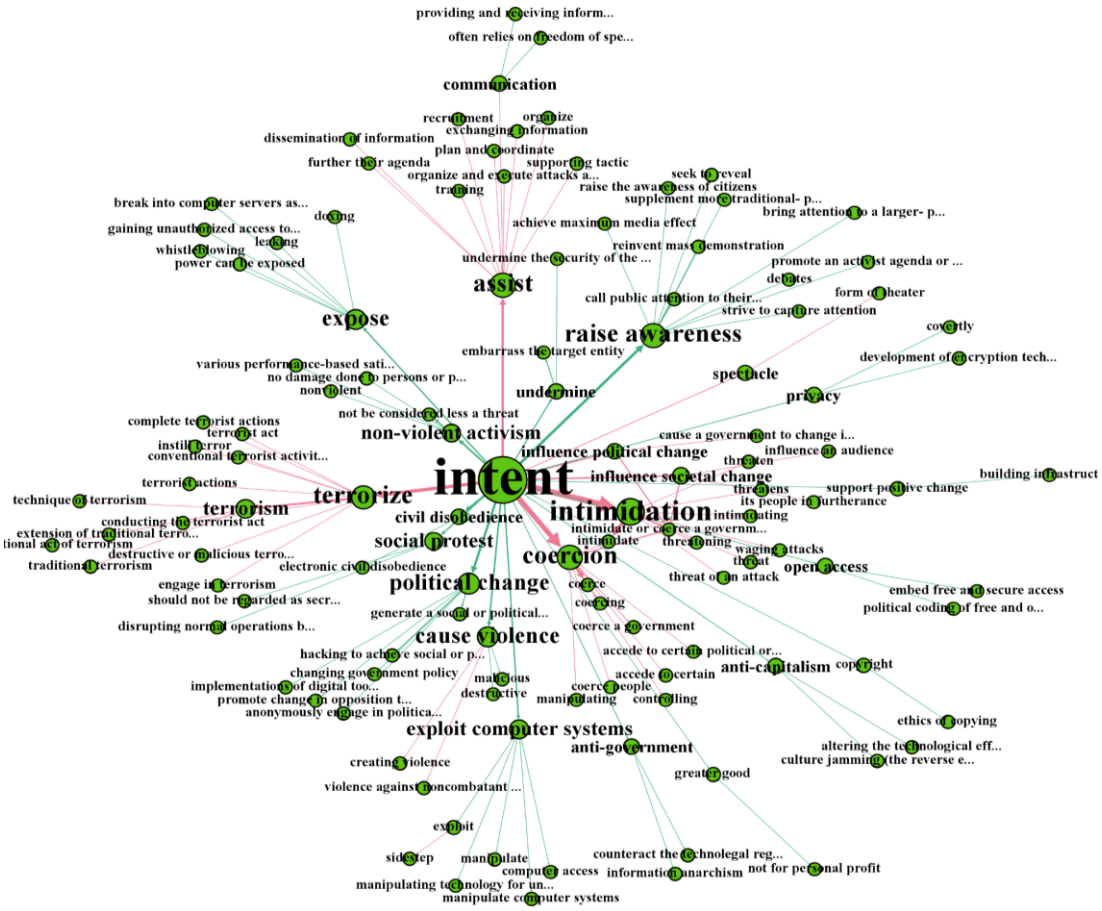


Figure 5.35 Network Distribution of Extracted Intent Terms

As previously mentioned, the intent classification is associated with the purpose pursued in both cyberterrorism and hacktivism. Al Mazari et al. (2015) propose that the intent can be related to gaining political, social, military, or ideological advantages. Figure 5.35 provides insight into what contributes to the intent of acts in both cyberterrorism and hacktivism, revealing a wide variety of terms.

In total, 133 raw terms were identified within the intent classification, and later coded into 32 distinct terms. Among these, 69 terms (52.7%) were associated with cyberterrorism, while 62 terms (47.3%) were related to hacktivism.

Means Classification

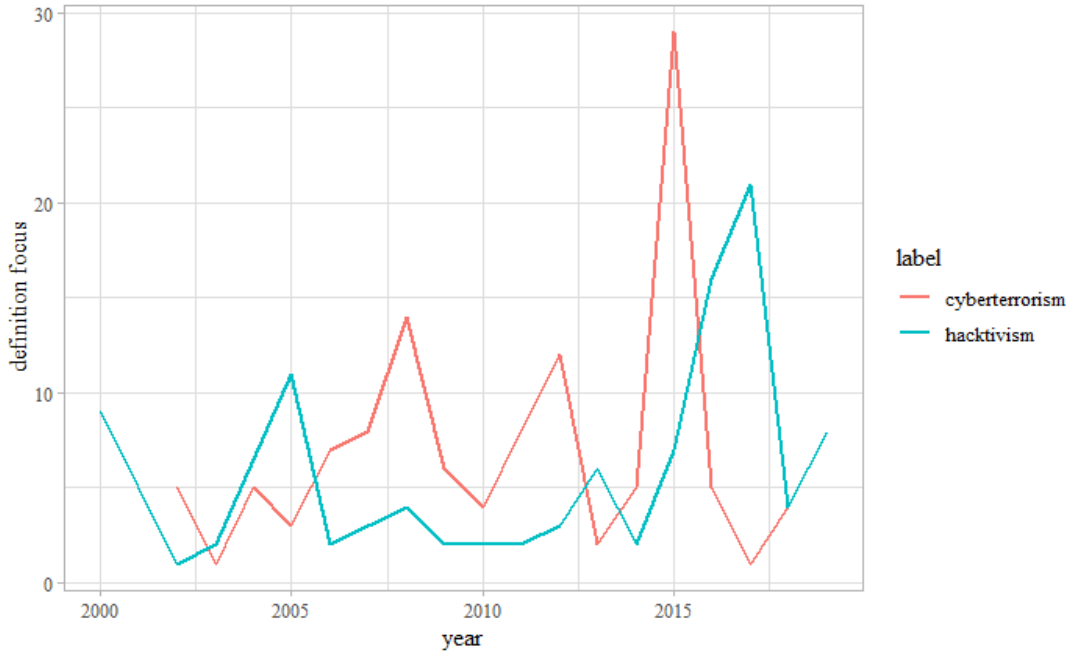


Figure 5.36 Yearly Distribution of Means Classification

Presented in figure 5.36 is the yearly distribution of the *means* classification for both cyberterrorism and hacktivism. Cyberterrorism (red line) is presented as a yearly range from 2002 to 20018, with hacktivism (blue line) ranging from 2000 to 2019.

The *means* classification focuses on how those conducting hacktivist or cyberterrorist activities achieve their intended outcomes and can be viewed as the modus operandi of the actor. The means classification, also known as the 'practice' classification by

Veerasamy (2009) mapped cyberterrorist practices (of which many can be extended to include hacktivism) such as the defacement of websites, distribution of disinformation, spreading propaganda, conducting denial of service attacks, and more directly: infecting computer systems with malware. These means of which to conduct cyberterrorism specifically were later extended by Veerasamy and Grobler (2010) to include means for the intent of anti-forensics, manipulation of data, and fundraising, and more modern utilities available with emerging cyber-technologies.

Comparatively, Figure 5.36 shows hacktivism with a significantly more prominent peak within the means classification, both earlier within the concepts range and later in its development. Coded terms identified within definitions of cyberterrorism present a more gradual increase in comparison with a significant peak in 2015, albeit with an equally significant drop off immediately following in 2016.

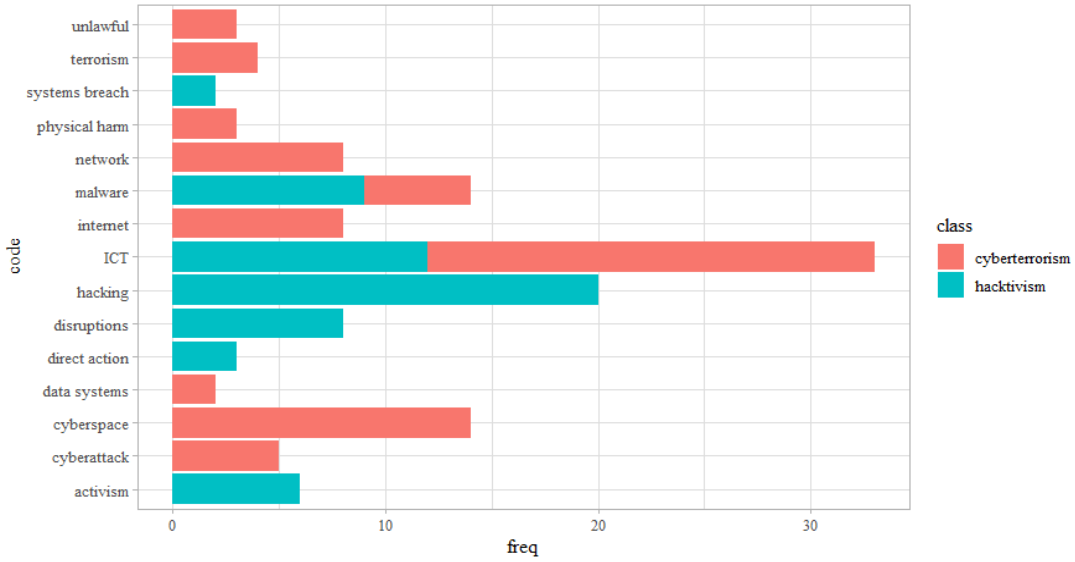


Figure 5.37 Total Frequency Distribution of Coded Means Terms

Figure 5.37 presents the distribution of coded terms within the means classification. Of the total 26 coded terms identified, 17 coded terms associated with definitions of cyberterrorism, and equally, 17 coded terms identified with hacktivism with eight of these coded terms shared between both definitions (malware; internet; infrastructure; influence; ICT; hacking; disruption; cyberattack). Key unique terms identified within cyberterrorism (9) include: terrorism (5), network (14), data systems (5), and cyberspace (16) attributing to the overall area of cyberterrorism in that much of the literature as discussed within the earlier bibliometrics findings chapter (see section 7.2.2.1 Identifying Key Themes from Co-citation Authors) discusses adoption of internet technologies by unspecified terrorist groups as a means of pursuing further terrorist activities such as those seen in the early 2000s post terrorist attacks of 9/11 (Goodman et al., 2007).

For unique key terms within definitions of hacktivism, only a single coded term (activism) was identified, followed by an array of smaller coded terms (systems breach; direct action; data breach) denoting to the traditional values of activism pursuing non-physical action by means of technically sophisticated actions.

Coded terms shared between both cyberterrorism and hacktivism contribute a considerable amount of term focus within the means classification, as illustrated by their frequency size in figure 5.37. Stark distribution exists between both cyberterrorism and hacktivism, as shown within the shared terms.

For example, although the coded term ‘cybercrime’ appears within both definitions, the frequency of use is considerably different with hacktivism (2) lower than cyberterrorism (9), equally the coded term ‘hacking’ is although similarly appears in select definitions, is considerably more common within definitions of hacktivism (29) in comparison to cyberterrorism (3). Notable shared terms with relatively similar usage frequency are both ‘malware’ or malicious software such as viruses and trojans used to exploit and manipulate computer systems (Rieck et al., 2008) within hacktivism (11) and cyberterrorism (10), and most significantly ‘ICT’ (information communication technology) having a coded term usage of 48 distributed between cyberterrorism (27) and hacktivism (21).

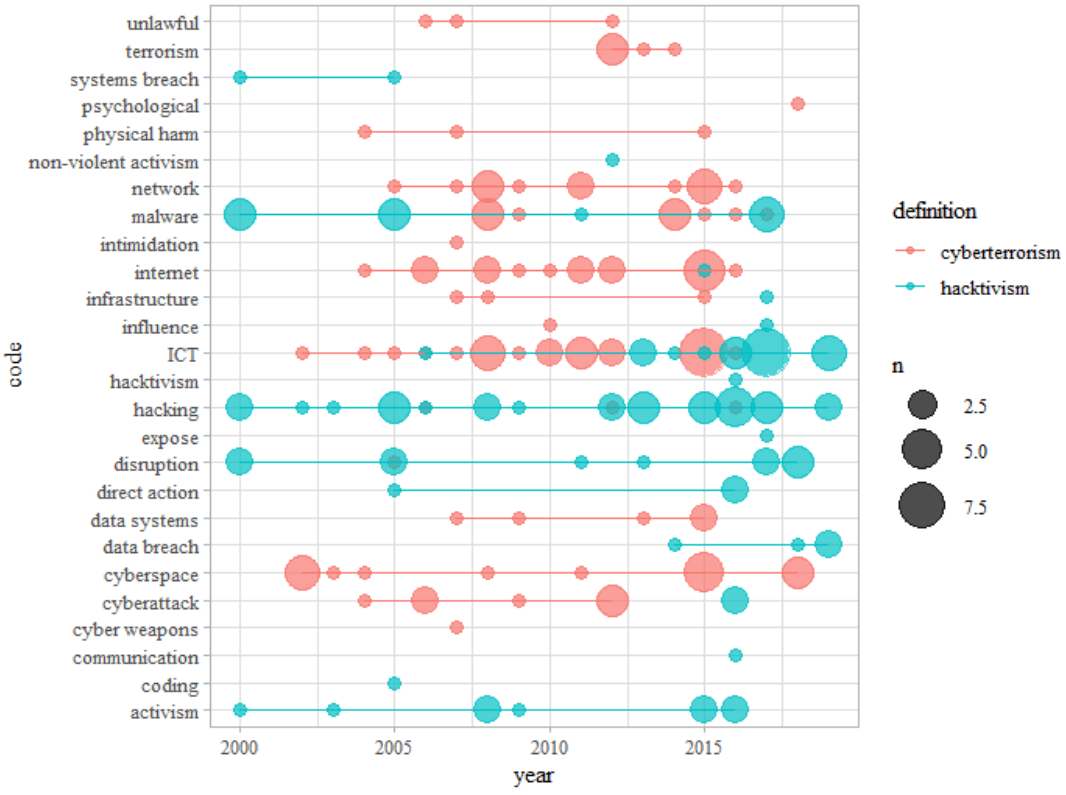


Figure 5.38 Means Code Distribution by Year & Frequency

Figure 5.38 presents the coded '*means'* terms as distributed by year and their frequency illustrated by point size (n). Key terms associated with cyberterrorism such as terrorism, network, data systems, and cyberspace have varying distribution rates. For example, '*cyberspace*' being one of the highest and earliest unique coded terms within cyberterrorism's *means* classification can be seen to have a variety of usage rates from 2002 to 2018, however. When viewing the distribution of '*terrorism*,' as a means of cyberterrorism, the coded term is brief in comparison to other key terms. Coincidently, both coded terms can be considered core components of cyberterrorism (Collin, 1997), the term itself being a portmanteau of *cyberspace* and *terrorism*. Therefore, to see terrorism only appear later into definitions of cyberterrorism as means may suggest the overall focus on viewing cyberspace, and its related key terms (network, data systems) as a major component. In comparison, terrorism and its more traditionally offline understandings are, although an important focus, not the focus when it comes to understanding the means of cyberterrorism.

Alternatively, the single key term '*activism*' associated within the means classification of hacktivism has seen relative use over several years. Certain shared terms, however, can be observed to relate more so with hacktivism in comparison to cyberterrorism. Notably, the coded terms '*hacking*' and '*disruption*,' as shown by Figure 5.38 are more frequently distributed amongst definitions of hacktivism in comparison to cyberterrorism definitions.

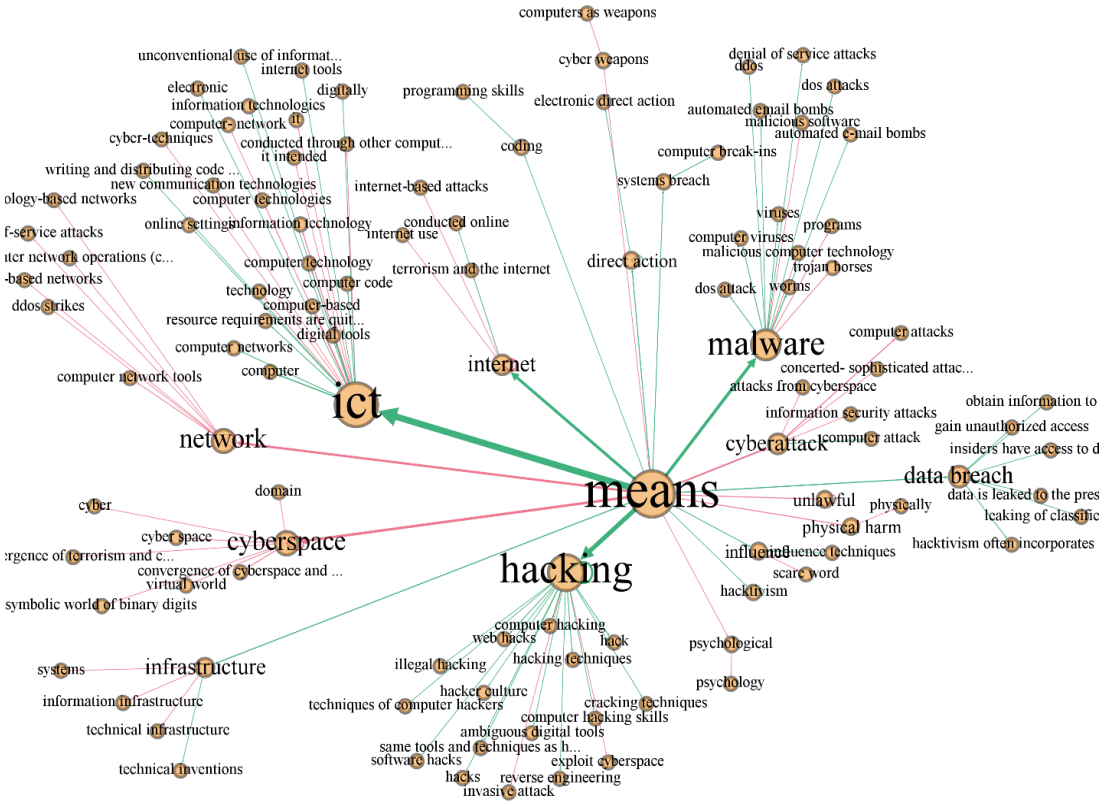


Figure 5.39 Network Distribution of Extracted Means Terms

Figure 5.39 presents the network distribution of extracted and coded terms within the means classification for both cyberterrorism (133) and hacktivism (84). As described earlier, the means classification maps the practices of those conducting either acts of cyberterrorism or hacktivism (Veerasamy, 2009). A total of 217 terms were extracted from definitions of both cyberterrorism and hacktivism, and later coded into 29 coded terms.

Motive Classification

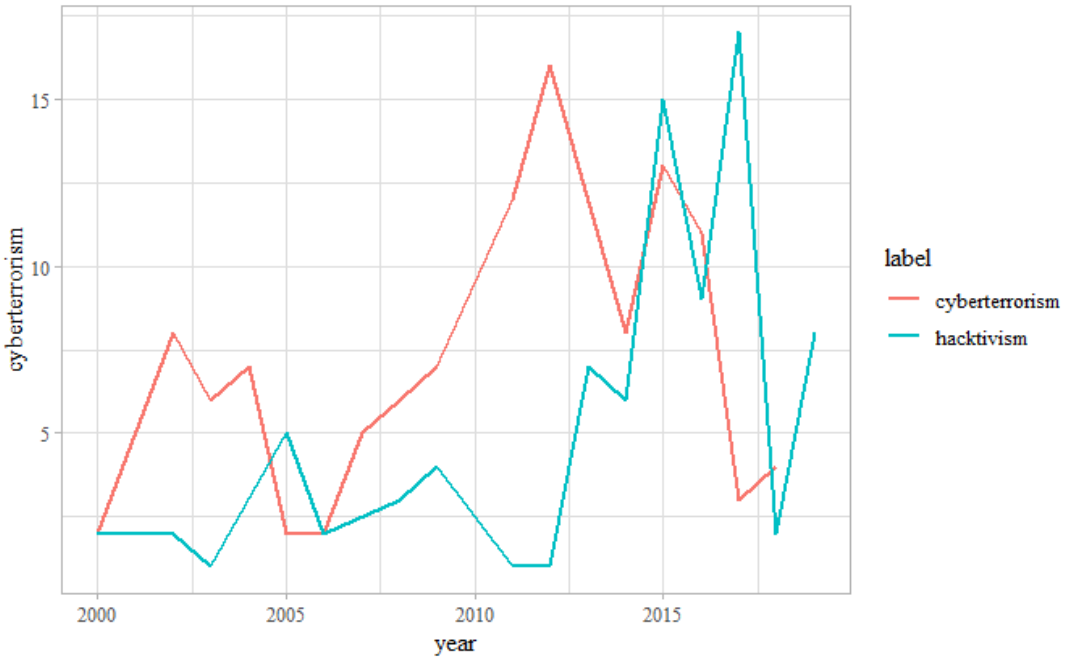


Figure 5.40 Yearly Distribution of Motive Classification

The motive classification delves into the driving forces behind the social phenomena of cyberterrorism and hacktivism. As previously mentioned, Veerasamy et al. (2012) associated motivation with numerous factors, including political, religious, and social ideologies, as well as economic, cultural, recreational, and premeditated reasons.

Figure 5.40 visually demonstrates the gradual increase in term usage within the motive classification for both cyberterrorism and hacktivism, with a notable dip in cyberterrorism in 2012. Intriguingly, as shown in figure 5.40, hacktivism experiences a significant surge in focus within the motive classification from 2013 onwards, while cyberterrorism displays a decline following its peak in 2012. The trend for hacktivism continues with substantial peaks in 2015 and 2017, followed by a considerable decrease in 2018.

The observed increase in terms associated with the motive classification over time suggests a growing interest in understanding the driving forces behind both cyberterrorism and hacktivism. This expansion may reflect researchers' attempts to delve deeper into the motivations of actors involved in these phenomena.

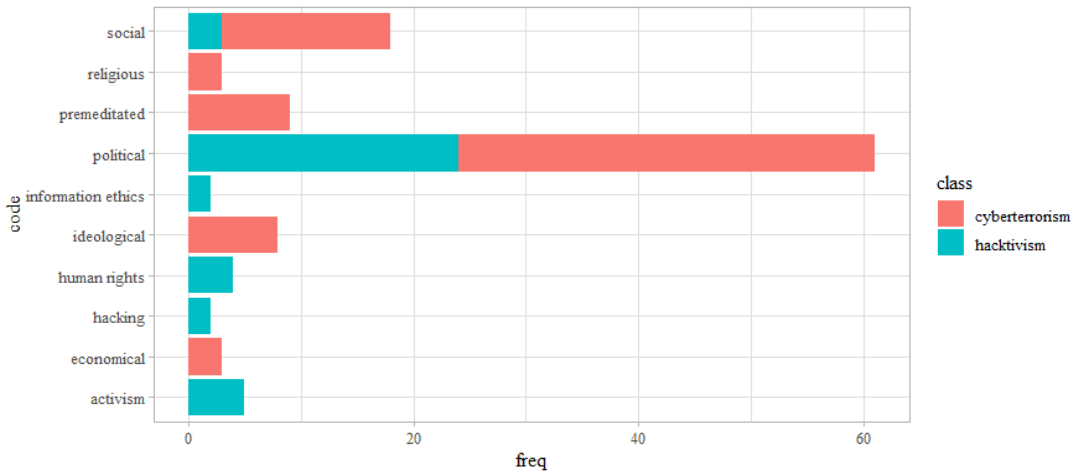


Figure 5.41 Total Frequency Distribution of Coded Motive Terms

Figure 5.41 displays the distribution of coded motive terms (197) within definitions of cyberterrorism (112) and hacktivism (85). The analysis reveals that cyberterrorism contributes four unique terms, while hacktivism offers eight unique terms, with four terms shared between both definitions.

Notably, the term 'political' (91) emerges as the most significant term in the motive classification, being the most frequently used term in both cyberterrorism (51) and hacktivism (40) definitions. The prevalence of the term 'political' as a motivation can be attributed to the extensive literature on terrorism and activism, which explores the political

motives, actions, and conflicts associated with both phenomena (Cohan, 2006; Abrahms, 2012; Norris, 2007).

Several terms are shared between both cyberterrorism and hacktivism, including ‘social’ (31), ‘ideological’ (17), and ‘religious’ (9). Additionally, definitions of cyberterrorism feature a unique term, ‘premeditated’ (13), while hacktivism introduces two unique key terms: ‘activism’ (9) and ‘human rights’ (7).

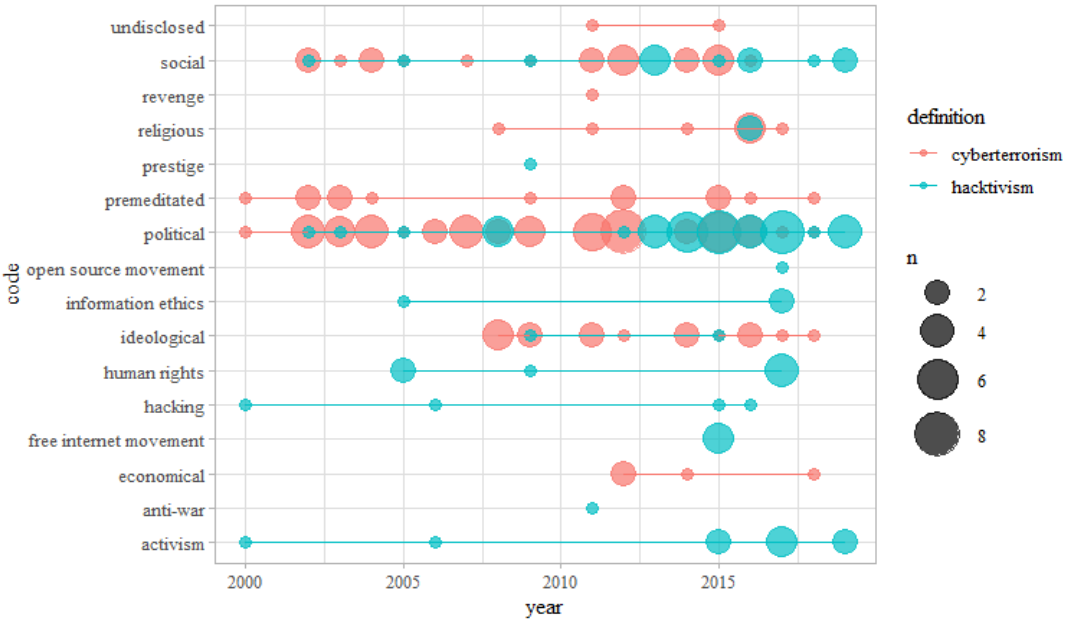


Figure 5.42 Motive Code Distribution by Year & Frequency

Figure 5.42 illustrates the distribution of coded terms within the motive classification plotted along a yearly timeline. The analysis reaffirms the significant usage of the coded term ‘political’ throughout the dataset period (2000 - 2020), with a notable increase in its usage within definitions of hacktivism from 2013 onwards.

This sudden emergence of political motivation can be attributed to specific events and cyberattacks conducted by activist groups during 2012. For instance, the online Marxist-Leninist activist group Redhack conducted politically motivated attacks on Turkish institutions (Polat et al., 2013). Additionally, the decentralised network Anonymous orchestrated cyberattacks against various American government institutions and media industries (Sauter, 2013). Both events in 2012 triggered significant interest in understanding hacktivism (Goode, 2004; Bodó, 2014; Tanczer, 2016; George and Leidner, 2019) and led to efforts in classifying hacktivism (Seebruck, 2015; Gupta and Badve, 2017; George and Leidner, 2019).

The notable increase in the usage of 'political' as a motive within hacktivism definitions from 2013 onwards suggests a growing emphasis on political ideologies driving hacktivist activities during this period. It reflects a shift in the focus of hacktivism towards politically motivated actions and causes. This observation is further supported by the significant growth in hacktivism's motive classification from 2013 to 2019.

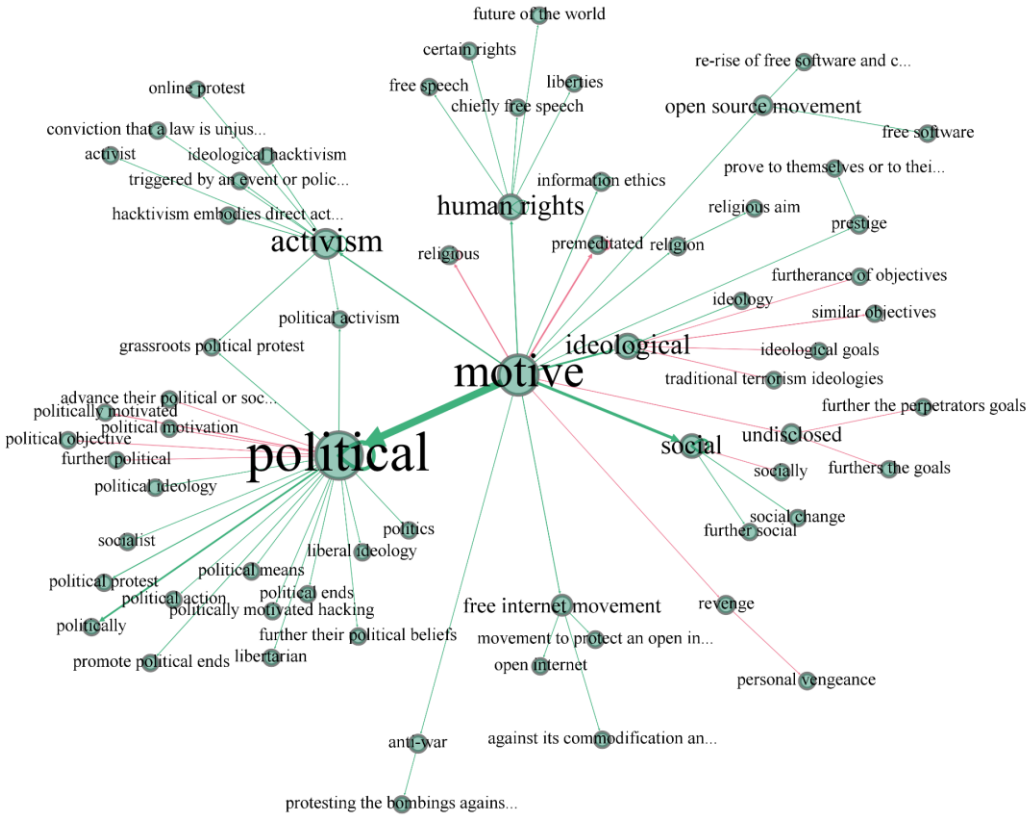


Figure 5.43 Network Distribution of Extracted Motive Terms

Figure 5.43 presents the network distribution of both coded and extracted terms within the motive classification, revealing a high degree of variety, particularly associated with definitions of hacktivism. For instance, the most prominent coded term ‘political’ shares many similarly themed extracted terms, focused on furthering political objectives and goals. Within the extracted terms associated with hacktivism, concepts such as liberalism and socialism were identified, indicating a diverse range of political ideologies that underpin hacktivist activities.

This comparative variety in the motive classification can also be observed beyond the ‘political’ code. Many unique coded terms contribute to a greater variety of extracted

terms within definitions of hacktivism when compared to cyberterrorism. This observation can be attributed to the more situational and case study-oriented usage of terms within hacktivism literature, as seen previously in the intent, effect, and actor classifications. Hacktivism, as a phenomenon driven by a wide range of political, social, and ideological motivations, tends to attract a diverse set of actors with varying objectives. Consequently, the coded terms within the motive classification capture a broad spectrum of motivations, leading to the diversity observed in the extracted terms.

Target Classification

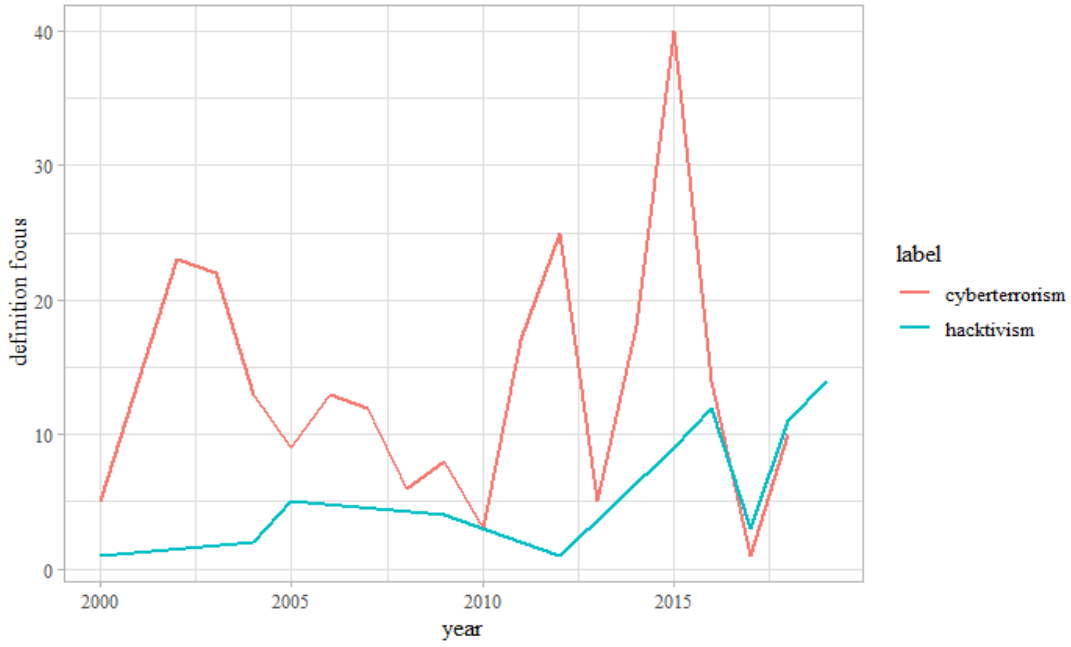


Figure 5.44 Yearly Distribution of Target Classification

Illustrated in Figure 5.44, the yearly distribution of the target classification as coded from definitions of both cyberterrorism and hacktivism is presented. The target classification refers to the intended recipient of the actor's effect (Veerasamy et al., 2012). In the context

of cyberterrorism, it is notable that targeting a single individual would not typically amount to an act of cyberterrorism. Instead, cyberterrorists seek to cause detrimental effects on critical targets with wide-reaching implications.

As shown in the figure, cyberterrorism (red line) exhibits more prominent peaks and valleys in term usage compared to the more gradual incline and decline observed in definitions of hacktivism (blue line). Cyberterrorism contributes significantly more extracted terms (244) to the target classification in comparison to hacktivism (64).

The higher number of extracted terms in cyberterrorism indicates a wider variety of targets associated with cyberterrorist activities. These targets may include critical infrastructure, government agencies, financial institutions, and other high-profile entities that, if disrupted or compromised, can have significant consequences on a large scale.

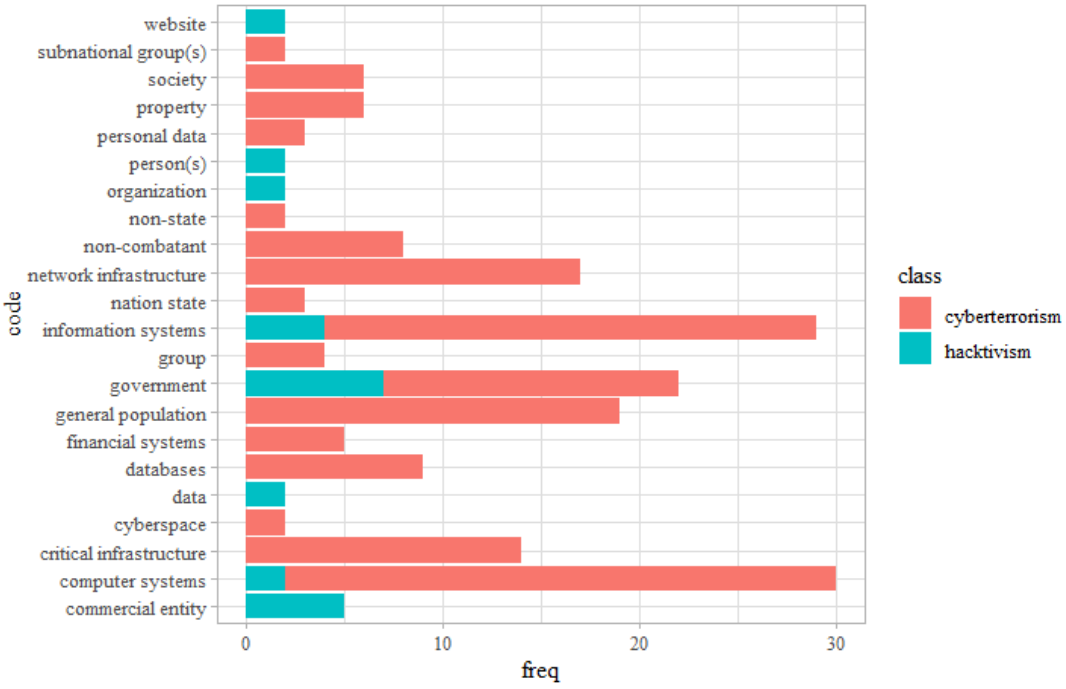


Figure 5.45 Total Frequency Distribution of Coded Target Terms

Figure 5.45 illustrates the contrast in coded term frequency for both cyberterrorism (21) and hacktivism (16) within the target classification. Cyberterrorism provides a higher number of coded terms (21) compared to hacktivism (16). Within these coded terms, cyberterrorism has 11 unique terms, hacktivism has 6 unique terms, and there are 10 terms shared between both social phenomena.

Key coded terms unique to cyberterrorism include “critical infrastructure” (25), “data systems” (11), “non-combatant” (11), and “property” (8). These terms align with Grobler et al.’s (2012) views that acts of cyberterrorism aim to cause detrimental effects on critical targets with far-reaching impacts, rather than targeting specific individuals. Cyberterrorism’s focus on critical infrastructure and data systems reflects its intention to disrupt essential services and cause considerable damage.

On the other hand, key coded terms unique to hacktivism include “commercial entity” (8) and “persons” (5). These terms suggest that hacktivism selects targets with more refinement and precision, without the intention of causing critical disruption and impact to the wider population. Hacktivism’s focus on commercial entities may be related to protests corporations or industries, while the term “persons” may indicate targeting specific individuals or groups associated with certain causes.

Among the terms shared between both cyberterrorism and hacktivism, the majority are associated with cyberterrorism. These terms include “computer systems'” (49), “general population” (36), “government” (31), “information systems” (34), and “network infrastructure” (29). These terms highlight cyberterrorism as having a much broader targeting approach, encompassing both government and civilian targets, along with information systems and computer networks. In contrast, hacktivism’s shared terms, such as “website” (7), “organization” (5), and “information” (5), indicate a more specific focus on online entities and data dissemination.

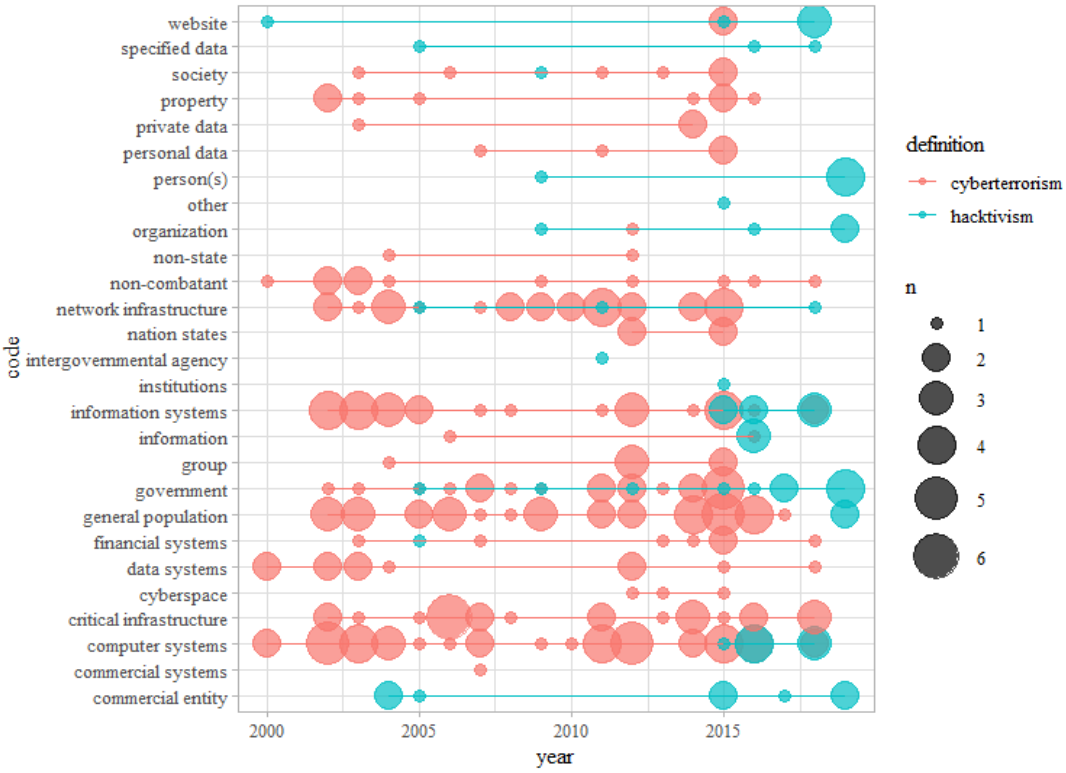


Figure 5.46 Target Code Distribution by Year & Frequency

Figure 5.46 illustrates the yearly distribution of coded terms within the target classification. The distribution shows that coded terms are associated with definitions of cyberterrorism, particularly between the years 2002 and 2015. On the other hand, definitions of hacktivism show a notable increase in term usage post-2014, with much of its distribution prior to 2015 consisting of singular use cases of coded terms.

The concentration of coded terms within cyberterrorism definitions between 2002 and 2015 may be attributed to the growing interest and research on cyberterrorism during that period. Cyberterrorism emerged as a significant concern in the early 2000s, especially in the aftermath of the 11th of September 2001 attacks, which prompted increased attention to potential cyber threats (Gross et al., 2016; 2017) This heightened interest led to a surge

in research and discussions on cyberterrorism, resulting in a larger number of coded terms associated with this social phenomenon.

In contrast, hacktivism appears to have gained more prominence in the academic discourse in the latter half of the analysed period, most notably post-2014 (Goode, 2015; Hai-Jew, 2015; Klein, 2015; Stamm, 2015). This could be linked to notable hacktivist activities during this time, such as the emergence of high-profile hacktivist groups like Anonymous and their involvement in various cyber operations (Machado, 2015; Sorell, 2015). These events sparked increased interest among researchers, leading to a rise in the usage of coded terms in defining hacktivism (Alexopoulou and Pavli, 2019).

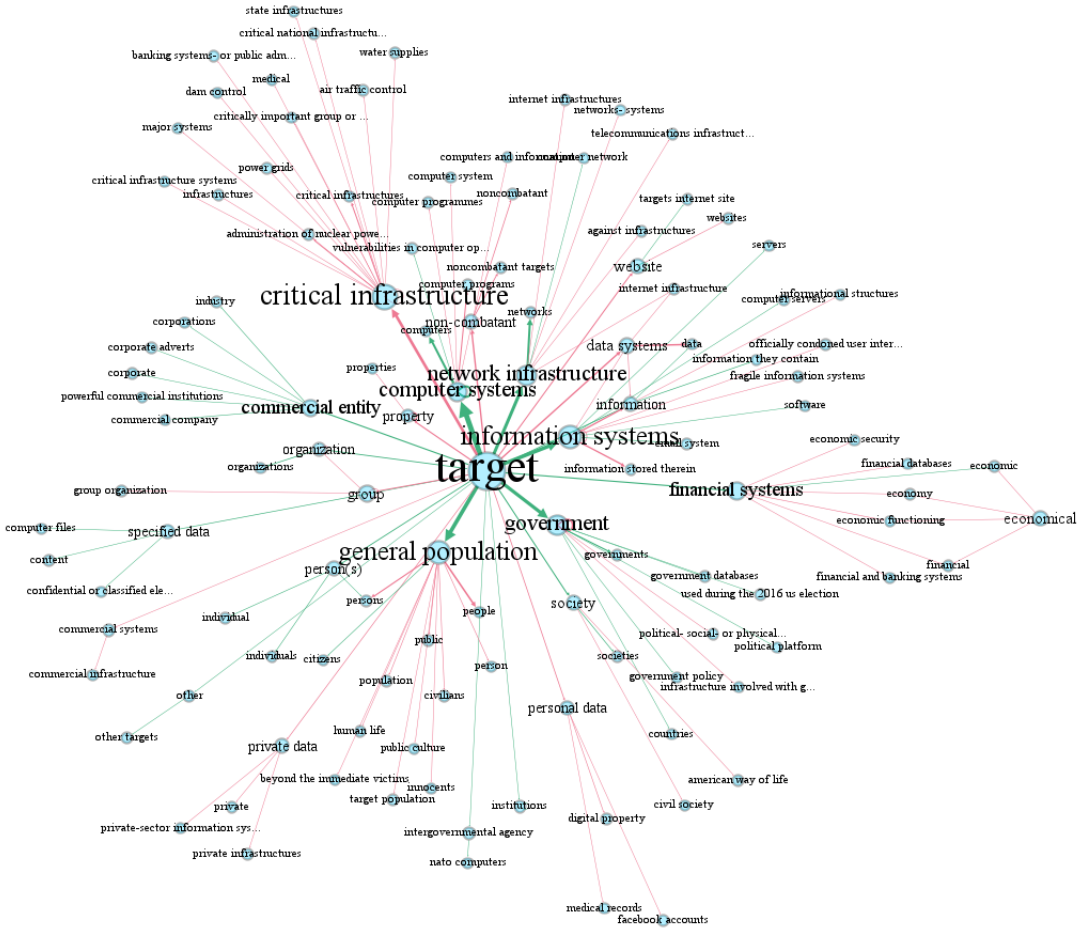


Figure 5.47 Network Distribution of Extracted Target Terms

Figure 5.47 represents the distribution of coded and extracted terms within the target classification, showcasing the intended recipients of the actor's effect in both cyberterrorism and hacktivism. The target can be an object, organisation, system, person, or any combination of the extracted and coded terms presented.

In the analysis, cyberterrorism contributed a total of 244 extracted terms, out of which 36.47% (89) were unique to cyberterrorism definitions. Hacktivism, on the other hand, provided 64 extracted terms, with a higher proportion of 65.6% (42) being unique to

hacktivism definitions. In total, the content analysis of cyberterrorism and hacktivism definitions within the target classification resulted in 308 extracted terms, out of which 42.53% (131) were unique.

5.3.3 Synthesising the Taxonomy

The present study undertook a systematic process of extracting, coding, and organising terms from definitions of cyberterrorism and hacktivism. The resulting terms related to cyberterrorism were then integrated into a consolidated taxonomy, which encompasses the existing ontological framework proposed by Veerasamy et al., (2012) along with the subsequently developed taxonomies by Al Mazari et al. (2015) and Plotnek and Slay (2021).

The aim of this consolidation was to establish a comprehensive and cohesive taxonomy that captures the multifaceted dimensions of cyberterrorism and hacktivism, as evident in the diverse definitions collected from the academic literature. The process involved identifying and categorising terms into relevant taxonomic classifications, such as actor, effect, intent, means, motive, and target.

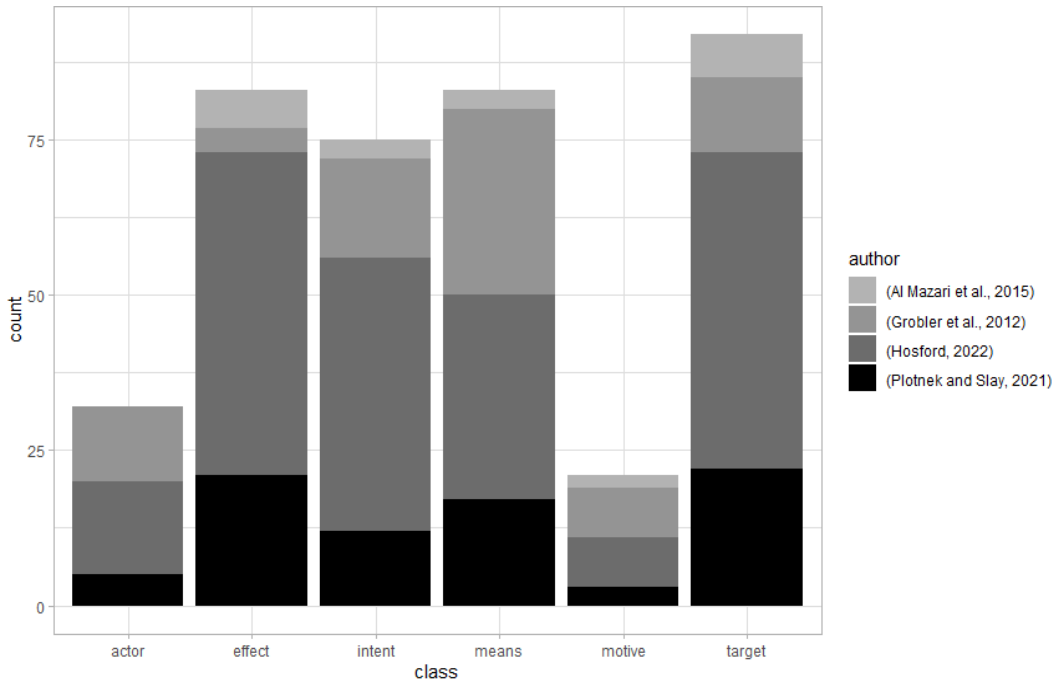


Figure 5.48 Updated Merged Cyberterrorism Taxonomy Term Distribution

Figure 5.48 presents an updated and refined version of figure 4.6 (Figure 4.6: Merged Cyberterrorism Taxonomy Term Distribution: 187) showcasing the distribution of each author's unique term contribution to the respective taxonomic classes within the merged cyberterrorism taxonomy. The content analysis of definitions yielded a significant increase in uniquely identified terms, amounting to 52.6% (203) of the total extracted terms. This represents a substantial growth of 130.12% in identified terms over the previous merged taxonomy, resulting in a total of 386 terms now present within the consolidated cyberterrorism taxonomy with a visual representation of this taxonomy provided within the appendix.[12]

[12] Visual network map of the modified taxonomy (see Appendix 7: 431)

Developing and Integrating a Hacktivism Typology

Having adopted a similar approach of both extracting, coding, and analysing terms associated with definitions of hacktivism similarly seen within the analysis of cyberterrorism definitions, a taxonomic model can be developed with the distribution of this taxonomy illustrated in Figure 5.49.

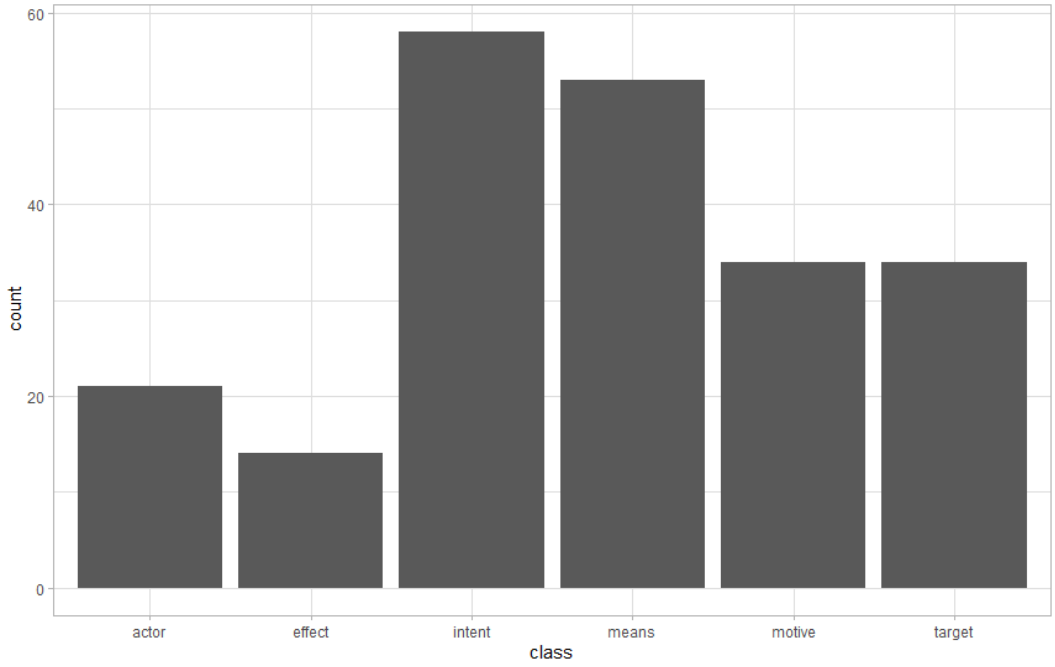


Figure 5.49 Overview of Hacktivism Taxonomy Term Distribution

Following a method analogous to the analysis of cyberterrorism definitions, a comprehensive examination of hacktivism definitions was conducted. This involved the extraction, coding, and analysis of terms associated with hacktivism, guided by the earlier taxonomic framework. The outcome of this process enabled the development of a refined taxonomic model, encapsulating the key themes and categories extracted from definitions of hacktivism. Figure 5.49 illustrates the distribution of this refined hacktivism taxonomy.

In a manner comparable to the cyberterrorism taxonomy, the hacktivism taxonomy offers valuable insights into the core elements and conceptual relationships within the domain of hacktivism. By consolidating the extracted terms and categorising them based on their thematic relevance, the taxonomic model provides a cohesive and systematic representation of hacktivism-related concepts.

5.3.4 Summary of Quantitative Content Analysis

In part two of the findings, a taxonomic framework based on prior works by Al Mazari et al. (2015) and Veerasamy et al., (2012) was used to classify the findings of the quantitative content analysis of cyberterrorism and hacktivism definitions. Extending Plotnek and Slay's (2021) taxonomy, this chapter provided a detailed distributional analysis of terms within six proposed classifications (actor, effect, intent, motive, means, and target) over a period spanning 2000 to 2020. The results provide valuable insights into the evolving conceptualisation of these phenomena and shed light on the choice of terminology of research in each classification over time.

In the actor classification, both cyberterrorism and hacktivism definitions primarily focused on actors with high ICT skills, such as hackers or hacktivists. Over time, hacktivism definitions expanded to include more traditional activist terms. In the effect classification, cyberterrorism was associated with more severe and harmful effects, while hacktivism focused on disruption and communication-based actions to bring attention to issues. The intent classification revealed that both cyberterrorism and hacktivism were

motivated by political objectives, with cyberterrorism exhibited more pronounced peaks in term usage over time.

Additionally, the motive classification showed a gradual increase in term usage for both phenomena, while hacktivism experienced a significant increase in focus from 2013 onwards. The target classification highlighted that cyberterrorism provided a larger number of extracted terms, concentrating on critical infrastructure and data systems, while hacktivism displayed a higher proportion of unique terms, suggesting a more precise targeting approach.

The analysis showcases the distinct trajectories of cyberterrorism and hacktivism over time, with hacktivism displaying a more gradual increase in terms and cyberterrorism experiencing more fluctuations in term usage. Conclusively, the study provided a comprehensive and systematic understanding of the evolving landscape of cyberterrorism and hacktivism definitions, serving to distinguish each phenomenon and provide a valuable resource for researchers seeking to navigate these complex and dynamic ideologically motivated forms of disruptive hacking.

Chapter 6. Discussion

6.1 Introduction and Project Aims

This research project is interested in understanding the development of cyberterrorism and hacktivism research, and how researchers have conceptualised and defined both phenomena throughout published academic publications. To achieve this, 126 high-impact peer reviewed articles related to cyberterrorism and hacktivism were identified, collected, and analysed using a triangulation design data transformation model (Creswell and Plano Clark, 2007:77) to investigate the academic literature using bibliometric and content analysis methods.

The collection and search criteria used four academic search engines and three publisher databases recorded using a PRISMA-flow process and limited to peer-reviewed academic articles with a minimum Google Scholar citation value of 10 (see section 4.2.4 Data Screening). The focus of the articles identified were limited to those with either cyberterrorism, hacktivism, or both as its primary research topic. A timeframe of 20 years (2000 to 2020) was adapted to capture most publications prior to analysis, starting with one of the earliest and most notable publications by Denning (2000a). The result of this literature collection process was a dataset of 126 high-impact peer-reviewed articles in which to evaluate using bibliometrics. Later, a review of these publications identified 87 publications with definitions of either cyberterrorism, hacktivism, or both for which to evaluate using quantitative content analysis. The result of this quantitative content

analysis was the evaluation of 237 definitions, which when analysed provided 1242 extracted terms that were then classified and developed into a pre-existing taxonomic framework.

6.1.1 Key Findings and Contribution

To complete the objective of this study, the following section will outline the key findings of the earlier bibliometric analysis and content analysis of high-impact journal articles pertaining to academic understandings of cyberterrorism and hacktivism. These findings address the central research questions concerning the evolution and current landscape of cyberterrorism and hacktivism within the academic discourse.

Finding One: How has the academic development of cyberterrorism and hacktivism research evolved over time.

The bibliometric analysis revealed that while earlier challenges such as the difficulty in achieving consensus definitions and a lack of empirical research based on primary data have hindered progress, these issues do not reflect the lack of effort towards consolidating definitions, nor engaging in data-driven research. Indeed, researchers have produced valuable studies contributing to the field. However, a more significant concern arises from the fragmented and dispersed epistemological landscape of cyberterrorism and hacktivism research making such efforts towards effective dissemination difficult. This limited exposure to the variety of research efforts leads researchers to recycle foundational theories, thus restricting the broader impact of their research output.

The study revealed that the field includes a diverse array of authors from disciplines within both the humanities, primarily terrorism studies, and computer sciences. However, the research contributions were single high-impact articles from the global north. The limited consistent publication output by individual authors or in peer-reviewed journals underscores the need for a more collaborative research environment. These findings suggest that the establishment of a dedicated annual academic journal could bring together researchers, and facilitate ongoing evaluation and contribution, enhancing the collective impact of research in this domain.

Finding Two: What distinct, key definitional characteristics have emerged for both phenomena.

A content analysis was conducted using a specific taxonomic framework to code definitions of cyberterrorism and hacktivism, revealing clear distinctions in their conceptual development. Initially, the operational aspects of both phenomena blurred their definitions. However, the analysis highlighted that cyberterrorism actors were often inadequately detailed, whereas hacktivism actors were distinctly associated with specific events and movements that clearly framed their motivations and impacts. Moreover, the motivations of hacktivists, driven by ideals such as social justice, freedom of speech, and anti-capitalist philosophies, stood in stark contrast to the vague intentions of cyberterrorists, who were primarily motivated by causing disruption and harm, backed by non-specific social and political ideologies.

These findings reveal that beyond the operational and practical actions of cyberterrorism and hacktivism, the phenomena of ideologically motivated cyber-events and their actors are distinct and warrant more multifaceted research. The findings urge future studies to adopt holistic approaches to deepen understanding beyond the techno-centric focus of both phenomena.

Unique Contributions of Study:

First, the study extends the limited academic research towards the understanding of cyberterrorism and hacktivism. This study is one of the first to provide a bibliometric analysis within the domain, mapping its production of knowledge within a focused lens of manually assessed key and highly cited peer-reviewed publications, and its contributing researchers. This contribution highlights the gaps in knowledge production, limited diversity, and the difficulties of fragmentation within the domain, raising awareness of a significant key issue impacting the production and dissemination of knowledge.

Second, to the knowledge of the author, this study is the first known to conduct a quantitative content analysis of academic definitions for both cyberterrorism and hacktivism, aiming to destandardize and replace existing definitions with a six-point taxonomy to better guide future research. The focus on academic definitions addresses the broader implications of how these phenomena are conceptualised within the scholarly community. By establishing a comprehensive taxonomic framework, this research clarifies current definitions and identifies areas lacking consensus or further knowledge, thus directing future studies to address these gaps. Additionally, the inclusion of temporal

mapping ensures that the evolving dynamics of cyberterrorism and hacktivism are more accurately understood and represented in academic discourse, fostering a more informed and effective research agenda.

Methodologically, this study contributes by adopting an innovative approach to knowledge mapping. In embracing both a mixed-methodological approach and leveraging open-source technologies, the study markedly advances upon a preceding knowledge framework initially introduced by Edna Reid and colleagues within the domain of terrorism studies (see Reid, 1993; Reid et al., 2004; Reid and Chen, 2006; 2008), thus contemporizing the methodology of science mapping to better suit the evolving landscape of research.

6.1.2 Outline of Discussion

To address the research questions, the discussion chapter is broken into two key areas to conclude the triangulation design framework by comparing results with findings, and subsequently concludes with the consolidation of findings to provide an overall interpretation (Creswell and Plano Clark, 2007:62). The first area will discuss the domain of cyberterrorism and hacktivism research over a 20-year period (2000-2020) and its productivity in reference to the challenges seen in collaboration and output. The second discussion focuses on the conceptual development of cyberterrorism and hacktivism through the analysis of definitions presented and adopted within the publications. This identifies key conceptual challenges and differences in defining both cyberterrorism and

hacktivism as unique and distinctive forms of ideologically motivated forms of disruptive hacking, organised into the six taxonomic classifications.

6.2 A Bibliometric Analysis of Cyberterrorism and Hacktivism Research.

Research on both cyberterrorism and hacktivism has experienced substantial growth since 2000. If this growth was to be indicative of an ideal outcome, it would suggest the domain is fulfilling that of a "Mertonian norm" (Anderson et al., 2010; Merton, 1942), where knowledge is shared, adequately scrutinised, and the possibility for new researchers and significant advancements within the field is fostered, promoting a collaborative and open scientific community dedicated to understanding and addressing the challenges posed by cyberterrorism and hacktivism. In fact, if we return to chapter two of this thesis, these ideals suggest a period of paradigm stability (Kuhn, 1970; 1977), consisting of shared beliefs, methodologies, and theories towards understanding both phenomena. However, when delving into cyberterrorism and hacktivism research output more critically, the apparent increase in research output raises concerns of a potential "stagnation" within these emerging domains as issues such as the lack of empirical data and definitional confusion emerge (Conway, 2014a; 2018; Gordon and Ford, 2002;2006; Jarvis and Macdonald, 2015; Jarvis et al., 2014; Macdonald et al., 2019), issues analogous to earlier discussions in related areas such as terrorism studies (Sageman, 2014; Schmid, 2014; Silke, 2001) and organised crime research (von Lampe, 2008).

6.2.1 A Domain of Stagnation or Fragmentation?

The concept of research stagnation draws heavy weight. A suggestion of such often brings immediate discussion, counter arguments, and potential criticism to such claims. Bhattacharya and Packalen (2020) propose that stagnation is tied closely to the production of "good" concepts, and that difficulties to propose these concepts inevitably leads to a slowdown of productive research that pushes knowledge forward. Returning to earlier discussions of Kuhn, scientists' have strong allegiance to successful definitions of scientific paradigms (1970:10). The suggestion of stagnation thus, rebels against these paradigms that many prominent scientists have established themselves alongside, and in turn suggests a potential lack of 'good' concepts, theories, ideas, etc. that push forward scientific progress.

One such notable 'rebellion', or more appropriately; 'critique' was that of Marc Sageman's (2014) argument that, despite significant research funding in response to the events of September 11th, terrorism studies was no nearer to understanding "what leads a person to turn to political violence?" than when started and as such, stagnated in introducing a conclusive answer. Sageman's critique drew significant and continuous reflection on the health of terrorism studies, but also strong criticism of the claim made. For example, Stern (2014) shortly after Sageman's publication criticised the argument suggesting that it was an oversimplification of a much grander issue, a criticism equally shared by Schmid (2014). Both place emphasis on the generalisation of Sageman's comment, focusing predominantly on its singular question and emphasis towards the inclusion of "a person" (Schmid, 2014:588; Stern, 2014:607), with Taylor later

acknowledging that such statement dismisses the extensive work that has been done by terrorism researchers (Taylor, 2014:582). Interestingly, Taylor further posited that younger researchers may see Sagemen's critiques more positively, viewing such comments as encouragement to work towards new and different perspectives within terrorism studies (Taylor, 2014). Interestingly Silke and Schmidt-Petersen (2017) later argued that terrorism studies was not seeing a period of stagnation at this time, but this was instead a period of innovation, as seen by the growing number of publications using wider ranges of data collection and analysis techniques (also Frumkin, Morrison, and Silke, 2023:6).

Therefore, as a novice researcher susceptible to being enticed by Sagemen's challenging critique, it is crucial to concentrate on avoiding a broadly generalised discourse regarding the apparent "stagnation" in cyberterrorism and hacktivism research. Analysing 126 high-impact articles might not adequately represent the entire domain but could instead offer insights primarily from its widely cited contributors. This parallels how a field survey or interviews with specific scholars might present a respectable yet selective viewpoint. This section of the discussion instead argues for the potential issue of fragmentation, not stagnation existing within the cyberterrorism and hacktivism research domain.

Argument for such fragmentation comes from the synthesis of bibliometric findings. Most notably, the sparse number of high-impact collaborative research efforts, and prominence of single-authored publications in a dispersed collection of journals. Although this study makes frequent reference to such outcomes in terrorism studies, the higher frequency of

single-authored publications outweighing co-authored exists in many striving fields (Del Carmen and Bing, 2000; Hosford et al., 2021; Lemke et al., 2015). Similarly identified within the bibliometric analysis was an over-abundance of unique journals. A total of 98 individual journals were identified from the 126 publications examined. Further, within this analysis, only 13 journals featured two or more high-impact articles. While there are valid arguments against using journals as a sole measure of research quality (see Seglen, 1997), they do serve as platforms for collaboration, reviewing and the dissemination of consistent and innovative research on specific topics. Consequently, journals gradually gain recognition as reputable outlets for interested researchers to publish their work, acting as a crucial point of contribution towards a specific field, thus fostering the domain's scientific cohesion and collaboration. However, the presence of a set of journals with consistent output of cyberterrorism and hacktivism research would be welcomed as "key" sources of highly relevant and topical research. The significantly limited number of sampled high-impact publications associated with journals identified within this study would suggest no such "key journals" are yet available, with such a journal potentially seeing significant interest.

The observation that, despite reviewing a substantial number of articles, only a small portion originates from the same journals, raises the question of why there isn't a concentrated collection of high-impact articles within a specific set of journals. Instead, these articles appear dispersed across various individual journals. This dispersion prompts inquiry into the factors contributing to the absence of a centralised body of literature

within a specific journal or group of journals, despite the existence of numerous impactful articles.

In a study concerning the coalition between high degrees of disciplinary fragmentation and limited scientific progress, Balietti, Mäs, and Helbing (2015) proposed three potential questions to explore the issues, that: (i) progress might decrease fragmentation, (ii) fragmentation might limit progress and, (iii) there might be other variables that affect both outcomes, thus, creating a spurious correlation between them (Balietti, Mäs, and Helbing, 2015). Interestingly, they found that limited progress does not lead to fragmentation, but fragmentation hampers progress (Balietti, Mäs, and Helbing, 2015:20). These findings coincide with Kuhn's earlier argument that scientific paradigms and their subscribed scientific communities are limited to progressing their cumulative intellectual knowledge within a robust internal consensus; identifying problems, techniques, and solutions valid within their bespoke paradigms, while often excluding those not adhering to the current framework (Balietti, Mäs, and Helbing, 2015; Marx and Bornmann, 2010:442).

As such, scientific communities of a particular paradigm can exist without any notable fragmentation, and even become more productive. This was identified by Silke (2001), when studying literature produced between 1995 to 2000, of which he found that over 80% of publications were largely literature reviews, with Dolnik (2011:5) later arguing that this lack of empirical research promoted a closed circular research system, operating as a feedback loop of self-citations, and internal validation of unsupported myths, of which ultimately serve as a foundation of knowledge until, as Kuhn (1970; 1977) suggests, a scientific crisis prompts the emergence of a new paradigm. Similar observation

by Reid (1993:28) argued that these closed systems are indicative of a static environment, resulting in authors often recycling the same hypothesis, definitions, and theories.

6.2.2 Knowledge Dispersion and Consistency

This conceptual recycling has been seen to emerge from cyberterrorism and hacktivism research with the frequent citing of Denning's (2000a) publication, which is cited within 37 of the 126 high-impact articles analysed and continues to see frequent and ample citation and definition quotation since its original publication (see Figure 5.13 Denning (2000a) citation distribution over time:219). In defence of these closed systems, Garvey, and Griffith (1979:29) considers them as part of the communication of science, arguing that such publications are designed to be used by scientists to produce more academic knowledge. This ideal circumstance, however, relies on a steady stream of research that pushes the domain forward with new findings and discussions (Dolnik, 2011). A similar circular system of knowledge can be seen within organisational science. Hirsch and Levin (1999) proposed that research has a "life cycle". Initially, the excitement of emerging topics and paradigms ignites a flurry of good "ideas" later research efforts become opaque and broad. This "idea" may become viewed as an "umbrella construct" (Hirsch and Levin, 1999), leading researchers to purposely separate these ideas into specialised subsets. These subsequent and specialised research endeavours, as mentioned by Gray and Meister (2003:259), tends to highlight distinctions among facets of the central concept or 'idea', rather than emphasising their shared features. With both arguing that in the absence of common ground and consensus, researchers follow divergent paths, undermining the

original concept and transforming the concept into a multitude of smaller, distinct ones that do not overlap (Gray and Meister, 2003), thus becoming fragmented.

The lack of a cohesive journal output (i.e. articles spread across multiple journals, lack of co-authorship) within cyberterrorism and hacktivism research as identified (see Figure 5.3 Journal Distribution:201), makes this cohesion difficult, instead researchers must rely on artificial collaboration often by means of informal research networks in which to glean knowledge from. Reliance on informal networks is not without risk. For example, the co-citation analysis conducted in this study (see Figure 5.16 Co-citation of Article Sources:219), revealed a substantial network of 4,586 individual authors cited amongst the 126 high-impact publications. When focusing on authors who received 10 or more citations within the network, only 26 authors (0.57% of the total) remained. This significant reduction in the number of authors highlights two crucial factors.

Firstly, it indicates that the literature analysed within the collected publications shows a significant dispersion of intellectual cohesion, with authors cited from an array of multi-disciplines providing an interdisciplinary perspective. The impact of such is difficult to assess. For example, Morrison, in a recent thematic analysis of interviews with pre/post 9-11 terrorism researchers, found that interdisciplinary input is mostly seen within a positive light in terrorism studies (Morrison, 2022:1511), with Youngman (2020) promoting their inclusions as to encourage cross-fertilisation of knowledge and historical awareness. Hegghammer (2013) on the other hand, earlier claimed its inclusion weakens

opportunities for terrorism researchers in an already competitive environment, thus potentially slowing scientific progress (in Morrison, 2022).

The high number of individual authors cited, and sparse number of authors having received 10 or more citations within the sample of 126 articles analysed raises further concerns about the potential challenges towards intellectual cohesion amongst researchers engaging in cyberterrorism and hacktivism research. As Rawlings et al., (2015:1690) note; intellectual cohesions pertain to secondary groups of which shared (or in this case; cited) knowledge and concepts are a basis of cohesion, and that such cohesion relies on the capacity to absorb specialised knowledge and developments. Thus, the presence of such findings would suggest potential issues related to collaborative agreement, coordination, or recognition of key concepts within the research community studying cyberterrorism and hacktivism, impacting its intellectual cohesion. Challenges in research collaboration have significant implications for further research. For example, González-Alcaide et al., (2013) identified that when analysing the collaborative productivity of criminologists, the increased number of collaborative works and multi-authorship publications often leads to the formation of prominent research groups within the field.

Secondly, the high number of *single-author/single-publication* high-impact articles within the collection raises concerns about the potential dissemination challenges of multi-publication outputs from any single or group of researchers. The majority (90|71.4%) of publications collected in the study were found to be single-author publications. While it is reasonable to assume that single-author contributors are aware of

the importance of collaborative research, given the various benefits associated with collaborative projects such as increased access to public funding, enhanced visibility, inclusion of well-established groups, and higher productivity (Lee and Bozeman, 2005; Hurley et al., 2013), the reasons for the limited collaborative efforts remain unclear. Further, the limited output of high-impact multi-publication authors raises questions about the underlying factors contributing to the lack of dissemination and awareness of these publications within the domain.

Silke (2001) argues, specifically in the context of pre-9/11 terrorism research, and more recently discussed in Hosford et al., (2021) that; when discussing organised crime research, one of the barriers limiting research collaboration was the limited number of researchers working in the field. Additionally, Silke (2001) highlighted that the existing workloads of researchers may not support the undertaking of complex and collaborative research ventures, suggesting that practical constraints and resource limitations within the research community may impede the formation of collaborative networks. Becher and Trowler (2001) similarly argued that academic departments, associated workloads, and complex university research structures contributed towards intellectual fragmentation discouraging broader interactions (in Rawlings et al., 2015:1688), or similarly, restricting the available time for researchers to effectively identify the broader research available, often instead relying on trusted journals and a familiar cohort of researchers.

Further critical perspective on the issue concerning criminological research comes from Hudson (2008:288), who posits that criminologists have established a figurative “walled

garden" that may inadvertently exclude individuals as what Hudson defines as "others." That is, those who do not align with preconceived inclusions, or are not familiar to the established cohort of researchers. Paradoxically, this perceived homogeneity among criminologists leads to the inclusion of certain "others" based on exaggerated differences, thereby exacerbating the fragmentation of specialised research areas (Hudson, 2008). This introspective analysis suggests that disciplinary boundaries such as those earlier discussed by Kuhn (1970) in discussion of scientific allegiance to paradigms, and normative 'safe' practices within criminology may hinder interdisciplinary collaboration and impede the formation of diverse research partnerships.

Both perspectives, although having a potential application to aid towards understanding the lack of consistent or collaborative high-impact output within cyberterrorism and hacktivism research, are difficult to identify with the available data. Knowledge on the citation behaviours of criminology researchers is scarce, and evaluating what can be considered 'collaboration' can also be difficult, subject to social conventions on where less formal links end and collaboration begins (see Katz and Martin, 1997:16). For example, if we were to take Jassawalla and Sashittal (1998:239) definition of collaboration as: "the coming together of diverse interests and people to achieve a common purpose via interactions, information sharing, and coordination of activities", than the issue of fragmentation towards collaborative and cohesive knowledge can be seen amongst authors of high-impact articles of cyberterrorism and hacktivism, and not so much an issue of potential stagnation.

Katz and Martin (1997) note that research collaboration enhances the quality of work and leads papers with more authors to be cited more, however. Although Fahmy and Young (2017) recognise co-authorship as the predominant form of scholarly collaboration in criminology, in the domain of cyberterrorism and hacktivism research, the bibliometric findings of author collaboration (see section 7.2.1 Basic Analysis: 217), found a total of 36 (28.6%) publications of the 126 high-impact articles were associated with two or more authors, significantly under-performing when compared to Wagner-Doebler's (2001) claim that over 50% of scientific publications are co-authored on average. Further, scientific research collaborations often extend beyond the cooperation among scientists and encompass partnerships between diverse organisations, with a growing emphasis on cross-border collaboration among countries (Katz and Martin 1997), thus when engaging research in such a transnationally connected phenomena such as cyberterrorism and hacktivism, such cross-border collaboration would be desired for representation, however. Amongst the 36 high-impact articles with multi-author collaboration, none showed collaboration with authors outside of national boundaries. Equally disheartening, a sizable proportion (97.3%) of the 126 publications were primarily affiliated with institutions in the Global North, particularly the United States (82) and the United Kingdom (33), accounting for 62.2% of the analysed publications showing a significant lack of international diversity amongst high-impact articles.

This limited diversity is extended when the distribution of gender was observed within high-impact articles. Findings from the analysis identified that researchers of high-impact articles in the field of cyberterrorism and hacktivism research consisted of 78.8% male

researchers (132), 27.2% female researchers (54), and no representation from non-traditional gender identities (see section 7.2.1 Basic Analysis: 2172). This gender disparity raises important questions about inclusivity and diverse perspectives within the field, as diverse perspectives and experiences are crucial for fostering innovative research and generating comprehensive insights. Stockdale and Sweeney (2022) suggest, the colonial nature of criminology has largely remained observed within a white, male, cis-gendered lens, alongside a rigid and focused spotlight on issues limited to the interests of the global north, an issue which has seen frequent discussion (Agozino and Pfohl, 2003; Blagg & Anthony, 2019; Carrington et al., 2018). For such transnational interconnected concepts such as cyberterrorism and hacktivism to be defined and discussed with such rigid confines, risks a loss of diverse and dynamic discourse, and research a more representative cohort of researchers could provide.

As noted earlier, a dearth of cohesive formal outputs such as journals that encourage collaboration and more importantly cohesion can lead researchers to rely on artificial collaboration often through citation practices. From the perspective of the observer, informal communities of cited researchers may if briefly observed, and appear as a form of “invisible college”, of which pertains to the informal diffusion of knowledge between researchers with existing relationships, a concept discussed at length (see Crane, 1977; de Solla Price and Beaver, 1966; Tarrant et al., 2018; Zuccala, 2006).

The existence of such informal structures amongst cyberterrorism and hacktivism researchers as earlier findings identified (see Figure 5.18 Co-citation of Cited Authors

with a minimum of 10 appearances:237), does not support the existence of such relationships as the infrequency of high-impact publications, the general disconnects between journal consistency, the high number of single author publications within individual journals, and limited collaboration would suggest otherwise. As Reid (1993:17–18) notes in concerns to an 'invisible college' of terrorism studies, these networks of researchers establish agendas, recruit new members, secure funding, sponsor conferences, and maintain informal contacts that nurture the development of the research area. Within cyberterrorism and hacktivism research, no such agendas, funding, or conferences appear to exist, let alone any notably dedicated journal in which to pursue for publication or nurture development. Therefore, if such an invisible college does exist within the domain, they are not as productive or as collaborative as the concept would suggest.

6.3 Identifying Distinctions Using Taxonomic Mapping of Cyberterrorism and Hacktivism Definitions:

Conceptual understandings of cyberterrorism and hacktivism have evolved throughout time alongside the rapid developments of ICT. Since Dorrothy Dennings (2000a) seminal piece on activism, hacktivism and cyberterrorism, a large body of literature has emerged, all providing multiple perspectives aimed at defining these emerging phenomena in an increasingly cyber-connected world. There have been consistent debates concerning the degree to which 'cyber' and 'terror' play within cyberterrorism (Brenner, 2006; Gordon and Ford, 2002; Weimann, 2005; 2011). These debates are often discussed alongside concerns regarding how hacktivism operates in the space between digital activism (see Asenbaum, 2018; Solomon, 2017), and illegal hacking (Broucek and Turner, 2013; Ruth and Stone, 2012). These debates, however, often discuss both phenomena along equal lines (Baldi, Gelbstein, and Kurbalija, 2003; Kenney, 2015; Yar, 2013; Yar and Steinmetz, 2017; 2019), making little effort towards discerning the two, inadvertently blurring both concepts, if not defining such as identical phenomena. This inadvertent blurring of concepts has significant impacts towards further research endeavours. As noted by Merton (1968:114), a significant portion of the work known as "theorising" is dedicated to clarifying *concepts*, of which DiRenzo (1966) describes as indispensable tools in the process of scientific explanation, emphasising that "precision in this fundamental area is imperative for the production of significant theory" (1966:3). Thus, this inadvertent blurring of both concepts makes conceptual precision of either cyberterrorism or hacktivism challenging, of which Gerring (2012) argues; hampers

social science endeavours, as without the ability to label a topic (be it cyberterrorism, or hacktivism), it becomes difficult to address even the more basic of research questions; "what are we even talking about?" (Gerring, 2012:112).

This thesis engaged with the literature and conducted a quantitative content analysis of academic definitions pertaining to both cyberterrorism and hacktivism to identify key themes and distinctions between both phenomena. This study also evaluated said definitions to understand the similarities and differences between both phenomena. The findings demonstrate that both hacktivism and cyberterrorism share common traits, that they are ideologically motivated behaviours involving or supporting social action, with the use of 'cyber' technologies as the predominant feature. Thus, this discussion is not simply to provide a list of 'traits' associated with either phenomenon, but to compare identified nuances as to evaluate the current state of cyberterrorism and hacktivism knowledge, and the academic behaviour of authors in how they defined both phenomena throughout a twenty-year period (2000-2020).

To continue, this portion of the discussion will employ the taxonomic framework outlined in (see 5.3.3 Synthesising the Taxonomy) to categorise and discuss the research findings. These six sections, namely: actor, effect, intent, means, motive, and target, will delve into the definition and classification of each aspect. The analysis will focus on identifying and discussing noteworthy findings and key concerns within these portrayals.

6.3.1 Lack of Actor Specificity

This section evaluates how actors of cyberterrorism and hacktivism are often defined in the academic literature. Notably, throughout the analysis of terms associated with the actor classification of cyberterrorism, these definitions often lacked clarity and specificity towards those labelled *"cyberterrorists*." As earlier findings illustrated (see Figure 5.25 Total Frequency Distribution of Coded Actor Terms:265), researchers made frequent use of conventional terms such as terrorists, sub-national groups, clandestine agents, and, unsurprisingly, cyberterrorists themselves. However, these descriptions were often limited in explanatory details making little comparison to any notable or distinct case studies or events. For those in terrorism studies, this is an unsurprising finding. The field itself makes considerable references towards the use of the term "terrorist" as a political instrument of delegitimization (Chagankerian, 2013), and justification for legitimising the use of more invasive security policy measures (Baele et al., 2019).

In the scope of this thesis, categorising individuals engaged in disruptive hacking or cyberattacks as either cyberterrorists or hacktivists carries consequences for how these actors are perceived, the concerns they evoke, including the extent of counterterrorism and cybersecurity measures applied (Shandler et al., 2023; Snider et al., 2021). In their study on the influence of cyber-threats and cybersecurity policies, Snider et al., concluded that public willingness to accept government cybersecurity policies, and potential reductions in civil liberties and privacy depends largely on the type of cyberattack in which citizens are exposed to (Snider et al., 2021:9), and how such an act is portrayed. Further, Shandler, Kostyuk, and Oppenheimer, (2023) concluded that the public are often

unwilling to label such attacks as an act of cyberterrorism when the actors are unknown, making such policies difficult to enact. This raises concerns when discussing the concept and portrayal of hacktivism, of which throughout this thesis was often discussed as being concerned with the protection of civil liberties, against digital censorship, and promotion of unrestricted access to informations (see Jordan, 2002; 2007; Karagiannopoulos, 2018b; Krapp, 2005; Samuel, 2004). If acts of hacktivism were to be perceived or portrayed as potential and dangerous threats, akin to depictions of cyberterrorism, then the acts of hacktivism themselves would be counterintuitive to their most prominent causes.

In contrast to this contextual description of cyberterrorism actors, researchers were seen to more consistently associate hacktivism actors with specific groups such as Strano Network (Denning, 2000a), LulzSec (Goode, 2015; Kelly, 2012), and Anonymous (Goode, 2015; Hai-Jew, 2015; Klein, 2015; Machado, 2015; Stamm, 2015) linking hacktivism actors within cyber-physical systems. Tan et al. (2009), defines these cyber-physical systems as a combination of attributes associated with an event's temporal, and spatial information, or to simplify; the space and time of an event. Thus, in associating hacktivism with specific groups, researchers inherently tie the events associated with these groups to acts of hacktivism, providing a historic benchmark in which to position future comparisons. Notably, since 2015, discussions of individual hacktivist groups have also seen a significant increase (see Figure 5.26 Actor Code Distribution by Year & Frequency:266), coinciding with the rise and widespread adoption of online social networking platforms acting as “deviant hacker networks” (Al-khateeb et al., 2016)

allowing “actors” the opportunity to publicly acknowledge their actions, whether criminal or not, in pursuit of their intended goals.

Returning to the lack of specificity regarding cyberterrorism actors within academic definitions, the inability to attribute actions to identified groups, or individuals can be linked to early disagreements among cyberterrorism researchers regarding the feasibility of such acts (see Conway, 1998; Baker and McKenzie, 2001; Embar-Seddon, 2002; Gordon and Ford, 2002; Berner, 2003; Emery, 2005). Earlier interpretations and discussions frequently portrayed cyberterrorism as the use of cyber technologies for terrorism, often describing methods that are now considered highly technical and unrealistic for conducting acts of violence (Denning, 2001; Desouza and Hensgen, 2003; Foltz, 2004). These discussions often lacked considerations for the practicality of such acts or acknowledgment of existing systems to mitigate them, a perspective emphasised in Pollitt's early conceptualizations of cyberterrorism (1998:10). Some expressions of concern were akin to portrayals of a “*cyber-doomsday*” scenario (Gross et al., 2016; 2017; Henschke, 2021; Henschke et al., 2021).

One could argue that heightened concerns about terrorism, particularly after the events of 9/11 (Onat et al., 2022), led to increased public fear and media scrutiny regarding the potential use of the internet for terrorist activities. This heightened attention compelled researchers to explore and explain this emerging phenomenon. Consequently, earlier literature on cyberterrorism and hacktivism often reflected uncertainty about the evolution of information and communication technology and related services, as well as society's

responses to these developments, a common theme seen in criminology in general, often called upon as a state funded apparatuses following a notable event (Lynch et al., 2020:6). In a time of increased fear and confusion, researchers grappling with an obscure threat that appeared to be anonymous had to rely on educated opinions to comprehend how this technology could be harnessed for terrorist and activist endeavours. However, many of these opinions, as outlined by Conway (2014a; 2014b), did not materialise. As noted by Gentner and Collins (1981), researchers frequently encounter situations where they must engage in reasoning based on incomplete knowledge, necessitating decisions to be made in the absence of all relevant facts. For example, when discussing crime prevention, Tilley and Laycock argued that findings from social science research is seldom unequivocal, often followed by debate concerning the methodologies adopted, and specificity of findings presented (Tilley and Laycock, 2018:233), thus often unable to fully address pressing issues, with both later commenting that in the arrival of cybercrime is likely to be more effectively addressed by those in the IT industry, rather than those in public service such as police (Tilley and Laycock, 2018:239).

This process of reasoning, seen within cyberterrorism research contributed to the prevailing sense of "cyberangst", as seen with seminal depictions of catastrophic cyber-attacks (Collin, 1998; Collin 2000; Denning, 2000a), and reinforced by media depictions (Weimann, 2005:132), only further exacerbated the expanding understanding, and somewhat glamorization of illicit hacking and society's growing dependence on information and communication technologies (Bastug et al., 2023), making further attempts to identify or perceive any potential actors more difficult, as the standards of

what a cyberterrorist, or even hacktivism "should be" have been potentially set to unrealistic standards.

6.3.2 Violence versus Non-Violence

Focusing on how researchers defined the events of cyberterrorism and hacktivism several notable nuances emerged. References to numerous extreme scenarios often linked to substantial harm and physical violence towards civilian populations were frequently included in definitions of cyberterrorism (Denning, 2000a; Weimann, 2005; Stohl, 2006). These definitions tended to favour the use of physically aggressive terminology, as indicated by research findings (see Figure 5.29 Total Frequency Distribution of Coded Effect Terms:271). Terms such as "violence," "attack," "destruction," and "physical injury" were linked to cyberterrorism definitions, drawing notable parallels to the perception of this phenomenon as a cyber-enabled extension of unconventional descriptions of terrorism (Jangada Correia, 2022). These terms remained persistent throughout the entire 20-year temporal scope of the study (see Figure 5.30 Effect Code Distribution by Year & Frequency:273). Interestingly, terms concerning the effects of hacktivism did not truly emerge until later in 2004, and were more tied to activist-based pursuits, such as undermining of government, and non-violent actions such as data-breach and various forms of disruption (Edyvane and Kulenovic, 2017). This lack of aggressive terminology is consistent with earlier discussions of hacktivism, and its strong alignment as a politically motivated act of hacking (Fowler, 2016; Gardner, 2014; Wright, 2008) that exercises in civil disobedience (Denning, 2000b:263). This is reflective of the limited

range of terms associated with hacktivism that projects a unidimensional view of hacktivism, where behaviours traditionally associated with activism are transposed into a cyber domain.

For example, when observing the effects of hacktivism from a raw-coded distribution (see Figure 5.31 Network Distribution of Extracted Effect Terms:275), The phenomenon is largely disruptive based within virtual environments, such as Electronic Disturbance Theatre's use of DDoS software to cause and further encourage the disruption of government websites (Deseriis, 2017; Mehrabov, 2016; Taylor, 2005), or further similar acts of nonviolent civil disobedience (Edyvane and Kulenovic, 2017). This contrasts earlier academic comparisons in which hacktivism was more closely paired with cyberterrorism (Andress and Winterfeld, 2014; Fowler, 2016; Gardner, 2014). Further, as noted earlier, hacktivism as a phenomenon is frequently associated with events linked to cyber-physical systems. As such many groups - such as Strano-Network, LulzSec and Anonymous - often engaged in non-violent operations of mass disruption and misinformation campaigns against perceived government or corporate exploitation[13]

In comparison, raw and coded terms associated with the effects of cyberterrorism echo earlier fears and associations of the phenomenon as an extension of more common understandings of terrorism (Jangada Correia, 2022). The large variety of term usage seen within the 'effects' classification is reminiscent of Wall's (2008) earlier tellings of myths, with further fears being added throughout time as newer avenues of technology and

[13] See Molly Sauters blog for archival essays of hacktivist use of disruption. Available at: http://oddletters.com/

potentials of exploitation emerge. However, unlike Hodgson and Tadros (2013) argument that defining characteristics of terrorism can be subject to the observations of those who witness such events, similar scepticism shared by George Fletcher (2006) and Jeremy Waldron (2004) regarding the necessity of investing time in grappling the definitional issues of terrorism, instead adopting a perspective to that of Justice Stewart's famous remark about pornography; “you’ll know it when you see it” (Fletcher 2006:2; Waldron 2004:6). Within the context of cyberterrorism, these “events” are often difficult to observe in virtual environments or have yet to occur. This depends on how such acts are defined (Conway, 2018:7), and given cyberterrorism and its definitional history, often in juxtaposition alongside terrorism, it may never truly be defined, as conceptual disagreements towards the involvement of cyber and terrorism, and when something goes from terrorism to cyberterrorism, vice versa, or is completely distinct from terrorism still remains unclear.

6.3.3 Conflicting Intentions and Spectacle

When examining the concept of “intent” in the context of cyberterrorism, referring specifically to the objectives pursued by the actors involved (Veerasamy et al., 2012), two prominent coded terms overshadow others: ‘intimidation’ and ‘coercion’, alongside more expected terms such as “terrorise” and cause “disruption” (see Figure 5.33 Total Frequency Distribution of Coded Intent Terms:278). The prevalence of these terms suggests a focus on achieving a certain level of control, which in turn requires the presence

of a public persona for effective impact at a societal level. For example, Hughes (2016) cites political scientist Gene Sharp's definition of intimidation as:

"The use of sanctions, or the threat to use sanctions, to induce others to take, or not to take, certain actions because of their fear of the likely consequences if they do not comply" (Hughes, 2016:5).

Hughes references the IRA's use of nonviolent sanctions (strikes, boycotts, political non-cooperation) to coerce and punish individual defiance towards compliance (Hughes, 2016:5). Findings from the analysis of cyberterrorism definitions, although giving significant reference towards intimidation, and in many parts alongside coercion, seldom provide context of such intentions. For example, Holt simply refers to the threat of an attack intended to interfere with the political, social, or economic functioning of a group organisation or country (Holt, 2012:340-341; also, Foltz, 2004). These threats of intimidation and coercion often suggest the presence of power-disparatie, of which Presbey in discussing power, consent, and coercion notes that such power is not the property of the 'actor' or any one group, but rather a relationship between actors (Presbey, 1992:2). As such, intentions, such as intimidation and coercion, function as an evaluation of the asymmetry between legitimacy and power.

Within definitions of cyberterrorism, the lack of associated actors or groups makes discerning the "legitimacy" or justifications of acts that would be considered cyberterrorism difficult. The "*act"* of terror operates as a form of communication whereby

the recipients of said terror are unwillingly made conduits for the communiqué of the terrorist actors (Argomaniz and Lynch, 2018:492). Thus, if we are to consider cyberterrorism as a "new" form of terrorism (alias pure cyberterrorism), or alternatively an extension to terrorism (cyber-enabled terrorism) it would warrant knowing who these "cyberterrorists" are, and their intentions. The academic research remains constrained by the tendency to rely on sensationalist portrayals of cyberterrorist attacks on critical infrastructure reminiscent of the "Die Hard" style narratives. These depictions often involve rogue and anonymous groups, which, as Conway (2014a:13) argues, may not align with the motivations often seen with terrorists. Cowen (2006) contends that terrorist groups place considerable effort towards the "spectacle" or, more commonly, the propagation of favourable propaganda which often accompanies acts of terrorism, serving to enhance the legitimacy of the actors involved, something missing from cyberterrorism research.

In comparison, hacktivism tends to have more, though still limited, mention of key motives such as "privacy," "open access," "exposure," and "raising awareness." These motives closely align with earlier discussions among hackers that emphasised the importance of free and open access to information (Jordan and Taylor, 2004:10-12). Additionally, they reflect activism against anti-globalization sentiments, which has steadily grown over the 20 years of analysis (Coleman, 2012; Jordan, 2001). Similar to observed intentions in cyberterrorism, these motives in hacktivism also require legitimation for their efforts to be considered effective, such as the case with what George and Leidner (2019) earlier described as "patriotic hacking" by non-state-sponsored

hackers using patriotism as a means of legitimising their actions (Lokot, 2017), often by bringing attention to their acts and capabilities to establish prestige and legitimacy in their actions (Seebruck, 2015).

Given the typically decentralised structure of hacktivist groups, exemplified by entities like Anonymous (refer to Deseriis, 2017; Jordan, 2017; Stamm, 2015), the flexible and decentralised nature of participation in hacktivism often involves individuals with diverse ideologies coming together for a shared cause or objective. This cause gains advantages by directing focus and awareness towards the collective actions of these groups. This shift often supplants the localised political solidarity and sensitization commonly observed in offline activist groups, which is frequently considered a defining feature of such groups (Jansen, 2011:83).

6.3.4 The Means and Practicality of Cyberterrorism and Hacktivism

As the publications analysed consistently depicted catastrophic scenarios involving the disruption of critical infrastructure, it is crucial to assess the feasibility and practicality of both cyberterrorism and hacktivism. Within the taxonomy framework, the means employed by actors engaging in hacktivism or cyberterrorism were identified and coded. This means classification, as outlined by Veerasamy (2009), focuses on how actors achieve their desired outcomes. The means classification closely relates to the earlier

discussed effect classification, and it is not uncommon to find overlapping terms between the two.

In the analysis of cyberterrorism and hacktivism definitions, most identified and coded terms were associated with both virtual means (e.g., cyber weapons, coding, malware) and behavioural means (psychological, influence). For example, when discussing virtual means for enacting hacktivism, Krapp's definition points to programming skills (coding) for achieving human rights/free speech, as well to conduct malicious and destructive acts (Krapp, 2005:73). Due to the analogous operations of cyber-technology, the means alone is insufficient to determine intent, motive, or target selection. This can be seen with both definitions and adoption of terms coded within ICT, and its dominance through the 20-year temporal period of this study (see Figure 5.36 Yearly Distribution of Means Classification:285). Since ICT is merely the adoption of network technologies as a means, the term itself cannot be used to refer to either cyberterrorism or hacktivism, nor can it be representative of intentional malevolence or lack thereof such as the case of earlier depictions of cyberterrorism (Collin, 1997; Brenner, 2006). For example, "malware," another means shared between both phenomena is a portmanteau of malicious software, used as an umbrella term to describe any programme or file that is designed to intentionally disrupt normal computer operations (King et al., 2018:6) The adoption of malware itself is not directly inherent towards any 'malicious' intent (Rieck et al., 2008).

Additional instances of using an overarching term can be observed in the adoption of the term "hacking," which is used in both phenomena definitions. However, it's noteworthy

that hacktivism, with a count of 29, significantly surpasses cyberterrorism, which amounted to a count of 3 in this study (see Figure 5.37 Total Frequency Distribution of Coded Means Terms:283). Commonly, hacking has been "equated towards illicit, illegal or unwanted computer intrusions" (Jordan and Taylor, 2004:5), with argument suggesting that an inability to converge on a consensus of "hacking" has permitted free rein for governments, law enforcement, media, and information security specialists to establish a criminogenic status of hacking (Yar and Steinmetz, 2019). A brief look at the earlier techno-centric history of the term 'hacking' provides memoirs of innovation, pioneering, and strongly anti-capitalist ideologies in support of a free and open information society (Clough and Mungo, 1992; Jordan and Taylor, 2004; Levy, 2010; Wall, 2008), aligning closely to earlier discussion on the intentions of hacktivists, potentially suggesting that researchers discussing hacktivism share an awareness of hackings more socially-active origins.

Reflecting on the practicalities of cyberterrorism by its means, Conway (2011b) criticised the phenomena, arguing that the technological complexities of potential events of hacking national infrastructure, aeroplanes, etc. are outside the means and training of many terrorist groups, and that outsourcing such tasks would only introduce further risks for the organisation (Conway, 2011b:27-28), instead arguing that at current, cyberterrorism is impractical, with Gambetta and Hertog (2007) further echoing terrorists groups lack effective skills in advanced cyber-technologies. This criticism, although potentially valid if those considered engaging in cyberterrorism are relegated to more known extremist and violently active groups, with some outright arguing such phenomena is no more than a myth (Emery, 2005), is seldom shared by other authors reviewed in this study. The divide

in which researchers view cyberterrorism as a means, of which Jones (2005) acknowledges as either a possibility or outright denying its likelihood as much of the insight in cyberterrorism's likelihood is absent of any evidence. While the majority, if not all, terrorist attacks traditionally take place in physical spaces rather than exclusively through cyber channels, recent research indicates a growing trend in the adoption of cyber-based methods. However, the bespoke techniques employed by extremist and ideologically motivated actors, subjects commonly discussed in the context of cyberterrorism if any, remain unknown (Holt et al., 2020:528).

6.3.5 The role of Ideology and Motivation in Cyberterrorism and Hacktivism Research

To begin, it is important to acknowledge that ideology alone is often insufficient to fully explain the motivations behind an individual or group's engagement in activities such as terrorism (Cowen, 2006:237; Morrison, 2016:48) with Morrison (2016) citing Taylor and Horgan, in that regardless of ideology, politics, or social processes, participating in terrorist behaviour fundamentally requires an individual to possess and seize an opportunity for engaging in such behaviour (Taylor & Horgan, 2006). This concept of ideology alone is not a sufficient means of explaining an act of terrorism is further explored by Holbrook and Horgan (2019), who argue that ideology is fluid, and can be part of shaping a much wider complex process towards engaging in an act of violence (Horgan, 2019:3).

When distinguishing cyberterrorism and hacktivism from other manifestations of deviant cyber activities (i.e. cyberstalking, scamming, online sexual exploitation) it was common for researchers to emphasise the significant role played by ideologies as a primary motive or "call to arms" for these actions. Definitions of cyberterrorism and hacktivism were frequently associated with motivations rooted in politics, society, and religion (see Figure 5.41 Total Frequency Distribution of Coded Motive Terms:289), with both phenomena seeing an increase of attention from researchers concerning the role of ideology as motivation throughout the later years of the collected literature, most notably from 2007 onwards (see Figure 5.40 Yearly Distribution of Motive Classification:288).

The most significant coded term identified within the analysis for both cyberterrorism and hacktivism was "Political" as a key motivation, and as identified earlier (see Figure 5.42 Motive Code Distribution by Year & Frequency: 290), has seen significant inclusion throughout the body of high-impact articles timeline of 20 years, with a recent case-study corroborating this (see Farmer, 2022). For example, adopting Romagna and Leukfeldt's (2023:5) definition of hacktivism as promoting socio-political agendas in cyberspace, Farmer (2022) identified 66.7% of operations conducted by hacktivist groups as being politically motivated. Although Farmer's analysis and inclusion of case-studies is broad, including an array of digital activisms (see George and Leidner, 2019), and focusing largely on sentiment analysis in order to infer findings, this study is indicative of the forward facing, and politically active approach often seen by groups associated with hacktivism, and given reference by key researchers.

When attempting to evaluate the prominence of the term 'political' within definitions of cyberterrorism, several challenges persisted. Notably, it was often used as a passive term used with little further context provided beyond association with earlier terrorism research. For example, Hua and Bapna identified cyberterrorism as adopting cyber with intentions to disrupt political functions, motivated by traditional terrorism ideologies (Hua and Bapna, 2012:104). Foltz acknowledges cyberterrorism as having similar political motivations as those often seen associated with terrorist groups and described political (social and economic) interference as qualifying criteria (Foltz, 2004:156). The trend of associating cyberterrorism alongside similar motivations seen within earlier terrorism research is not surprising given the domain of the phenomenon, encouraged by the scarcity of empirical case-studies.

There have been few efforts to evaluate the motivations for cyberterrorism. Adopting and modifying an earlier framework to the one adopted in this thesis, Yunos et al. was only able to recognise motivations for cyberterrorism to be strongly linked to its 'intent' and are often described interchangeably (Yunos et al., 2015:7). Veerasamy's publication "*Motivation for Cyberterrorism*" is similarly limited, providing a summary of terrorist groups and their adoption of ICT for various activities such as dissemination of radical propaganda and website defacement, and echoing earlier commentary concerning terrorism as a theatrical performance motivated by gaining attention (Veerasamy, 2010:4).

A more recent, yet broader study by Holt and colleagues (2019) attempted to remove the necessity of deciding between an act being cyberterrorism or hacktivism when exploring

the ideological motivations of the Far Left. They cite Majid Yar's (2013) argument that, without case-studies or empirical data, cyberterrorism could simply be a projection by homeland security and anti-terrorism apparatuses to gain more funding and stoke public fears (Yar, 2013; Holt et al., 2019:2). In their study, Holt and colleagues identified through the analysis of 26 case-studies, those with ideological alignment to Far-Left(isms) were mainly focused on raising attention of their targets perceived injustices and societal wrongs, aligning closely to discussions similarly seen associated with definitions of hacktivism (see Alexopoulou and Pavli, 2019; Sovacool et al., 2019; Stoehrel and Lindgren, 2014; Travaglino, 2019), further reinforcing similar discussion of terrorism relationship with ideology (Holbrook and Horgan, 2019; Morrison, 2016, Taylor and Horgan, 2006) being participatory and fluid and not in itself able to fully explain why a person would pursue engaging in an act of cyberterrorism, or hacktivism.

6.3.6 Targets and Security Narratives of Cyberterrorism and Hacktivism Research

Within this study, the target classification emerged as the most prominent among the six classifications, with the quantitative content analysis contributing a total of 308 raw uncoded terms. This classification pertains to the intended recipient of the actor's effect (Veerasamy et al., 2012). The results of the analysis of 'target' terms focused primarily within the domain of cyberterrorism, with only recent attention being directed towards defined targets within the domain of hacktivism and associated definitions from 2015 onwards (see Figure 5.46 Target Code Distribution by Year & Frequency:297).

It is noteworthy that literature on cyberterrorism analysed within this thesis often adopts an inclusive perspective when examining potential targets. Notably, as the earlier analysis highlighted (see Figure 5.47 Network Distribution of Extracted Target Terms:299), numerous raw terms extracted from cyberterrorism definitions are associated with critical infrastructure, for example airports, water and power plants (Hansen et al., 2007; Jarvis et al., 2014; Hua et al., 2018), data systems (Denning, 2000a; Foltz, 2004), non-combatants (Cassim, 2012; Boys, 2018), and property (Yunos et al., 2015; Ayres and Maglaras, 2016). Nevertheless, the in-depth exploration and elucidation of these identified terms within the reviewed publications, particularly regarding the actual and measurable risks posed by cyberterrorism to the targets or the realities and probabilities of such scenarios, remain limited (Conway, 2014a; 2014b). Thus, considerable room for interpretation persists.

Eroukhmanoff (2017) asserts that the consideration of potential targets plays a vital role in the defence and mitigation of hacktivism and cyberterrorism. Moreover, a definition of either cyberterrorism or hacktivism can be conceived as a "speech act" wherein words not only describe reality but also shape it, thereby triggering specific responses (Eroukhmanoff, 2017:106; see Buzan, 2004).

Hansen and Nissenbaum (2009) note that early cybersecurity scholarship, often unfamiliar with a rapidly expanding cyber environment, tended to exaggerate the risks associated with cyber, in turn contributing to security measures beyond what would be considered "normal". Much has been written on the use of ICT to facilitate events of fear and violence by the media and policy makers (Conway. 2005; 2008a; Stohl, 2007; Lawson, 2013; Lawson et al., 2016; Weimann, 2005).

As Lawson et al., (2016) discusses concerns that such "scenarios" could encourage propositions towards excessive countermeasures being necessary to effectively protect potential targets against exaggerated threats, with Cavelty and Van Der Vlugt (2015) noting a tendency for policymaker's expert commentators, and news media to often adopt such extreme metaphors when discussion the need to further cyber-security efforts (2015:25). Frequent nods towards the amalgamations of real events and cybertechnologies, such as "Digital Pearl Harbours" (Panetta, 2012;), were often used to place emphasis on catastrophic threats. Hansen and Nissenbaum (2009) suggest that such narratives are often formulated to secure potential partnerships and compliance between security experts and government/private agencies. With such partnerships, built upon

these narrated scenarios, the perceived reality of these exaggerated scenarios is only further legitimised, and reiterated by cybersecurity experts whom due to the limited understanding by the public, stakeholders, and researchers outside of cybersecurity or computer science fields, often goes unquestioned as the necessary knowledge to understand such complex technologies is often daunting or inaccessible (Nissenbaum, 2005:72).

Consequently, researchers strive to convey a sense of urgency by encompassing diverse terms related to critical infrastructure and non-combatants within these definitions, even in the absence of concrete evidence regarding the actual risks involved, a persistent issue noted several times throughout this thesis. This aligns with Weimann's (2004) notion of "cyberangst," wherein cyberterrorism researchers acknowledge the growing concerns pertaining to unpredictable, illicit, and undetectable cyber actions that inflict substantial harm upon nation states and the general populace. Coincidently, more recent research identified that, although there is a limited number of studies that account for the fear of cybercrime both in specialised instances and cybercrime in general, the levels of fear associated with these acts were generally low to moderate amongst the general populace (Brands and Van Doorm, 2022), with a previous study conducted by Lawson et al. (2016) revealing that depicting extreme cybercrime scenarios, commonly linked with acts of cyberterrorism, can hinder security efforts aimed at addressing real cyber-attack threats. This challenge is particularly pronounced when such messages lead individuals to ignore or downplay the actual potential dangers (Lawson et al., 2016:75).

In contrast to cyberterrorism, the domain of digital activism, including hacktivism, has experienced significant proliferation due to the widespread adoption and accessibility of web-based technologies such as social media platforms, high-speed broadband networks, and internet-enabled portable devices. Traditional movements such as Greenpeace, alongside more contemporary initiatives like Black Lives Matter and *#MeToo*, have effectively harnessed these technologies for purposes of outreach and mobilisation. However, it is crucial to discern that hacktivism constitutes a facet of a larger multiplex of digital actions (George and Leidner, 2019), with hacktivism characterised by direct, targeted interventions (Jordan and Taylor, 2004:69). Consequently, the identified terms associated with hacktivist actions reflect a diminished proclivity for inflicting physical harm or destruction upon targets, instead prioritising endeavours such as website defacement, the acquisition of information for public exposure via data breaches, and public condemnation of individuals, groups, or organisations deemed morally objectionable.

Shifting the focus to hacktivism, this phenomenon manifests a diminished quantity of unique terms within the target classification when compared to cyberterrorism. Coded terms associated with hacktivism include “commercial entity,” “persons,” and “specified data.” These terms reflect the more focused and controlled targeting strategies employed by hacktivists, which contrasts with the indiscriminate targeting often associated with cyberterrorism (Douai, 2015:439). The efficacy of hacktivist endeavours is heavily reliant upon perceived motivation and societal support in attaining their objectives (Kutlaca et al., 2020). Consequently, meticulous consideration of targets becomes imperative to

mitigate the risk of misinterpretation, a factor that is frequently overlooked within the domain of cyberterrorism research.

A comprehensive evaluation of the target typology within the domains of cyberterrorism and hacktivism necessitates the inclusion of neighbouring classifications to grasp the contextual nuances inherent within these phenomena, and not based on target alone, and vice versa when exploring the other classifications present. Notably, discussions pertaining to safeguarding critical infrastructure from external cyber-based disruption environments, including distributed denial-of-service (DDoS) attacks, have persistently occupied the cybersecurity research agenda (Ellis et al., 1997; Bessani et al., 2008), indicating their ongoing significance (see Booth and Andersson, 2017; Lehto, 2022). As there is little evidence that such attacks were conducted by non-state funded actors, it is difficult to identify such targeted attacks as a means of non-state cyberterrorism or even hacktivism. Interestingly, there exists a higher likelihood that such cyberattacks are potentially state funded, with Conway (2018) proposing that even states, with political motive, necessary means, and intent are likely to engage in acts that can be perceived as cyberterrorism.

6.4 Strengths and Limitations

There are important considerations and limitations to consider when considering the usefulness of this study within the much broader domain of criminological research. This section explores both the strengths and limitations of the thesis findings and discussion as original and significant contributions to the understanding of cyberterrorism and hacktivism.

For its strengths, the study benefits from its innovative approach to knowledge mapping, blending comprehensive bibliometric findings with detailed quantitative content analysis. This robust integration of quantitative and qualitative data facilitates a nuanced 'birds eye view' and discussion of the complex ecological issues within the production of cyberterrorism and hacktivism academic research. By effectively presenting a wealth of data, the study not only deepens the understanding of current academic discourse, how this discussion has evolved over time, and potential issues, but also highlights trends and patterns that may shape future research directions. This methodological sophistication aids towards understanding the distinctions and similarities in how cyberterrorism and hacktivism are conceptualised and studied, making a significant contribution to the academic community.

Further strength lies in the use of taxonomic mapping within this study to analyse and categorise definitions within cyberterrorism and hacktivism research, offering insightful revelations into the nuanced differences and potential overlaps within these fields. This not only deepens ontological understanding of the research but also introduces new

analytical tools to the academic community. It holds the potential to guide future studies exploring complex phenomena within the social sciences, particularly by highlighting how terms and concepts evolve in response to rapid technological advancements. This approach proves especially beneficial for unravelling the complexities of these dynamically changing fields, contributing significantly to academic theory and empirical research.

Despite these strengths, the study is not without limitations. A significant limitation concern is the potential over-reliance on quantitative data (i.e. citation metrics, descriptive statistics, and term frequencies), which, while providing a robust foundation for empirical analysis, may underrepresent the nuanced aspects of cyberterrorism and hacktivism that more thematic or discursive qualitative analyses could potentially reveal. This is further exacerbated by the narrow focus on aspects of cyberterrorism and hacktivism knowledge (i.e. high-impact peer-reviewed articles), which may not fully capture the diversity and complexity of the domain. Expanding the scope of analysis to include a broader range of sources, particularly those with specific regional focuses or those outside the mainstream academic channels, or by including more qualitative centred methodologies such as interviews, case studies, or thematic analysis would provide additional perspectives and trends not prevalent in high-impact publications.

One notable limitation is the limited engagement with contradictory literature. While the chapter does an excellent job of outlining the current state of research, it could benefit

from a more robust discussion of studies that contest or contradict the prevailing views. This could include literature that may redefine or challenge the established definitions and conceptual frameworks that the chapter relies on. Engaging more deeply with alternative or dissenting views would not only strengthen the analytical depth of the chapter but also enhance its credibility by demonstrating a comprehensive understanding of the field's discourse.

Further limitations in this thesis concerns how the production of academic knowledge is framed. Using the concept of scientific paradigms as proposed by Thomas Kuhn, the study contends that 'normal science' is achieved through cohesive research where theories and key assumptions are shared across the domain, and that their incoherence is illustrative of a fragmented domain. This was determined through the analysis of citation patterns, sources, and journal distribution of high-impact peer review articles. Future research could benefit by expanding the scope of review for determining fragmentation, such as lowering the citation score from 10, or building upon MacDonald, Jarvis, and Lavis' (2019) earlier survey of terrorism experts by including a wider collection of researchers from contributing disciplines to capture a larger sample of academic experiences.

6.5 Conclusion

By examining the findings of 126 peer-reviewed articles focusing on cyberterrorism and hacktivism, along with their corresponding definitions in Sections 8.2 and 8.3, it is evident that the study of these phenomena exists within a complex terrain marked by both expansion and obstacles.

Concluding this discussion, section 8.2 assessed the trajectory of research within the field, questioning whether the substantial growth since 2000 signifies progress or was indicative of potential issues. While the increasing proliferation of research in this domain might suggest a collaborative and open scientific community, concerns reflective of earlier issues within terrorism studies (Silke, 2004; 2008), and discussions of a potential stagnation emerge (Sageman, 2014). However, the section contends that an alternative perspective of fragmentation, and not "stagnation" may better capture the state of the domain, emphasising the importance of intellectual cohesion and collaboration within cyberterrorism and hacktivism research. Aligning with Balietti et al.'s (2015) proposition that limited progress does not lead to fragmentation but that fragmentation hampers progress.

This chapter argues that fragmentation is seen in the prevalence of conceptual recycling, particularly the consistent citation of Denning's (2000a) work and definitions of cyberterrorism and hacktivism, potentially hindering the development of new ideas and theories. Further, the analysis of citations used by authors of the 126 publications analysed presented an over-reliance on informal networks due to the absence of cohesive journal output, of which further exacerbates the issue. The analysis of author collaboration reveals a significant dispersion of intellectual cohesion, with limited interdisciplinary input and a lack of cross-border collaboration. The gender and geographical disparities among researchers contribute to a narrow perspective and potential biases within the field.

Further exploration of intellectual cohesion in Section 8.2 also highlighted the dominance of single-authored publications and a dispersion of high-impact articles across numerous journals. The lack of collaborative efforts by authors of publications with a citation value above 10, and the absence of a centralised body of literature raises questions about the factors hindering cohesive collaboration. The study introduces the concept of a research "life cycle," (Hirsch and Levin, 1999) proposing that excitement around emerging topics may lead to a flurry of ideas but later result in fragmentation as researchers pursue specialised paths.

Section 8.3 of the discussion shifts to taxonomic mapping, specifically the examination of definitions related to cyberterrorism and hacktivism. The study underscored the blurred definitions of these terms in the literature, citing challenges for further research and theoretical advancement (Baldi et al., 2003; Kenney, 2015). Through a quantitative content analysis and taxonomic framework, the discussion examined key themes and distinctions between cyberterrorism and hacktivism across actor, effect, intent, means, motive, and target classifications. Findings from this examination revealed a lack of actor specificity in cyberterrorism definitions, with terms such as terrorists and sub-national groups lacking detailed explanations or comparisons to specific case studies. The section emphasises the importance of contextual descriptions in shaping public perceptions of cyber threats and policies (Cavelty and Van Der Vlugt, 2015; Nissenbaum, 2005).

Recognising the importance towards having a multi-dimensional overview of social phenomenon and avoiding the risk of using one category alone as determining an act as

either cyberterrorism or hacktivism (Cowen, 2006; Holbrook and Horgan, 2019; Morrison, 2016; Taylor & Horgan, 2006), the discussion examined the conflicting motives and manifestations of cyberterrorism and hacktivism. Analysing the terminology used by researchers to describe the effects of both phenomena, notable differences emerged highlighting the aggressive language in cyberterrorism definitions (Denning, 2000a; Weimann, 2005; Stohl, 2007), contrasting with the more activism-focused language in early hacktivism definitions (Edyvane and Kulenovic, 2017; Fowler, 2016; Gardner, 2014; Wright, 2008). Examining the "intent" in cyberterrorism revealed coded terms like “intimidation” and “coercion,” emphasising its focus on control and societal impact. However, the lack of identifiable actors complicates discerning the legitimacy of such intentions. In hacktivism, motives such as “privacy,” “open access,” and “raising awareness” align with hacker discussions and civil disobedience in the cyber domain. The study assessed the means and feasibility of both phenomena, emphasising the dominance researchers placed towards information and communication technology (ICT) as a dominant means. While the practicality of cyberterrorism remains debated (Conway, 2014a; Jacobsen, 2022; Jarvis and Macdonald, 2014), ideology was presented as playing a crucial role, with "political" being a prevalent term in motivations throughout the sample studied. Evaluation of targets and security narratives in both revealed a focus on critical infrastructure and potential catastrophic scenarios, prompting a caution against exaggerating cyber threats. In contrast, researchers defining hacktivism focused on describing hacktivists objectives towards minimising physical harm, employing controlled targeting, and considering perceptions' impact on goals.

In summary, the study highlights an empirical deficit, conceptual confusion, obstructed by fragmented knowledge in cyberterrorism and hacktivism research, leading to an over-reliance towards media representation, and educated knowledge assumptions of both phenomena. Thus, to move cyberterrorism and hacktivism research towards a more cohesive knowledge framework to foster more robust and collaborative research endeavours, this thesis as part of its contribution, developed a conceptual ontology to map historic, current, and emerging ideologically motivated disruptive cyber-events. This conceptual knowledge-mapping ontology, discussed in the proceeding chapter, provides researchers of various levels of knowledge a framework in which to record events for further breakdown and comparative analysis.

Chapter 7. A Conceptual Ontology for Ideologically Motivated Disruptive Cyber-Events

7.1 Introduction

To alleviate the earlier identified pattern of literature-based and transitory contributions by individual authors that inadvertently contributes towards the fragmentation of the domain of cyberterrorism and hacktivism research, and support efforts towards more primary-data driven empirical studies. This chapter introduces a foundation for empirical understanding by establishing and introducing a data collection methodology. Consequently, through the development of a knowledge mapping ontology using the open-source software Protégé,[14] an accessible framework for collecting and visually mapping offensive cyber events was devised to support the recording and subsequent analysis of ideologically motivated disruptive cyber-events.

The struggle to arrive at shared conceptual definitions is a common obstacle encountered in various academic fields. Levitt (1986) referred to this difficulty within earlier terrorism studies as a "quest for the Holy Grail." While the comparison may seem light-hearted, it is worth considering the possibility of accepting these endeavours as mythical and shifting focus towards more constructive research approaches. Despite the persistent pursuit of a singular and all-encompassing definition of cyberterrorism, early definitions, such as Pollitt's description of "violence against non-combatant targets by subnational groups or

[14] See https://protege.stanford.edu/about.php

clandestine agents" (Pollitt, 1998:9), merely focused on attacking computers, while Collin's (1997) envisioned more fantastical scenarios involving hacking aeroplanes, causing ecological disasters, and inexplicable explosions. Such apocalyptic predictions akin to "cyber doom days" are still prevalent (Gomez and Whyte, 2021; Lawson et al., 2016). Recent attempts at formulating definitions seek to address the ambiguity in conceptualising the phenomenon by adopting more rigorous methodologies, as demonstrated in Plotnek and Slay's (2021) homogenised taxonomy. This approach consolidates various interpretations of cyberterrorism from different researchers, resulting in a robust and well-constructed definition.

The pursuit of a definitive definition is commendable, as it aims to foster shared understanding and standardisation, which could significantly enhance knowledge in the domain. However, the current state of cyberterrorism and hacktivism research is characterised by a lack of empirical studies, and abundance of definitions. Given this context, the quest for a singular conceptual definition may seem impractical or self-serving, leading to the creation of yet another unused definition that quickly becomes overshadowed or outdated in a yet to be charted domain.

To offer a more practical application of the research findings, an ontological model focusing on offensive events in the cyber environment was developed. The choice of "offensive events" over "attack events," as used by Donalds and Osei-Bryson (2019) in their ontology of cybercrime, is driven by the intention to classify events as either cyberterrorism, or hacktivism. The use of terms as evident throughout this study, plays a significant role on how such phenomena are perceived. Cavelty and Van Der Vlugt (2015)

raised concerns about the use of “attack” when discussing cyberattacks, quoting; “the concept of "attack" suggests an immediate visible effect delivered by a visible attacker” (Cavelty and Van Der Vlugt, 2015:25). Yet, when examining occurrences in a virtual setting, they can frequently evade detection for an extended period after initiation. Embracing the term "offensive" imparts a more nuanced comprehension to the ontology regarding motivations and actions in the cyber domain. This acknowledges that disruptive cyber events may not manifest or be observable immediately upon execution.

7.2 Background to Ontologies

Noy and McGuinness (2002: 3) define ontologies as formal, explicit descriptions of concepts within a specific domain of discourse. Each concept is characterised by its properties, features, attributes, and restrictions. When combined with individual instances of classes, such as those seen within the earlier taxonomy, an ontology forms a knowledgebase. However, there exists a fine line between where the ontology ends, and the knowledgebase begins.

To put it simply, Gruber (1993:199) describes ontologies as formal representations of shared concepts within a standardised framework. These shared concepts facilitate accurate communication between individuals and computer systems, promoting the sharing and reuse of accumulated knowledge (Frantz and Franco, 2005) due to the establishment of common standards. The reasons for developing ontologies, as provided by Noy and McGuinness (2002), include:

1. Enabling a common understanding of information structure among people and software agents.
2. Facilitating the reuse of domain knowledge.
3. Ensuring explicit domain representation when making domain assumptions.
4. Better distinguishing between domain knowledge and operational knowledge.
5. Allowing for the analysis of domain knowledge.

Recent work has expanded the typological model of hacker types by focusing on variables such as skill and motivations, enabling a better differentiation of several types of hackers rather than limiting them to a singular type (Hosford, 2021; Rogers, 2006; Seebruck, 2015). Similarly, ontological modelling has been used to classify cybercrime, as seen in the research of Donalds and Osei-Bryson (2019). Their study identified limitations in existing classification schemes for cybercrime, such as taxonomies that lacked consistency and fragmented terminologies, hindering effective classification (Donalds and Osei-Bryson, 2019:417). Donalds and Osei-Bryson's approach adopts a holistic view, drawing from previous cybercrime-focused ontological works while flexibly classifying multiple variations and dimensional properties associated with cybercrime events.

In contrast, cyberterrorism has seen only one published ontological model (see Veerasamy et al., 2012), while hacktivism has not been subjected to any previous ontological modelling. A more recent effort although not specifically focused on ideologically

motivated disruptive cyber-activities, but instead more broadly towards social media and terrorist cybercriminal activities is seen in Rawat's (2023) ontological model. Like this study, Rawat adopts the ontology web language (OWL) approach to collect and analyse social media (specifically Twitter "*X*" data) pertaining to news reports of terrorism. Although interesting in its approach, this study excludes the automated use of social media posts for multiple purposes, first; many Online Social Networks (OSN) such as Twitter or "X", and Reddit which sees frequent use within social network analysis within terrorism studies (see Cheong and Lee, 2011; Gaudette et al., 2021; Weimann, 2010), recent studies often rely upon the use of closed source application programming interface (API) in order to automate access to the volumes of data used to analyse.

Instead, this study takes a similar, albeit with modifications to an approach as seen in Veerasamy et al. (2012) who developed a general ontology of cyberterrorism to distinguish between acts of cyber-terror, acts of terror supported by cyber means, and general cyber-events. The decision to employ an ontological approach in discerning cyberterrorism and non-cyberterrorism events stemmed from the significant overlap of cyberterrorism activities and ICT hacking. Their ontology was constructed by capturing key concepts and relationships from previous research findings (van Heerden et al., 2012; Veerasamy, 2009; Veerasamy and Grobler, 2015) using the ontological language Protégé, like Donalds and Osei-Bryson (2019).

However, Veerasamy and Grobler's (2015) adoption of Protégé for their cyberterrorism ontology proved insufficient in capturing logical relationships between different

classifications, relying heavily on individual inferences, and making cross-comparison of findings difficult. Therefore, by combining the efficiency and breadth of Donalds and Osei-Bryson's (2019) cybercrime ontology with the differentiating features of Veerasamy and colleagues (2012; 2015) ontology of cyberterrorism, an ontological model capable of classifying and differentiating characteristics of cyberterrorism and hacktivism can provide a common and compatible framework for capturing historical and emerging events within the domain of cyberterrorism and hacktivism for future sharing and research.

This combined ontological model offers significant advantages in the study of cyberterrorism and hacktivism. By integrating the strengths of previous ontologies, it can provide a more comprehensive and cohesive understanding of these phenomena. The use of Protégé as the ontological language allows for logical mapping, graphical visualisation, and easy sharing of ontologies (Musen, 2015). The improved ontological approach ensures that the logical relationships between different classifications are well-captured, enhancing the effectiveness of the model.

7.3 Developing the Ontology

Drawing upon the earlier works of Veerasamy et al. (2012) and Donalds and Osei-Bryson (2019), a formal ontological base model was developed to capture and classify cyberterrorism and hacktivism events based on previous understandings and findings. Prieto-Diaz (2003:548) highlighted that ontology development begins with an ad-hoc

creation of a controlled vocabulary, defining key terms, and later establishing relationships between concepts to construct the ontology.

The complexity of ontologies varies, based on factors such as logical frameworks, philosophies, classifications, and the degree of mutual understanding within the discipline. Prior to constructing a controlled vocabulary and defining relationships, it is essential to outline the process of ontological modelling. Uschold and colleagues (1995; 1998) proposed a "skeletal" methodology for building ontologies, which involves the following steps:

1. Identify the purpose of the ontology.
2. Build the ontology:
a. Ontology Capture
b. Ontology Coding
c. Ontology Integration
3. Evaluate the ontology.
4. Document the ontology.

Clearly describing the purpose of the ontology is crucial (Uschold and King, 1995). Thus, to ensure a clear understanding of the purpose of this research project's ontology, it is restated as follows.

The ontology is developed with the aim of providing a common and compatible framework for capturing, classifying, and differentiating characteristics of cyberterrorism and hacktivism from both historical and emerging events. Its utility lies in facilitating future sharing and research endeavours.

Ontologies are designed for practical applications. Their versatility allows for adoption in various settings and contexts. Furthermore, the development of an ontology itself is not an end goal but a means of establishing standardisation. Noy and McGuinness (2002: 2) liken this standardisation process to defining the structure and parameters of data for use in other programs.

Given the significance of ensuring the ontology's standard and compatibility within an IT environment, a design science research method was adopted. This approach ensures that the ontology of cyberterrorism and hacktivism meets rigorous standards and aligns effectively with IT systems and processes.

7.3.1 Design Science Research Methodology

Like Donalds and Osei-Bryson (2019), this chapter adopts a design science approach to developing an ontology of cyberterrorism and hacktivism. Design science is a research paradigm of creating and evaluating IT (information technology) “artefacts” such as models and methods of which are developed through a rigorous process of design and evaluation (Offermann et al., 2010) and intended to aid in solving research problems (Peffers et al., 2007:49). Reasonings for adopting Design Science Research Methodology (DSRM) is akin to Donalds and Osei-Bryson (2019) reasoning:

1. It accommodates the construction of practical artefacts by focusing on the development of said artefact.
2. It does not require formal embedding for the evaluation of the artefact.

3. It allows for the building upon of previous research efforts that similarly adopted design science guidelines.
4. It can provide a synthesised model.

To achieve the above reasoning, several steps are provided within DSRM, similar to Donalds and Osei-Bryson's (2019) cybercrime ontology, this section of the study follows Peffers and colleagues (2007) six step guide to the construction of ontologies using "design science research methodology": This includes the Problem Identification and Motivation, Define the Objectives for a Solution, Design and Development, Demonstration, Evaluation, and Communication, of which will be briefly discussed:

Problem Identification and Motivation: The initial step, as discussed by Peffers et al. (2007: 53) and Donalds and Osei-Bryson (2019) involves defining the specific research problem and justification for the solution. The problems that exist within cyberterrorism and hacktivism research has been extensively mapped, analysed, and discussed within the previous chapters, most notably.

- The inability to meet a consensus on definitions of hacktivism and cyberterrorism, inhibiting cohesive research.
- A significant lack of empirical data, of which to base foundational understanding from.
- Knowledge fragmentation re-enforcing a permissive trend of the earlier issues.

Therefore, the objective of this research stems from the need for a practical means of standardising cyberterrorism and hacktivism data collection to mitigate conceptual conflicts and anecdotal observations from limiting the collection and analysis of empirical data attributed to cyberterrorism and hacktivism events, promoting more cohesive and potentially more collaborative research.

Define the Objectives for a Solution: The objective of the solution is inferred from the problem definition. Therefore, to clearly state the objective of this ontology, of which based on Donalds and Osei-Bryson (2019:406) stated objectives of cybercrime, but specified to cyberterrorism and hacktivism is to address the lack of empirical and cohesive research within cyberterrorism and hacktivism research by designing an ontological model that provides:

1. An explicit integrated conceptualization of cyberterrorism and hacktivism classification for use by cybercrime stakeholders such as researchers, investigators, and practitioners.
2. A comprehensive and holistic, multiperspective cyberterrorism and hacktivism classification and analysis model that involves a parsimonious set of relevant concepts and direct relationships.
3. A flexible artefact that can easily accommodate new concepts and new relationships, capable of classifying current and future cyber-disruptive acts that may involve elements of cyberterrorism and hacktivism.

4. A formal cyberterrorism and hacktivism classification ontology that could allow for sharing of knowledge.

Design and Development: As Peffers et al., (2007:55) notes, once the creation of the artefact is completed, which can be anything like structures, models, methods, or different information sources (citing Järvinen, 2007:49). This process entails defining the desired functionality and architecture of the artefact before its actual creation. Essential resources for progressing from objectives to design and development include the application of theoretical knowledge to formulate effective solutions.

Demonstration: A demonstration is needed to show that the artefact solves identified problems. This often includes activities like experimentation, simulation, or case studies. Additionally, users of the artefact should know how to use it for problem-solving effectively (Peffers et al., 2007).

Evaluation: Observe and measure how well the artefact supports a solution to a defined problem. This involves comparing the solution's goals with the actual results observed during the artefact demonstration (Peffers et al., 2007). Evaluating the artefact, like the cyberterrorism and hacktivism ontology, requires understanding the relevant factors. Potential future evaluations of the results can help researchers decide on further improvements and implementations for the artefact.

Communication: It's important to communicate the problem when presenting the artefact as a potential solution for researchers to adopt. According to Peffers et al. (2007:56), researchers might use the structure of this process in scholarly research publications, like the common structure of empirical research papers. Lastly, effective communication requires an understanding of the disciplinary culture linked to the artefact.

7.3.2 From Taxonomy to Ontology

Upon describing the ontologies' purpose, it is now possible to proceed with the development of a controlled vocabulary as mentioned earlier (see Prieto-Diaz, 2003; Uschold and King, 1995). This ontology adopts both taxonomies discussed previously (see section 6.4.2 Building the Taxonomy: 191), which were constructed from a quantitative content analysis method to extract, code, and analyse definitions of both cyberterrorism and hacktivism.

During the development of the previous two taxonomies (cyberterrorism and hacktivism), key terminology was categorised under six independent classifications (actor, effect, intent, means, motive, target). Therefore, the organisation of terms within these classifications was initially unstructured and organised only by one of six classifications. To organise and unionise a large corpus of terms that included similar terminologies and differences in spellings, a brief organisation coding was introduced to consolidate terms for the benefit of clearer visualisation (see Figure 5.31 Network Distribution of Extracted Effect Terms:275).

For the purposes of this ontology, the organisation coding introduced in the quantitative content analysis was further refined to provide clarity. As the previous chapters' purpose involved quantification of term frequencies and the presentation of different variations of such terms, albeit identical in their meaning to collectively illustrate the variety of terminology, the ontology benefits from strict and concise terminology to ensure consistency. Therefore, terms with slight variations such as the use of hyphens and acronyms are reduced to their core terms and organised within groups based on their associated type.

Grouping of terms allows for the categorization of diverse types associated with the term. For example, virus, ransomware, trojan, and worms are all individual types of malwares (a subclass of the means classification) with unique properties, therefore, within an ontology these individual types would be grouped under the malware subclass.

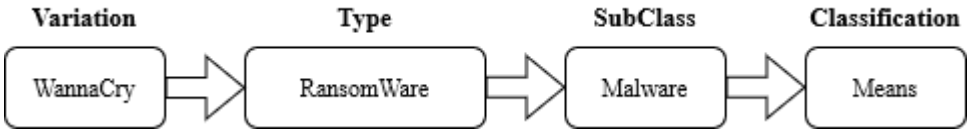


Figure 7.1 Bottom-Up breakdown of Schema

Figure 7.1 illustrates a bottom-up approach to organising and classifying key terms within an ontological model. As noted by Noy and McGuinness (2002:6), a bottom-up development process starts with the definition of the most specific classes, the leaves of the hierarchy, with subsequent grouping of these classes into more general concepts.

Therefore, to generalise figure 7.1, WannaCry is a specific type of ransomware, of which is a form of malware, and is used as a means towards a specific goal, as stated in the previous chapter; the means classification focuses on how those conducting hacktivist or cyberterrorist activities achieve their intended outcome (Veerasamy, 2009). Previous organisational methods used earlier for the taxonomies would have limited this classification to only malware, or when presenting the taxonomy, as only a means. This in turn ignores the economic aspect of ransomware, limiting the scope of understanding available from a taxonomy.

Further, in adopting an ontological approach, we can extend this understanding to incorporate unique properties and knowledge associated with different variation types. Since WannaCry is a version of ransomware, its primary goal is to coerce victims into paying the declared ransom, this is achieved by encrypting the contents of the victims infected storage drive with threat of deletion if the ransom is not paid within a limited period (Whittaker, 2019). From this brief example, it can be discerned that WannaCry provides additional contributions to the means classification by including coercion and encryption as additional attributes that simply would not be associated if prior taxonomy was used without pre-existing knowledge.

1. Conceptual Modelling of Classifications

Prototyping of the conceptual model adopted an entity-relationship model. Developed by Peter Chen (1976), an entity-relationship model is a diagrammatic technique frequently

used in the planning and development of database design, adopting real world semantics allowing for the relationship between different entities to be defined.

Figure 7.2 (next page) illustrates the conceptual model of the cyberterrorism and hacktivism ontology. Visually presented within figure 10.02 are key classifications and subclasses and the relationships (alias connection type) shared. These key classes and subclasses will be further discussed below; however, it should be noted that the ontology itself is more extensive, with additional characteristics and relationships not represented in figure 7.2.

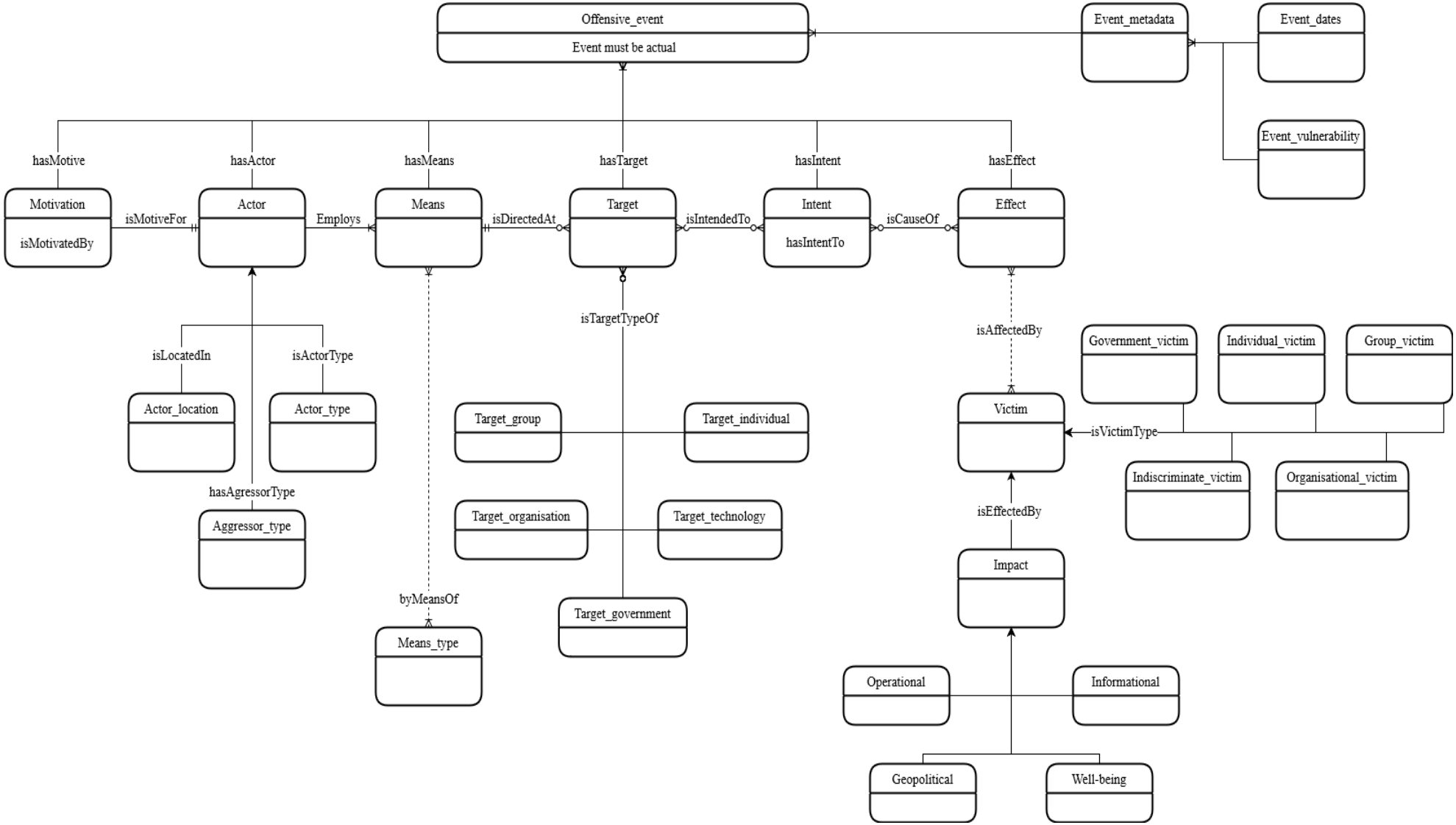


Figure 7.2 Conceptual Ontological Model

Offensive event

The offensive event is associated with the real-world act committed by the actor classification. Data recorded could, if known, include start date of the event, date targets become aware of the offensive event, and the end date including resolution should be recorded. For example, the HSE cyberattack began on the 16th of March 2021,[15] HSE operations security staff became aware of the breach on the 13th of May 2021 with the attack ending on the 14th switching off IT systems to prevent further spread of the Conti ransomware. Donalds and Osei-Bryson (2019) suggest that recording the above details has the potential of aiding practitioners and researchers in identifying trends and patterns over time.

Motivation

The motivation class is a key element in recording events of cyberterrorism and hacktivism. Positioned first and pertaining to prominent levels of motivation as a driving force of the actor (Veerasamy et al., 2012), the motivation of an offensive event aids in discerning cyberattacks as either ideological, political, religious, or more generalised cybercrimes. The subclasses of the motivation class are criminal, social, ethical, premeditated, recreational, religious, political, and financial.

Actor

The actor class pertains to those who both intentionally contribute and execute the offensive event. As figure 7.2 shows, the actor class has three subclasses; **actor type**

[15] See: 'Number of days' before systems back working - HSE. Available at: https://www.rte.ie/news/health/2021/0514/1221519-hospital-it-problem/

referring to the composition of the actor such as: collective group, organisation, individual, nation state, and unknown actor. The **actor location** refers to the physical origin of the attacker or where the attack was launched, such as a foreign actor, local actor, or indeterminate actor. Lastly, the **aggressor type** refers to those associated with the actor type such as a sponsor or those who sanction an offensive event (Donalds and Osei-Bryson, 2019: 409). **Aggressor types** can be categorised under commercial aggressor, individual aggressor, unknown aggressor, state aggressor, and self-instigator referring to those who both instigate and conduct the offensive event.

Means

Means refers to both the practical utility and the approach adopted to conduct the offensive event. Subclasses include physical means, psychological means, illegal means, and ICT means of which is extended by further subcategories; communication systems, data systems, exploiting digital infrastructure, exploiting physical infrastructure, network tools, and malware.

Target

Chosen as the recipient of the offensive event by the actor and not to be confused with a victim, the target refers to the intended receiver. The target classification can be further classified under the target type subclass as: target group, target technology, target individual, target government, and target organisation. Due to the complexities of ICT, the target technology subclass is further broken down into five categories; target infrastructure, target network device, target site, target software, and target personal device.

As figure 7.2 illustrates, the connection between the target classification and target type is dotted and associated with many options. Therefore, many targets for the offensive event can exist in varying degrees of complexity. For example, a private company employee may have their personal mobile device targeted, which if catalogued would include the target organisation, target individual, and target personal device categories.

Intent

The intent classification refers to low-level purposes of the offensive event (Veerasamy, 2009). The intent classification is based upon findings from the previous quantitative content analysis and taxonomies (see 5.3 Part Two: Quantitative Content Analysis of Definitions), providing the following subclasses: intimidate, terrorise, cause disruption, coerce, attack, destroy, damage, influence, and assist. To note, the intent of an offensive event can be both similar and different to the result (i.e., the effect).

Effect

Different from Veerasamy et al. (2012) ontology of cyberterrorism, the effect classification is broken into two subclassifications: victim classification and impact. Within this classification the victim subclass is required to be defined as opposed to being assumed or suggested, and similarly to the target type subclass, multiple victim(s) can exist for a single offensive event. The categories associated with the victim subclass are 'government victim, individual victim, group victim, organisational victim, and indiscriminate victim.'

Impact

Attributed to the victim subclass is the impact subclass. The impact refers to the actual effect of the offensive event on the victim. Categories within the impact subclass include information such as disruption and dissemination, geopolitical, economic, and well-being such as physical and psychological impact. As noted previously, the intent and effect classifications are not related. The intention of an offensive event and the adopted means, depending on various circumstances, may result in a different effect than originally expected. Further, the nature of the effect may also include victims outside those originally conceived within the intent and target; however, effort should be taken to discern between purposely pursuing an offensive event that results in an indiscriminate victim and those with specific victims that may include other victims as collateral.

7.3.3 Developing the Ontology in Protégé

Having now conceptualised, defined, and mapped key classifications and subclassifications, it is now possible to begin constructing the ontology model. Both Donalds and Osei-Bryson's (2019) cybercrime ontology, and Veerasamy et al. (2012) ontology of cyberterrorism make use of the Protégé software package. Protégé is an open-source ontological development package developed by Stanford University that allows for the logical mapping, graphical visualisation and sharing of ontologies (Musen, 2015).

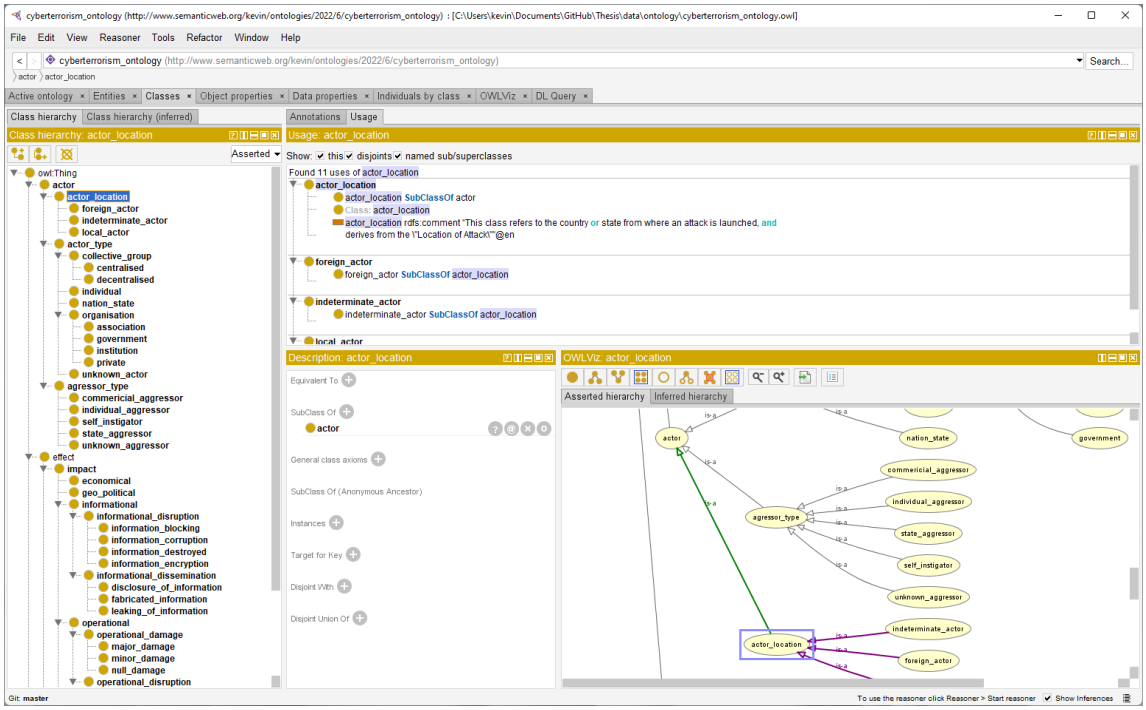


Figure 7.3 Example of Protégé user interface

Figure 7.3 presents the general user interface of Protégé. In this example, the list presented on the left illustrates the hierarchical layout of the ontology consisting of classes (upper hierarchy), preceded by several levels of subclasses (lower hierarchy). The classes adopted within this ontology are derivative of the previously developed taxonomy classifications (actor, effect, intent, means, method, target), based on Plotnek and Slay's (2021) taxonomy. Subclasses are, however, as noted by Prieto-Diaz (2003:548), developed ad-hoc, dependent on previous findings and continuous review and revision.

This ad-hoc multi-level classification allows for the adaption of the ontology as further revisions result in updated iterations. Noy and McGuinness (2002) note that as domain knowledge often denotes the notion of time such as time intervals, points of time, and relative measures of time, having an adaptable ontology allows future researchers to

simply reuse or build upon the ontology. Further, in adopting a standardised model via Protégé, the developed ontology can be further integrated into existing or future ontological systems.

2. Implementation of Conceptual Model in Protégé

Ontologies are used to capture knowledge about a particular topic, explaining different concepts and the relationship between these concepts. To help standardise this knowledge capture, Protégé adopts the OWL 2 Web Ontology Language (OWL), which is an ontology language for the Semantic Web with formally defined meaning. OWL formatted ontologies provide classes, object properties, individuals, and data values which can be used to capture, breakdown and organise domains and its associated knowledge (Hitzler et al., 2009).

a. Implementation of Classes

"Classes" are concrete representations of formal categories and allow users of the ontology to observe classes as sets containing individual domains of discourse (such as key terms, individuals, locations, and events) that fulfils the requirements to be associated with the specific class (Horridge, 2011: 12).

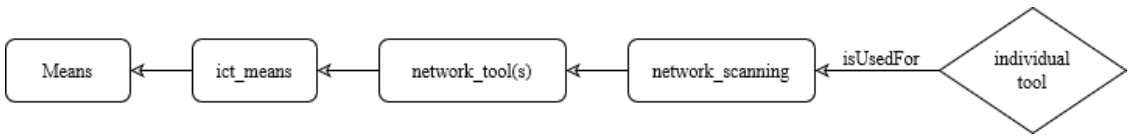


Figure 7.4 Example Class Structure

For example, consider the classes “network tool(s)” and “network scanning,” the network scanning class is a subclass of network tools(s) as specific individual tools exist to scan networks. This implies that all network scanning tools are network tools. Further, network tool(s) is itself a subclass of ICT means, of which itself is a subclass of Means as illustrated in figure 7.4. Therefore, all network tools can be considered a means within the ontology. Having classes and subclasses structured in this manner allows for vital details of an offensive event such as a cyber-attack on national infrastructure to be recorded in more consistent detail.

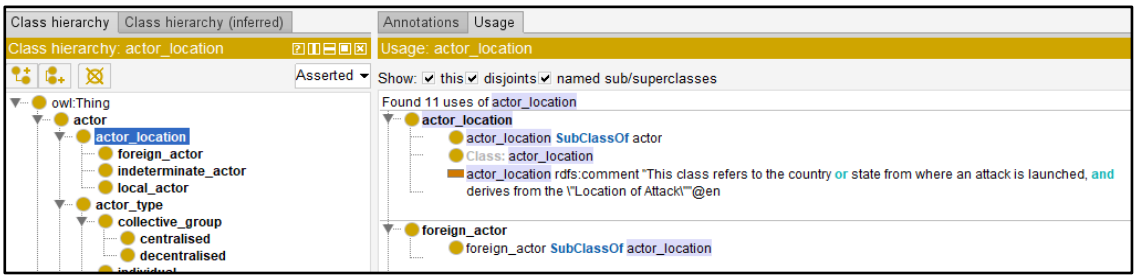


Figure 7.5 Example of Class Annotation

Implementing classes within the ontological model was straight forward. Using the conceptual ontology model (figure 7.2), each class was added in order of class and hierarchical position. As the ontology is envisioned to provide practical utility, each class as shown in figure 7.5 is given annotation into describing the purpose of the class as to avoid interpretational confusion. Having established a baseline class structure for the ontology, it is now possible to begin representing relationships between classes using object properties.

b. Implementation of Object Properties

“Object Properties” provide a binary relationship between individual domains of discourse (Horridge, 2011: 11). These relationships form the basis of whether a potential query involving two or more concepts is answerable (Donalds and Osei-Bryson, 2019: 411). For example, the hacker group known as ‘Wizard Spider’ breached the servers of Ireland’s healthcare system the HSE (Gallagher and McQuinn, 2021). If the relationships between both parties was to be objectified within the ontology it would be at its base level; HSE “isTargetedBy” Wizard Spider. Having standardised variables associated with the specific relationship between individual domains provides for consistent recording and analysing of these relationships.

Oddly, although Protégé was adopted, Veerasamy et al. (2012) chose to exclude the use of “object properties” within their ontology of cyberterrorism and instead focused heavily on classes and basic ‘is-a’ or ‘is’ relationships, thus object properties within this ontology are initially based on those developed by Donalds and Osei-Bryson (2019).

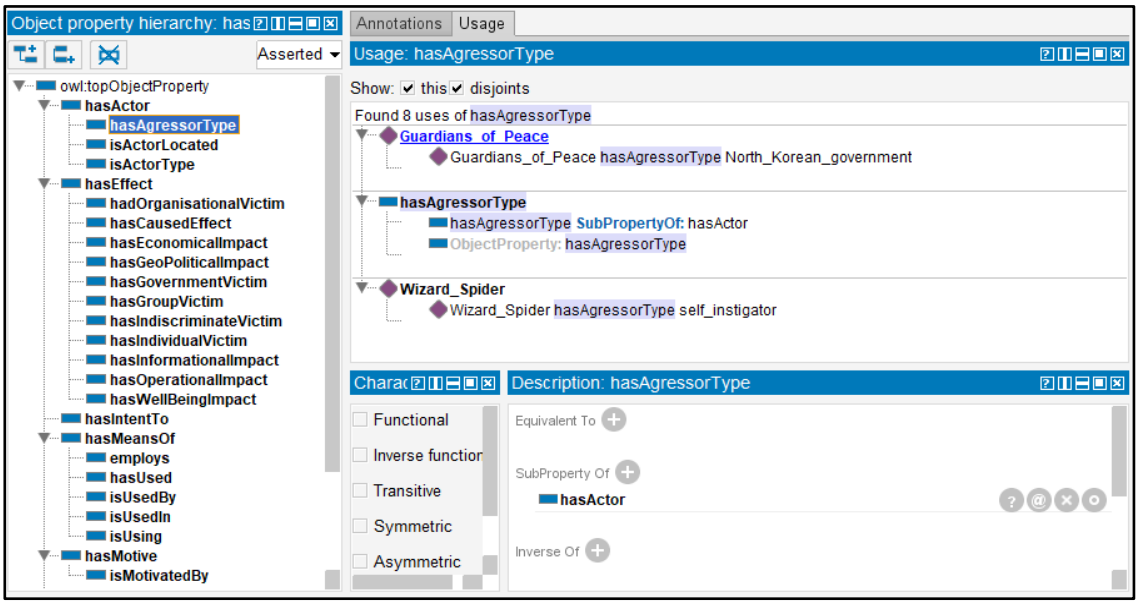


Figure 7.6 Example of Object Property Annotation

As shown in figure 7.6, the "object properties" are based on those developed by Donalds and Osei-Bryson (2019). However, to provide compatibility to the classification model introduced by Veerasamy, Grobler, and Solms (2012) and refined by Plotnek and Slay (2021), additional "has" object properties were implemented to accommodate this inclusion with the appropriate object properties becoming sub-object properties. For example, the "hasAggressorType," which is a sub-object property of "hasActor," is selected in figure 7.6, which shows the usage of this object property. Hacker group Guardians of Peace are labelled as "hasActor" who, for a specific event, were supported by the North Korean Government which is labelled "hasAggressorType." This organisational approach allows users of the ontology a natural understanding of the hierarchy of object property when recording an offensive event. Thus, reducing the risk of misinterpretation.

c. Implementation of Individuals

Known as the domain of discourse, "Individuals" represent the objects themselves within the domain of which we are interested in (Horridge, 2011:10). Individuals are the key terms present within an offensive event such as key actors, targets, both specific and broad technologies adopted and effected, victims, ideologies, intents, and such. As these individuals are derived from the offensive event, they are not predefined nor assumed but instead collected and organised by pre-existing classes and object properties.

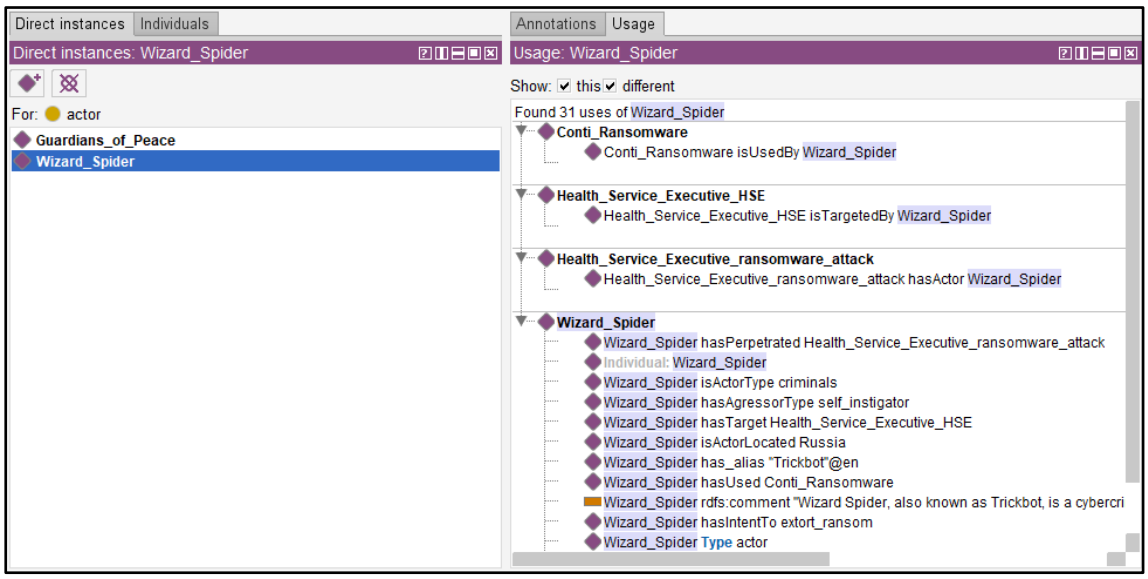


Figure 7.7 Example of Individual's Annotation

Figure 7.7 presents the individual Wizard Spider. Its relationships with other individuals can be seen using defined object properties. For example, we can see that the individual Conti ransomware was adopted and used by Wizard Spider in its use of the 'isUsedBy' object property against the target Health Service Executive HSE by the presence of 'isTargetedBy' during the Health Service Executive ransomware attack event of May 2021. In adopting this approach, only factual details are recorded from an offensive event and the relationships between these details (alias "individual's annotations") is established and recorded. This removes ambiguity associated with previous means of recording of events deemed offensive (Donalds and Osei-Bryson, 2019; Veerasamy, Grobler, and Solms, 2012) which often rely too heavily on the interpretation of the researcher (Jarvis et al., 2014, Macdonald et al., 2015).

7.4 Evaluation of the Ontology

Having conceptually established, presented, and discussed the ontological model, and later implementing this model within Protégé, the utility of the ontology can now be evaluated. Two real world cyberattacks; the Health Service Executive ransomware attack, which involved a state funded public service as a target, and Sony Pictures Hack, in which a private organisation was a target. The reasoning for using both a state provided service and private organisation for evaluation is to demonstrate the adaptability of the ontology as non-restrictive to any target and victim type, be it a nation state or private company.

Example: Health Service Executive ransomware attack

Using details available from official documentation of the event as published by the Health Service Executive (HSE) of Ireland,[16] key terms and factors of the event can be recorded. Further information of the offensive event was collected and compared to enrich the recorded information and better categorise derived individuals. For example, within the official report the actors of the offensive event are not mentioned. These actors are, however, mentioned in numerous state and non-state news publications (Gallagher and McQuinn, 2021; Reynolds, 2021). Therefore, a brief synopsis of the event based on the collected material is presented and included within the offensive event annotation:

On 14 May 2021, the HSE suffered a major ransomware cyberattack which caused all its IT systems nationwide to be shut down. The group responsible was identified as a

[16] HSE publishes independent report on Conti cyber-attack, available here: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

criminal gang known as Wizard Spider, believed to be operating from Russia. The same group is believed to have attacked the Department of Health with a similar cyberattack.

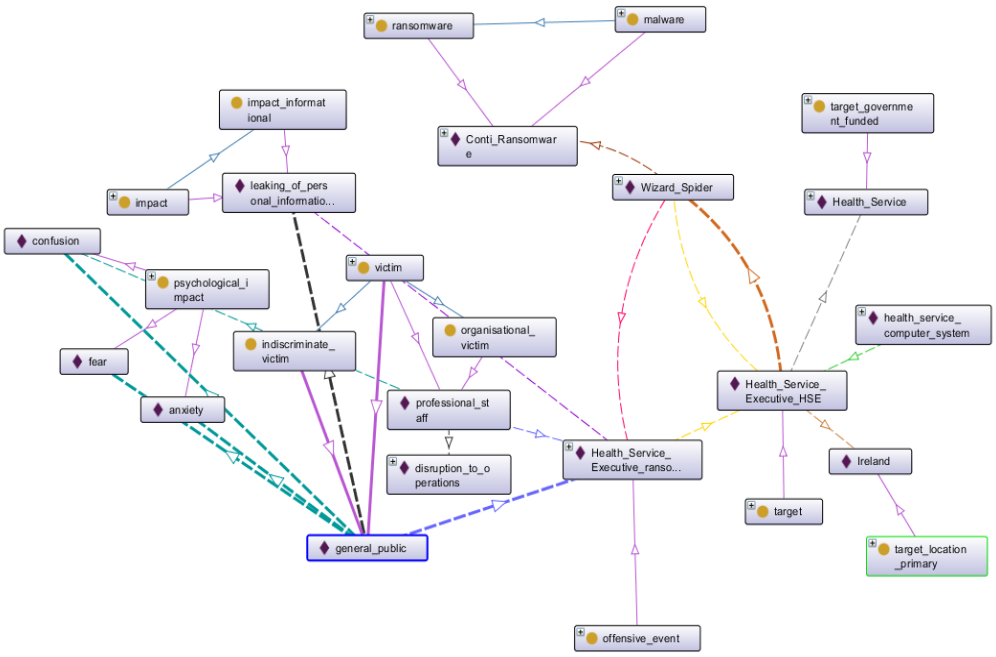


Figure 7.8 Offensive Event Perspective of HSE ransomware attack

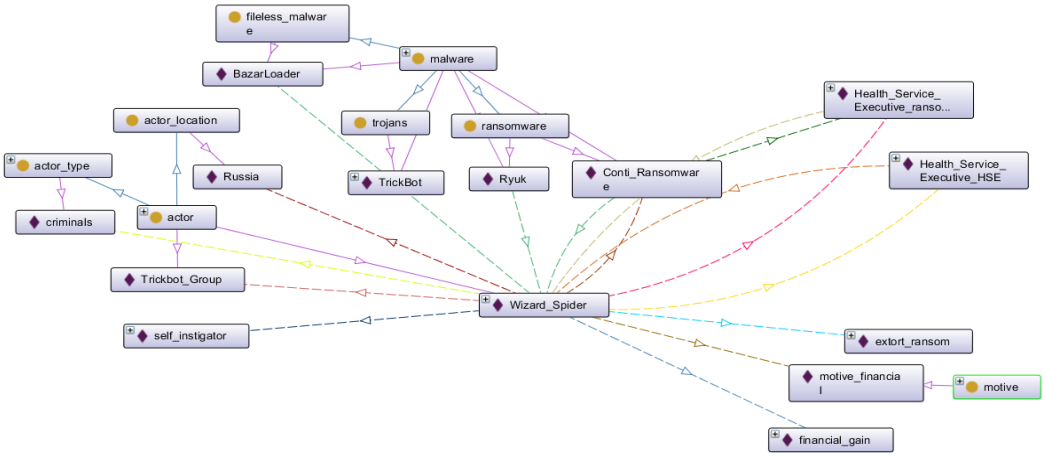


Figure 7.9 Actor Perspective of Wizard Spider

As a data collection utility, key terms represented as individuals within the Protégé ontology are classified accordingly with the relationship between these individuals in a standardised manner. This standardisation in how individuals are collected and organised allows for the visual representation of the event as illustrated in both figure 7.8 and figure 7.9 to be generated and associated with specific individuals of a recorded event with directional relationships between these terms represented as dashed lines having arrows representative of the direction of the relationship. As shown, both figures relate to the same event, however, the complexity of data presented can be defined to provide only information relevant to the individual selected.

This framework provides researchers a concise means of exploring the event in a more practical manner, essentially giving each individual that has been recorded a level of agency higher than previous case-study approaches that often records the entirety of an event in a long form narrative account (Jarvis et al., 2014, Macdonald et al., 2015), providing an unbiased empirical repository for further analysis and interpretation of the event and key aspects for future research.

Example: Sony Pictures Hack

Continuing as a data collection method, the ontology allows for the collecting and organising of a variety of offensive events. The brief synopsis below provides a summary of the offensive event: On November 24, 2014, a hacker group identifying itself as “Guardians of Peace” leaked a release of confidential data from the film studio Sony

Pictures Entertainment (SPE).[17] The data included personal information about Sony Pictures employees and their families, emails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, plans for future Sony films, scripts for certain films, and other information.

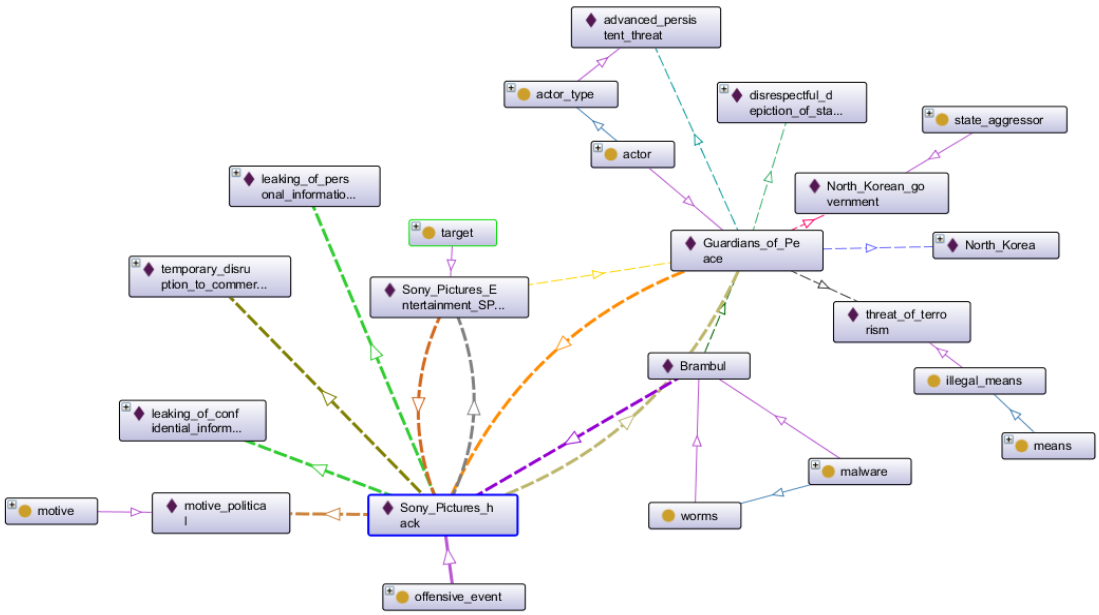


Figure 7.10 General Perspective of Sony Pictures Hack

Figure 12.10 illustrates a general overview of the offensive event. The complexity of the knowledge graph can be modified to show only information meaningful to the observer at their discretion and show key individuals irrespective of the event's perceived definitional classification. By not attempting to define the offensive event and instead collect and organise relevant details within a standardised format, each key individual can be more critically compared to other offensive events that may otherwise have been

[17] Trend Micro: The Hack of Sony Pictures: What We Know and What You Need to Know (2014), at: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know

defined as a different social phenomenon. More importantly, the issues as frequently discussed (Conway, 2014a; 2018; Gordon and Ford, 2002;2006; Jarvis and Macdonald, 2015; Jarvis, Macdonald, and Whiting, 2016; Leukfeldt and Yar, 2016; Macdonald et al., 2019) concerning a lack of empirical data for further analysis can be further mitigated by taking an inductive approach to analysis and discussion mitigating the challenges imposed by relying on firstly defining the social phenomenon.

For example, if we were - To address these challenges, a conceptual ontology for mapping ideologically motivated disruptive cyber-events was developed, aiming to foster robust and collaborative research by providing a framework for recording and analysing events for comparative analysis.

to firstly define the offensive event discussed under any of the recorded definitions analysed within the earlier content analysis chapter (see 7.3 Part Two: Quantitative Content Analysis of Definitions: 249), then neither the HSE ransomware attack nor the Sony Pictures hack would be classified as cyberterrorism nor hacktivism. This would be for two reasons. First, the HSE ransomware attack was financially motivated as opposed to religious, social, or political, and the Sony Pictures hack, although politically motivated and the threat of terrorism was declared, did not result in any considerable impact to critical infrastructure or posed any significant risk, fear, or harm. Secondly, neither event was in pursuit of any significant social justice or betterment of the disfranchised but instead largely driven by individual gain and retribution. As such, following the ontology, neither of these two events would be classified as cyberterrorism or hacktivism.

7.5 Conclusion

To rectify this pattern of literature-based and transitory contributions by individual authors, and to introduce a foundation for empirical understanding, this research project recognizes the necessity of establishing and introducing a data collection methodology. Consequently, through the development of a knowledge mapping ontology using Protégé, an open-source software tool, an accessible means of collecting and visually mapping offensive cyber events was devised to standardise the data collection phase and subsequent analysis.

The ontology is proficient in gathering and organising various facets associated with a range of cyber events, doing so in an impartial manner. Its objectivity comes because the emphasis lies in categorising facets of the event, rather than the event itself. This approach obviates the need for consensus on definitions as a prerequisite for data collection and organisation. This is advantageous, as prior methods constrained researchers to observe and gather cyber events within a predefined and frequently anecdotal framework, potentially leading to challenges and inconsistencies when attempting to identify past events for analysis.

Moreover, by adopting an ontological approach that eschews definitions that often centred on potential targets of these social phenomena, more nuanced and distinctive facets (motivation, skill, means, affiliations, victims etc.) can be recorded to furnish a more comprehensive dataset for subsequent analysis. Finally, by adhering to a standardised approach for decomposing, recording, and classifying cyber events, this methodology is not confined for use by any specific individual or research team, but can

instead be updated, expanded, and employed by an indefinite number of stakeholders, facilitating alignment with emerging trends and technological advancements that may arise. Overall, this chapter provides a pivotal contribution towards rectifying the prevailing deficit of empirical evidence in the study of cyberterrorism and hacktivism, offering a methodological framework that can enhance the rigour and comprehensiveness of future research in this critical field.

Chapter 8. Conclusion

8.1 Introduction

To start the conclusive closing chapter of this thesis, a brief reflection on the doctoral thesis by Dr Maura Conway (2006) felt fitting. Conway's thesis provided support towards 'making sense' of earlier understandings of cyberterrorism, and in part hacktivism. Conway introduces her conclusion with a quote from Jon Guice;

> *"In 'Internet time,' as in 'dog years,' eons have passed since the first messages were sent between computers. The Internet now has its own history, though most of the events took place just years ago, and portentous changes are taking place today" (Guice, 1998:201)*

Conway, recognising the Internet as an avenue for rich culture and historical significance, proposed a means of understanding the "current history" of the Internet. Like this research project, Conway very early on acknowledges that much of the academic and public discussion of the Internet and its role within cyberterrorism and hacktivism, and the wider area of cybercrime, was often conducted within hyperbolic channels, an issue still discussed nearly two decades later (Brantly, 2020; Neufeld, 2020; Shandler and Gomez, 2022). This often involved amplifying the over-reaching practicalities of ICT, often in lack of technical understanding (Brantly, 2020:100), or outright ignoring the realities such technologies have (Neufeld, 2020:3), instead favouring more colourful hypothetical reasonings, or as Conway (2011a; 2014a; 2014b) suggests, a 'hollywoodised' depiction of the phenomenon of cyberterrorism, giving reference to earlier Die Hard movies.

Attempts to recognise the wider complex nature of cybercrime has been varied. For example, the earlier conceptual framework introduced by Wall (2007), advocated for cybercrime to be viewed as a categorical range of criminal activities, offering a more nuanced and multi-dimensional perspective outside previous generalisations. This categorization allows for a more nuanced analysis of cybercrimes to be more comparatively positioned with their kinetic counterparts. Alternatively, Yar and Steinmetz's (2017) adaptable understanding of cybercrime typologies aligns with the dynamic nature of this field, emphasising the need for flexible conceptualised definitions to "future-proof" our understanding. Nonetheless, the difficulty in detecting, interpreting, and researching cyber-crimes persists, underscoring the urgency for improved tracking and data collection mechanisms.

Seebruck's (2015) circumplex model, later extended to recognise cyberterrorism (Hosford, 2021), attempts to offer a more inclusive typology in which to categorise cybercrime actors, by acknowledging the diverse motivations and skills of hackers, while also accounting for the emergence of cyberterrorism as a distinct category, the typology intends to capture the multifaceted nature of cybercrime actors, and often under-researched component of cybercrime research (Franklin et al., 2007; Pastrana at al., 2018). Further attempts such as McQuire and Dowling's (2013) categorization of cyber-enabled and cyber-dependent crimes, sees use to provide a valuable framework and reinforce cybercrime and cyber-enabled crimes to examine the role of ICT in illegal activities, and evaluate distinctions between both practices, providing avenues for specialisation. Approaches towards a bilinear perspective that distinguishes between crimes that use ICT to enhance criminal activities and those that are fundamentally

dependent on it, has seen frequent discussion within cyberterrorism literature. Concepts such as “pure” cyberterrorism (Gordon and Ford, 2002), and “cyber-enabled” terrorism (Jangada Correia, 2022) illustrate cyberterrorism's long academic history of researcher’s efforts to distinguish the phenomenon from its more widely researched counterpart, terrorism. However, such attempts are not equally seen to distinguish the phenomenon from concepts that share a similar cyber-based genus, more specifically; hacktivism (Kenney, 2015)., with many researchers often blurring both conceptual understandings, often discussed along equal lines (Baldi et al., 2003; Kenney, 2015; Yar and Steinmetz, 2019), making distinguished research on either, or both difficult.

8.2 The Health of Cyberterrorism and Hacktivism Research

The trajectory of cyberterrorism and hacktivism research to date has been a labyrinthine journey, navigating challenges stemming from the absence of dedicated platforms for consistent scholarly discourse, and a significant fragmentation of knowledge-cohesion. Unlike their more established counterparts in terrorism and organised crime studies (see Schmid, 2004; von Lampe, 2015; Symeonidou-Kastanidou, 2007), cyberterrorism and hacktivism research remains in their formative stages, lacking dedicated journals, conferences, and academic curricula. This nascent state has given rise to a dearth of empirical quantitative research and an enduring definitional debate mirroring issues encountered in broader criminological domains (see Gordon and Ford, 2002; Conway, 2002; Berner, 2003; Foltz, 2004; Gorge, 2007; Smith, 2015).

In this study, a bibliometric evaluation of the literature was used as a means of mapping the intellectual contours of cyberterrorism and hacktivism research. In approach to the first aim of gaining insight into the academic development and status of cyberterrorism and hacktivism and answering how the academic development of cyberterrorism and hacktivism research evolved over time, an examination of 126 high-impact articles unveiled an intriguing demographic, and geographical distribution. Despite being an inherently transnational phenomena, the predominant corpus of research studied emanates from male-dominated regions in the global north, with the United States and the United Kingdom at the forefront. This limited perspective forms a critical challenge in gaining a comprehensive understanding of these globally tied phenomena. In alignment with Morrison's (2022:1525) remarks on the comprehensive evaluation of terrorism research, it is imperative to incorporate a range of perspectives and voices from diverse disciplines, demographics, regions, and genders. This inclusive approach should aim for greater unity to enhance both the depth and breadth of our understanding, with the intention of being mirrored in upcoming research initiatives.

Collaborative endeavours, a cornerstone of robust academic inquiry (Fisher et al., 1998; Hosford et al., 2021, Smith et al., 2023), present another facet of concern within the cyberterrorism and hacktivism research landscape. Out of 146 individual authors identified within the sample of 126 publications, only 11% (16) of authors provided more than one contribution towards the collection, reflecting potential dissemination challenges and sustained collaborative, and consistent high-impact publication outputs. This trend echoes the earlier challenges faced in broader terrorism (Silke 2001; 2004; 2008) and organised crime research (Hosford et al., 2021). Equally concerning, the presence of a

robust transnational authorship collaboration when discussing such globally interlinked phenomena, a potential wellspring of enriched perspectives, remains absent amongst highly cited researchers within the domain. The absence of international collaboration is disheartening and mirrors a broader issue observed in cybercrime studies within criminology. Payne and Hadzhidimova's (2020) study indicate that among 201 criminologists investigating cybercrime, a mere 12.5% (25 researchers) engaged in international collaboration. This prompts Payne and Hadzhidimova to question whether "cyber" criminologists have ventured across international borders in their research, highlighting a deficiency in cross-cultural studies or awareness within the field of cybercrime research (Payne and Hadzhidimova, 2020:87).

Returning to the earlier implied empirical deficit found within cybercrime and hacktivism research, the recurrence of a prevailing reliance on secondary media-based data sources such as the "Washington Post", "New York Times", and "the Guardian" was a prominent theme within the research, of which, like cybercrime research, is often explored within exaggerated channels that depict "cyber-doom" scenarios (Brantly, 2020; Neufeld, 2020; Shandler and Gomez, 2022) described by Lawson (2013) and Lawson et al. (2016) as apocalyptic depictions of hackers causing significant physical destructions and harm. It is not uncommon to see the use of media reports within crime-related research. For example, a systematic analysis of organised crime research output identified news and media as the third most used data source (Windle and Silke, 2019). However, within the study of cyberterrorism and hacktivism, this source is considered a main and often over-relied-upon repository of data for cyberterrorism and hacktivism research. Notably, pre-9/11 terrorism research extensively depended on data sourced from media outlets and

media-derived databases, raising concerns about the limited detail and uncertain accuracy of secondary sources like news articles (Silke, 2006:80), a concern later echoed by Schuurman (2018), with Woodward et al., (2016) suggesting criminological research in general has long developed an overarching trend toward an over-reliance on secondary data sources, despite criminology's shift toward quantitative analysis over qualitative approaches, as emphasised by Nelson et al. (2014).

The bibliographic synthesis of key authors within the diverse sample of 126 publications distilled through a compare and contrast of their use within publications (Creswell and Plano Clark, 2007:62) has seen cyberterrorism and hacktivism research develop into four interconnected groups, based on a rich cohort of researchers of various disciplines: "cyberterrorism," "hacktivism," "ICT Security and Infrastructure," and "cyber-criminology". For publications focusing on *cyberterrorism*, the discourse revolves around its conceptualization as a method of terrorism, encompassing both traditional and emerging forms, with incisive critiques on the lack of empirical research methodologies within the domain (Conway, 2002; Berner, 2003; Foltz, 2004; Gorge, 2007; Smith, 2015). *Hacktivism*, on the other hand, often focuses on theoretical knowledge, exploring the myriads of sociological, philosophical, and ideological motivations underpinning hacking activities, particularly focusing on the preservation of freedom of information and privacy concerns (Carducci, 2006; Sorell, 2015; McCarthy, 2015). *ICT Security and Infrastructure* emerged as a dominant topic, centering on the risk of ICT as a potent tool in offensive actions by state or non-state actors, with far-reaching implications for national and international security, and enterprise operations (Giacomello, 2004; Jarvis et al., 2016a; Matusitz and Breen, 2011; Mott, 2016; Shad, 2019; Sieber, 2006). However,

the speculative nature of many of these scenarios limits their utility (Jarvis, Macdonald, and Whiting, 2016a; Mott, 2016; Shad, 2019). Lastly, cyber-criminology, although relatively niche in comparison, was largely composed of research by Holt (2007; 2010) and colleagues (Holt et al., 2010) exploring the phenomenon alongside theoretical frameworks such as routine activity theory (see Cohen and Felson, 1979), and social learning (see Bandura, 1969), specifically tying cyberterrorism to more familiar criminological concepts.

8.3 The Conceptual Comparison of Cyberterrorism and Hacktivism

To satisfy the aim of identifying key definitional characteristics within definitions of cyberterrorism and hacktivism. A content analysis employing a taxonomic framework (see Al Mazari et al., 2015; Veerasamy et al., 2012; Plotnek and Slay, 2021) was conducted to provide a nuanced distributional analysis of terms within six pivotal classifications: actor, effect, intent, motive, means, and target, across the temporal span of twenty years (2000 to 2020). The comprehensive findings unveil the dynamic evolution of cyberterrorism and hacktivism definitions throughout the past two decades (2000-2020), shedding light on the focal points of research within each classification over time.

The dominant consensus of both cyberterrorism and hacktivism definitions within the literature studies primarily defined those who engage in such a phenomenon as having an advanced assortment of ICT skills, such as hackers or hacktivists. Over time, hacktivism definitions have expanded to encompass a broader range of event-driven terminology

associated with specific groups such as “lulzsec,” “antisec,” “cult of dead cow,” and “electrohippies” (Krapp, 2005) and decentralised collective “anonymous” (Coleman, 2015). However, the same cannot be said for definitions of cyberterrorism, which, due to a lack of notable case-studies in absence of empirical data in which to base further knowledge from, researchers often had limited terms to discuss the evolving nature of the phenomenon and define its actors. When discussing the effects of such acts, the research further illuminates nuanced conceptual distinctions between both, bringing further attention towards cyberterrorism’s often more ambiguous terminology in the absences of empirical evidence, associating the phenomenon with more severe and destructive effects, lending further applicability to Lawson’s (2013) earlier concerns of the phenomenon being framed as “cyber-doom”. To elaborate, Lawson brings attention to the use of superficial scenarios by news media, expert commentators, and policymakers when discussing topics such as cyberterrorism (Lawson et al., 2016), a usage noted frequently within scholarly work (Conway, 2008a; 2008b; Lawson, 2013; Weimann, 2005). This ambiguity does not similarly appear within definitions of hacktivism, with the terminology concerning events using the defined actors to centre the phenomenon on disruption and communication-based actions that draw attention towards their issues. These contrasting comparisons highlight the importance of primary case-driven data in which to position cyberterrorism and hacktivism actors, and the effects they cause, making cohesive and collaborative understandings of the phenomena, more specifically “cyberterrorism” more challenging for researchers. However, simply bringing attention to the lack of primary data and willing such change into existence is insufficient, as when looking at the “lack of “data in which to infer from more broadly, the suggestion of such insufficiency of data within the domain is misguided.

As the domain of cybercrime expands, and further recognising the interdisciplinary value of the domain, future research will reflect this. For example, the issue of limited primary data within the cyberterrorism and hacktivism domain is not in direct reference to the non-existence of data. In fact, cybercrime is entrenched in data, but as Holt, Freilich, and Chermak (2017:3) recognises, cybercrime research (and by virtue; cyberterrorism and hacktivism research), lacks a "common language", as social scientists often lack the expertise to interpret such data (Bossler, 2017:51), making collaboration with those in disciplines such as computer science difficult, as researchers in such domains often don't focus on the "human" element of cybercrime (Bossler, 2017:52). Thus, the issue may not be lack of data, but instead a lack of shared collaborative knowledge.

8.4 Moving the Needle Forward Towards More Cohesive Research

A prominent concern identified in this study is the dearth of cohesive and collaborative publications within cyberterrorism and hacktivism research authors with high impact publications, as shown through the analysis of bibliographic data (see section 5.2.1 Basic Analysis). In absence of specialised platforms such as dedicated journals, and conferences for ongoing scholarly discussion, research pertaining to cyberterrorism and hacktivism has become fragmented, exacerbating the blurring of conceptual distinctions between both phenomena (Baldi et al., 2003; Kenney, 2015; Yar and Steinmetz, 2019). The earlier findings and discussion demonstrate that these issues are multifaceted and overlapping, not caused by any singular factor or combination of researchers or their efforts, and that

although a conceptual blurring does exist concerning techno-centric factors, so too do significant of behavioural and motivational distinctions warranting further evaluation. To foster future, more collaborative and promote cross-cultural cyberterrorism and hacktivism research, this thesis developed an ontological framework to record cyber-disruptive event details that can include ideologically motivated characteristics as seen in earlier definitions of cyberterrorism and hacktivism.

Ontologies provide formal representations of shared concepts within a standardised framework (Gruber, 1993:199). These shared concepts support efforts towards what Donalds and Osei-Bryson (2019:415) describes as a "common language," providing opportunities for interdisciplinary research and further collaboration as researchers have a shared and accessible knowledge framework in which to operate from. Like Donalds and Osei-Bryson (2014; 2019) use of ontologies within cybercrime research, ontologies provide a means to promote more cohesive classification of event details (artefacts) and reduce the risk of fragmentation. Using the earlier taxonomic framework (see section 5.3.3 Synthesising the Taxonomy) and findings from the content analysis of cyberterrorism and hacktivism definitions, this ontology provided the necessary terminology to capture and code potential ideologically motivated disruptive cyber-events, and their encompassing events. Built using the open-source ontological development package Protégé (Musen, 2015), two examples were used to evaluate the ontological framework. Firstly, the cyberattack towards the Health Service Executive (HSE) of Ireland was evaluated due to its significance as a critical public infrastructure. Second, the 2014 Sony Pictures Hack is chosen due to its strong ideological pertinent by the "Guardians of Peace" long assumed to be state funded hackers by the North Korean

government (see Haggard and Lindsay, 2015), with the ontology demonstrating its flexibility in capturing such events in similar detail. Both demonstrations illustrated the ontologies capability to capture and map significant criteria using the six defined categories developed from the taxonomy (actor, effect, intent, means, motive, and target), providing a wealth of information that is easily accessible, providing researchers access to further information as the ontological framework and database grows.

This ontological framework, unlike earlier use cases (Donalds and Osei-Bryson, 2019; Veerasamy et al., 2012) is not intended to remain static, and recognises the domain's fluidity (Dahan, 2013; Goode, 2015; and Klein, 2015) within an ever-changing environment of techno-centric development. Thus, this ontology is intended to be similarly fluid and easy to use for non-techno-centric researchers and be added too by current and future researchers alike as a potential resource for researchers to engage in cohesive and potentially collaborative research within an open-science platform. Equally, such as Hosford (2021) modified an earlier typology of hacker motivations and skills (see Rogers, 2006; Seebruck, 2015), the ontological framework should be similarly seen as "upgradable", adapting to future developments in the domain, and modified to further extend its potential utility for researchers, an open-source framework if to compare to earlier hacker cultures (see 3.2 Hacking as Subcultures).

8.4.1 Future Directions

The dynamic nature of cyberterrorism and hacktivism necessitates continuous refinement of definitions and conceptual frameworks. The ontological framework developed in this thesis provides a starting point for capturing and classifying event details. As Silke

(2001:12) notes, the process of research can place a "relatively heavy burden on the researcher", this is only furthered by the need to independently collect data and build databases for future analysis, a concept James Lynch (2018) terms "the entrepreneur model", with researchers in criminology constructing datasets, whether or not they receive funding, and use these datasets to investigate a specific question or set of questions that shapes their research priorities. This data is often locked away, protected by researchers to use in support of establishing their careers in an increasingly competitive space. There are limited (if any) motivations to share data with other researchers unless there is an opportunity to associate names and credit with the shared information (Lynch, 2018:444).

Thus, researchers both in early career and established, should be encouraged to actively share, collaborate, and contribute to the development and enhancement of such frameworks to keep pace with the evolving landscape of cyber threats. The dominant corpus of existing research produced in male-dominated global-north regions raises concerns about the comprehensive understanding of globally tied phenomena. Future research should actively seek out and encourage diverse perspectives from different demographics, disciplines, and regions. Incorporating voices from underrepresented groups and regions can enrich the depth and breadth of our understanding of cyberterrorism and hacktivism, moving towards a more inclusive and representative body of knowledge.

In addition, future research initiatives should prioritise the establishment of specialised platforms just as dedicated journals, conferences, and virtual demonstrations to facilitate

ongoing scholarly discourse and collaboration. Additionally, fostering interdisciplinary research collaborations, particularly between social scientists and computer scientists, is essential to bridge the gap in understanding the technical aspects of cybercrime. Initiatives to establish a common language within the field, as suggested by Holt, Freilich, and Chermak (2017), should be pursued to facilitate collaboration and interpretation of diverse datasets.

In conclusion, future research on cyberterrorism and hacktivism should strive towards the development of a core journal in which to function as catalyst for collaborative, interdisciplinary, and inclusive approaches while embracing evolving definitions and conceptual frameworks. By addressing these aspects, the field can advance towards a more cohesive, nuanced, and globally informed understanding of cyber threats and ideologically motivated uses of digital disruption.

References

Abrahms, M. (2012) The political effectiveness of terrorism revisited, *Comparative Political Studies*. 45, 3, 366–93.

Abramson, B. (2005) *Digital phoenix : why the information economy collapsed and how it will rise again*. [Online]. Cambridge, Mass.: MIT Press.

Acedo, F.J., Barroso, C., Casanueva, C. and Galán, J.L. (2006) Co-authorship in management and organizational studies: An empirical and network analysis, *Journal of Management Studies*. 43, 5, 957–83.

Addicott, J.F. (2007) The emerging threat of cyberterrorism, *NATO SECURITY THROUGH SCIENCE SERIES E*.

Addley, E. and Halliday, J. (2010) Operation Payback cripples MasterCard site in revenge for WikiLeaks ban. *The Guardian*. 8 December.

Agozino, B. and Pfohl, S. (2003) *Counter-colonial criminology: A critique of imperialist reason*. [Online]. Pluto Press.

Ahmed, Y. and Lynch, O. (2021) Terrorism Studies and the Far Right – The State of Play, *Studies in Conflict & Terrorism*. 1–21.

Akhgar, B., Chorąś, M., Brewster, B., Bosco, F. (2016) Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism, *and Cyberterrorism*.

Al Mazari, A., Anjariny, A.H., Habib, S.A. and Nyakwende, E. (2015) Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies, *International Journal of Cyber Warfare and Terrorism*. 6, 1, 1–12.

Alalehto, T.I. and Persson, O. (2013) The Sutherland tradition in criminology: a bibliometric story, *Criminal Justice Studies*. 26, 1, 1–18.

Alexopoulou, S. and Pavli, A. (2019) ‘Beneath This Mask There is More Than Flesh, Beneath This Mask There is an Idea’: Anonymous as the (Super)heroes of the Internet?, *International Journal for the Semiotics of Law*.

Al-khateeb, S., Conlan, K.J., Agarwal, N., Baggili, I. and Breitinger, F. (2016) Exploring Deviant Hacker Networks (DHN) on Social Media Platforms, *Journal of Digital Forensics Security And Law*. 11, 2, SI, 7–20.

Amutuhaire, T. (2022) The Reality of the 'Publish or Perish' Concept, Perspectives from the Global South, *Publishing Research Quarterly*. 38, 2, 281–94.

Andersen, H., Barker, P. and Chen, X. (2006) *The cognitive structure of scientific revolutions*. [Online]. Cambridge University Press.

Anderson, M.S., Ronning, E.A., DeVries, R. and Martinson, B.C. (2010) Extending the Mertonian norms: Scientists' subscription to norms of research, *The Journal of higher education*. 81, 3, 366.

Andress, J. and Winterfeld, S. (2014) Cyber Threatscape. In Andress, J. and Winterfeld, S. (eds.) *Cyber Warfare (Second Edition)*. [Online]. Boston: Syngress. pp. 19–34.

Argomaniz, J. and Lynch, O. (2018) Introduction to the Special Issue: The Complexity of Terrorism—Victims, Perpetrators and Radicalization, *Studies in Conflict & Terrorism*. 41, 7, 491–506.

Aria, M. and Cuccurullo, C. (2017) bibliometrix: An R-tool for comprehensive science mapping analysis, *Journal of Informetrics*. 11, 4, 959–75.

Arksey, H. and O'Malley, L. (2005) Scoping studies: towards a methodological framework, *International Journal of Social Research Methodology*. 8, 1, 19–32.

Asal, V., Mauslein, J., Murdie, A., Young, J., Cousins, K. and Bronk, C. (2016) Repression, Education, and Politically Motivated Cyberattacks, *Journal of Global Security Studies*. 1, 3, 235–47.

Asare, S., Mitchell, R. and Rose, P. (2021) How Accessible are Journal Articles on Education Written by Sub-Saharan Africa-based Researchers?, *Development and Change*. 52, 3, 661–9.

Asenbaum, H. (2018) Cyborg activism: Exploring the reconfigurations of democratic subjectivity in Anonymous, *New Media & Society*. 20, 4, 1543–63.

Atwan, A.B. (2008) *The secret history of al Qaeda*. University of California Press.

Auty, C. (2004) Political hacktivism: tool of the underdog or scourge of cyberspace?, *Aslib Proceedings*. 56, 4, 212–21.

Awan, I. (2014) *Debating the Term Cyber-Terrorism: Issues and Problems* 14.

Awan, I. (2017) Cyber-Extremism: Isis and the Power of Social Media, *Society*. 54, 2, 138–49.

Ayres, N. and Maglaras, L.A. (2016) Cyberterrorism targeting the general public through social media, *Security and Communication Networks*. 9, 15, 2864–75.

Baele, S.J., Sterck, O.C., Slingeneyer, T. and Lits, G.P. (2019) What Does the "Terrorist" Label Really Do? Measuring and Explaining the Effects of the "Terrorist" and "Islamist" Categories, *Studies in Conflict & Terrorism*. 42, 5, 520–40.

Bahoo, S., Alon, I. and Floreani, J. (2021) Corruption in economics: a bibliometric analysis and research agenda, *Applied Economics Letters*. 28, 7, 565–78.

Bailey, K.D. (1994) *Typologies and Taxonomies: An Introduction to Classification Techniques*. SAGE.

Baker, T. and McKenzie, R. (2001) Cyberterrorism: bytes, not bombs., *Maryland medicine : MM : a publication of MEDCHI, the Maryland State Medical Society*. 2, 4, 44.

Baldi, S., Gelbstein, E. and Kurbalija, J. (2003) Hacktivism, Cyber-Terrorism and Cyberwar, *The Information Society Library, DiploFoundation, Geneva, Switzerland*.

Balietti, S., Mäs, M. and Helbing, D. (2015) On Disciplinary Fragmentation and Scientific Progress, *PLoS ONE*. 10, 3, e0118747.

Bandura, A. (1969) Social-learning theory of identificatory processes, *Handbook of socialization theory and research*. 213,262.

Bastug, M.F., Onat, I. and Guler, A. (2023) Threat Construction and Framing of Cyberterrorism in the US News Media, *International Journal of Cybersecurity Intelligence & Cybercrime*. 6, 1, 29–44.

Baumard, P. and Baumard, P. (2017) A Brief History of Hacking and Cyberdefense, *Cybersecurity in France*. 17–30.

Baxter, L.A. (1991) Content analysis. In *Studying Interpersonal Interaction*. New York, London: The Guilford Press. pp. 239–54.

Becher, T. and Trowler, P. (2001) *Academic tribes and territories*. [Online]. McGraw-Hill Education (UK).

Beck, C. (2016) Web of resistance: Deleuzian digital space and hacktivism, *Journal for Cultural Research*. 20, 4, 334–49.

Becker, H.S. (2008) 20012. *Outsiders*. Simon and Schuster.

Bell, S.J. (2004) The infodiet: how libraries can offer an appetizing alternative to Google, *The Chronicle of Higher Education*. 50, 24, B15.

Berger, P.L. (1963) *Invitation to sociology: A humanistic perspective*. Open Road Media.

Berner, S. (2003) Cyber-terrorism: Reality or paranoia?, *SA Journal of Information Management*.

Bessani, A.N., Sousa, P., Correia, M., Neves, N.F. and Verissimo, P. (2008) The Crutial Way of Critical Infrastructure Protection, *IEEE Security & Privacy*. 6, 6, 44–51.

Bhattacharya, J. and Packalen, M. (2020) *Stagnation and Scientific Incentives*. [Online]. p.w26752.

Biesenthal, C. and Wilden, R. (2014) Multi-level project governance: Trends and opportunities, *International journal of project management*. 32, 8, 1291–308.

Bjorgo, T. and Horgan, J.G. (2008) *Leaving terrorism behind: Individual and collective disengagement*. [Online]. Routledge.

Blagg, H. and Anthony, T. (2019) *Decolonising Criminology: Imagining Justice in a Postcolonial World*. [Online]. London: Palgrave Macmillan UK.

Bodó, B. (2014) Hacktivism 1-2-3: How privacy enhancing technologies change the face of anonymous hacktivism, *Internet Policy Review*. 3, 4.

Boghossian, P. (2006) *Fear of Knowledge. Against Relativism and Constructivism. Oxford (Clarendon Press) 2006.*

Booth, T. and Andersson, K. (2017) *Critical infrastructure network DDoS defense, via cognitive learning*. In 2017 IEEE. pp. 1–6.

Bornmann, L. and Daniel, H. (2008) What do citation counts measure? A review of studies on citing behavior, *Journal of Documentation*. 64, 1, 45–80.

Bossler, A.M. (2017) Need for Debate on the Implications of Honeypot Data for Restrictive Deterrence Policies in Cyberspace, *Criminology & Public Policy*. 16, 3, 681–8.

Bossler, A.M. (2021) Neutralizing Cyber Attacks: Techniques of Neutralization and Willingness to Commit Cyber Attacks, *American Journal of Criminal Justice*. 46, 6, 911–34.

Bossler, A.M. and Berenblum, T. (2019) Introduction: new directions in cybercrime research, *Journal of Crime and Justice*. 42, 5, 495–9.

Boys, J.D. (2018) The Clinton administration's development and implementation of cybersecurity strategy (1993-2001), *Intelligence and National Security*. 33, 5, 755–70.

Brands, J. and Van Doorn, J. (2022) The measurement, intensity and determinants of fear of cybercrime: A systematic review, *Computers in Human Behavior*. 127,107082.

Brantly, A. (2020) Beyond Hyperbole, *The Cyber Defense Review*. 5, 3, 99–120.

Brenner, S. (2002) *Cyberterrorism: How Real is the Threat?*. 3. [Online]. United States Institute of Peace.

Brenner, S.W. (2004) *Cybercrime Metrics: Old Wine, New Bottles?* 9, 13, 54.

Brenner, S.W. (2006) Cybercrime, cyberterrorism and cyberwarfare, *Revue Internationale de Droit Penal*. 77, 3, 453–71.

Brenner, S.W. (2012) Cyber-threats and the limits of bureaucratic control, *Minnesota Journal of Law, Science and Technology*.

Brophy, J. and Bawden, D. (2005) Is Google enough? Comparison of an internet search engine with academic library resources, *Aslib Proceedings*. 57, 6, 498–512.

Broucek, V. and Turner, P. (2013) Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective, *Journal of Computer Virology and Hacking Techniques*. 9, 1, 27–33.

Brunst, P.W. (2010) Terrorism and the internet: New threats posed by cyberterrorism and terrorist use of the internet, *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications*. 51–78.

von Busch, O. (2015) 00000. *Hacktivism as Design Research Method*. Rodgers, P.A. and Yee, J. (eds.). Abingdon: Routledge.

Buzan, B. (2004) A Reductionist, Idealistic Notion that Adds Little Analytical Value, *Security Dialogue*. 35, 3, 369–70.

Caldwell, T. (2011) Ethical hackers: putting on the white hat, *Network Security*. 2011, 7, 10–3.

Carducci, V. (2006) Culture Jamming: A Sociological Perspective, *Journal of Consumer Culture*. 6, 1, 116–38.

Carrington, K., Hogg, R., Scott, J. and Sozzo, M. (2018) Criminology, Southern Theory and Cognitive Justice. In Carrington, K., Hogg, R., Scott, J., and Sozzo, M. (eds.) *The Palgrave Handbook of Criminology and the Global South*. [Online]. Cham: Springer International Publishing. pp. 3–17.

Carroll, P. and Windle, J. (2018) Cyber as an enabler of terrorism financing, now and in the future, *Journal of Policing, Intelligence and Counter Terrorism*. 13, 3, 285–300.

Cassim, F. (2012) Addressing the spectre of cyber terrorism: a comparative perspective, *Potchefstroom Electronic Law Journal/Potchefstroomse …*.

Castells, M. (2014) The impact of the internet on society: A Global Perspective, *Open Mind, BBVA*. 132–47.

Castle, N. (2000) Internet Art and Radicalism in the Digital Culture Industry, *Retrieved from Lulu website: http://video. lulu. com/items/volume_1/89000/89324/2/preview/netart_preview. pdf*.

Caswell, B., Beale, J. and Baker, A. (2007) *Snort intrusion detection and prevention toolkit*. Syngress.

Cavelty, M.D. and Van Der Vlugt, R.A. (2015) A Tale of Two Cities: Or How the Wrong Metaphors Lead to less Security International Engagement on Cyber V: Forum: Critical Infrastructure, *Georgetown Journal of International Affairs*. 16, 3, 21–9.

Chagankerian, A. (2013) The Delegitimizing Power of the 'Terrorism' Label. *E-International Relations*. [Online].

Chakrabarty, D. (2008) *Provincializing Europe: postcolonial thought and historical difference-New edition*. Princeton University Press.

Chen, H., Reid, E., Sinai, J., Silke, A. and Ganor, B. (2008) *Terrorism informatics: Knowledge management and data mining for homeland security*. Springer Science & Business Media.

Chen, Peter.Pin.Shan. (1976) The entity-relationship model—toward a unified view of data, *ACM Transactions on Database Systems*. 1, 1, 9–36.

Chen, T.M. (2014) 00000. *Cyberterrorism after Stuxnet*. [Online]. apps.dtic.mil.

Cheong, M. and Lee, V.C. (2011) A microblogging-based approach to terrorism informatics: Exploration and chronicling civilian sentiment and response to terrorism events via Twitter, *Information Systems Frontiers*. 13,45–59.

Cherry, S. (2010) *How stuxnet is rewriting the cyberterrorism playbook. Computerworld*.

Chertoff, M., Bury, P. and Richterova, D. (2020) Bytes not waves: information communication technologies, global jihadism and counterterrorism, *International Affairs*. 96, 5, 1305–25.

Chesney-Lind, M. and Chagnon, N. (2016) Criminology, Gender, and Race: A Case Study of Privilege in the Academy, *Feminist Criminology*. 11, 4, 311–33.

Cheung, T.M., Lindsay, J.R. and Reveron, D.S. (2015) *China and cybersecurity: espionage, strategy, and politics in the digital domain*. Oxford University Press.

Chiesa, R., Ducci, S. and Ciappi, S. (2009) *Profiling hackers: the science of criminal profiling as applied to the world of hacking*. Boca Raton: Auerbach Publications.

Choo, K.-K.R. (2008) Organised crime groups in cyberspace: a typology, *Trends in Organized Crime*. 11, 3, 270–95.

Choo, K.-K.R. and Smith, R.G. (2008) Criminal Exploitation of Online Systems by Organised Crime Groups, *Asian Journal of Criminology*. 3, 1, 37–59.

Chua, Y.T. and Holt, T.J. (2016) A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors, *Victims & Offenders*. 11, 4, 534–55.

Clem, A., Galwankar, S. and Buck, G. (2003) Health implications of cyber-terrorism, *Prehospital and disaster medicine*.

Cloudflare (n.d.) *What is a distributed denial-of-service (DDoS) attack?*. [Online]. Cloudflare.

Clough, B. and Mungo, P. (1992) *Approaching Zero: Data Crime and the Computer Underworld*. Faber & Faber.

Clough, J. (2015) *Principles of cybercrime*. Cambridge University Press.

Cohan, J.A. (2006) Neccessity, Political Violence and Terrorism, *Stetson Law Review*. 35,79.

Cohen, L.E. and Felson, M. (1979) Social change and crime rate trends: A routine activity approach. In *Classics in environmental criminology*. Routledge. pp. 203–32.

Cohen, S. (2002) 11653. *Folk devils and moral panics: The creation of the mods and rockers*. Psychology Press.

Cohen-Almagor, R. (2017) *Jihad online: how do terrorists use the Internet?* In 2017 Springer. pp. 55–66.

Cohn, E.G. and Farrington, D.P. (2014) Publication Productivity of Criminologists, *Journal of Criminal Justice Education*. 25, 3, 275–303.

Cole, S. (1992) *Making science: Between nature and society*. Harvard University Press.

Coleman, E.G. (2012) Phreaks, hackers, and trolls: The politics of transgression and spectacle, *The social media reader*. 5,99–119.

Coleman, G. (2011) Hacker politics and publics, *Public Culture*. 23, 3, 511–6.

Coleman, G. (2015) *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books.

Coleman, G. (2019) How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing?, *Media Culture & Society*. 41, 4, 565–71.

Coleman, G. and Jandrić, P. (2019) Postdigital Anthropology: Hacks, Hackers, and the Human Condition, *Postdigital Science and Education*. 1, 2, 525–50.

Collin, B.C. (1997) The future of cyberterrorism: Where the physical and virtual worlds converge, *Crime and Justice International*. 13, 2, 15–8.

Collin, B.C. (1998) *Cyberterrorism from virtual darkness: New weapons in a timeless battle*. San Luis: Obispo.

Collin, B.C. (2000) The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge 11th Annual International Symposium on Criminal Justice Issues, *Crime and Justice International*. 12, 1, 15–36.

Collins, S. and McCombie, S. (2012) Stuxnet: the emergence of a new cyber weapon and its implications, *Journal of Policing, Intelligence and Counter Terrorism*. 7, 1, 80–91.

Collyer, F.M. (2018) Global patterns in the publishing of academic knowledge: Global North, global South, *Current Sociology*. 66, 1, 56–73.

Connolly, L.Y. and Wall, D.S. (2019) The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, *Computers & Security*. 87,101568.

Conway, M. (1998) Cyberterrorism : Media Myth or Clear and Present Danger ?, *War and virtual war: the challenges to communities* . 1–11.

Conway, M. (2002a) Reality bytes: cyberterrorism and terrorist 'use' of the Internet, *First Monday*. 7, 11.

Conway, M. (2002b) What is cyberterrorism?, *Current History*.

Conway, M. (2003a) Cyberterrorism: The Story So Far, *Journal of Information Warfare*. 2, 2, 33–42.

Conway, M. (2003b) Hackers as terrorists? Why it doesn't compute, *Computer Fraud and Security*. 2003, 12, 10–3.

Conway, M. (2005) Terrorist web sites, *Media and conflict in the twenty-first century*.

Conway, M. (2006) *Reality bytes : cyberterrorism and terrorist use of the Internet*. thesis. [Online]. Trinity College (Dublin, Ireland). Department of Political Science.

Conway, M. (2007) *Cyberterrorism: Hype and reality*

Conway, M. (2008a) *Media, fear and the hyperreal: the construction of cyberterrorism as the ultimate threat to critical infrastructures*. [Online]. doras.dcu.ie.

Conway, M. (2008b) The media and cyberterrorism: A study in the construction of 'reality, *The politics of securing the homeland …*.

Conway, M. (2011a) Against Cyberterrorism: Why cyber-based terrorist attacks are unlikely to occur, *Communications of the ACM (CACM)*.

Conway, M. (2011b) Privacy and security: Against cyberterrorism, *Communications of the ACM*. 54, 2, 26–8.

Conway, M. (2014a) Reality Check: Assessing the (Un)Likelihood of Cyberterrorism. In Chen, T.M., Jarvis, L., and Macdonald, S. (eds.) *Cyberterrorism*. [Online]. New York, NY: Springer New York. pp. 103–21.

Conway, M. (2014b) What is Cyberterrorism and How Real is the Threat?: A Review of the Academic Literature, 1996–2009, *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*.

Conway, M. (2018) *Is cyberterrorism a real threat? Yes: Why we should start from this assumption*

Cornish, D.B. (1994) *Crimes as scripts*. In 1994 Florida Criminal Justice Executive Institute Tallahassee, FL. pp. 30–45.

Cothren, J., Smith, B.L., Roberts, P. and Damphousse, K.R. (2008) Geospatial and temporal patterns of preparatory conduct among American terrorists, *International Journal of Comparative and Applied Criminal Justice*. 32, 1, 23–41.

Coupland, D. and Faye, J. (2001) Microserfs, *The American Review of Canadian Studies*. 31, 3, 501.

Cowen, T. (2006) Terrorism as theatre: Analysis and policy implications, *Public Choice*. 128, 1–2, 233–44.

Cox, C. (2022) *U.S. banks processed roughly $1.2 billion in ransomware payments in 2021, according to federal report*. [Online]. 1 November 2022. CNBC.

Crane, D. (1977) Social structure in a group of scientists: a test of the "invisible college" hypothesis. In *Social networks*. Elsevier. pp. 161–78.

Creswell, J.W. (2009) *Research design: Qualitative, quantitative, and mixed methods approaches*.

Creswell, J.W. and Clark, V.L.P. (2007) Choosing a Mixed Method Design. In *Designing and Conducting Mixed Methods Research*. SAGE. p.

Creswell, J.W. and Clark, V.L.P. (2017) *Designing and conducting mixed methods research*. Sage publications.

Critical Art Ensemble (1996) Electronic civil disobedience and other unpopular ideas, *Autonomedia*.

Cucari, N., Tutore, I., Montera, R. and Profita, S. (2023) A bibliometric performance analysis of publication productivity in the corporate social responsibility field: Outcomes of SciVal analytics, *Corporate Social Responsibility and Environmental Management*. 30, 1, 1–16.

Dahan, M. (2013) *Hacking for the homeland: Patriotic hackers versus hacktivists* 51–7.

Daly, S.A. and Gerwehr, S. (2006) *Al-Qaida: Terrorist Selection and Recruitment*. [Online].

De Langhe, R. (2017) Towards the discovery of scientific revolutions in scientometric data, *Scientometrics*. 110, 1, 505–19.

De Vries, D.R., Marschall, E.A. and Stein, R.A. (2009) Exploring the Peer Review Process: What is it, Does it Work, and Can it Be Improved?, *Fisheries*. 34, 6, 270–9.

Del Carmen, A. and Bing, R.L. (2000) Academic productivity of African Americans in criminology and criminal justice, *Journal of Criminal Justice Education*. 11, 2, 237–49.

Delmas, C. (2018) Is Hacktivism the New Civil Disobedience?, *Raisons politiques*. 69, 1, 63–81.

Delost, M.E. and Nadder, T.S. (2014) Guidelines for initiating a research agenda: Research design and dissemination of results, *American Society for Clinical Laboratory Science*. 27, 4, 237–44.

Denning, D.E. (2000a) Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, *Computer Security Journal*. 16, 3, 15–35.

Denning, D.E. (2000b) Cyberterrorism: Real or not, *Computer Security Alert*.

Denning, D.E. (2000c) Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives, *Focus on Terrorism*.

Denning, D.E. (2001) Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy, *Networks and netwars: The future of terror, crime …*.

Denning, D.E. (2002a) Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, *Committee on Armed Services, US House of* .

Denning, D.E. (2002b) *Is Cyber Terrorism Coming?*. apps.dtic.mil.

Deseriis, M. (2017) Hacktivism: On the Use of Botnets in Cyberattacks, *Theory, Culture & Society*. 34, 4, 131–52.

Desouza, K.C. and Hensgen, T. (2003) Semiotic emergent framework to address the reality of cyberterrorism, *Technological Forecasting and Social Change*. 70, 4, 385–96.

Di Salvo, P. (2017) 'Coder,' 'Activist,' 'Hacker': Aaron Swartz in the Italian, UK, US, and Technology Press, *International Journal of Communication*. 11,1149–68.

Digital Shadows (2020) *The Modern Cybercriminal Forum*. [Online]. 2020. Digital Shadows.

DiRenzo, G.J. (1966) Conceptual definition in the behavioral sciences, *Concepts, theory, and explanation in the behavioral sciences*. 6–18.

Dolnik, A. (2011) Conducting Field Research on Terrorism: a Brief Primer, *Perspectives on Terrorism*. 5, 2, 3–35.

Donalds, C. and Osei-Bryson, K.-M. (2014) *A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction* 13.

Donalds, C. and Osei-Bryson, K.-M. (2019) Toward a cybercrime classification ontology: A knowledge-based approach, *Computers in Human Behavior*. 92,403–18.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N. and Lim, W.M. (2021) How to conduct a bibliometric analysis: An overview and guidelines, *Journal of Business Research*. 133,285–96.

Dooley, B.D. and Goodison, S.E. (2020) Falsification by atrophy: The Kuhnian process of rejecting theory in US criminology, *The British Journal of Criminology*. 60, 1, 24–44.

Douai, A. (2015) Technology and terrorism: Media symbiosis and the 'dark side' of the web. In Cantoni, L. and Danowski, J.A. (eds.) *Communication and Technology*. Berlin 11: De Gruyter Mouton. pp. 439–53.

Drake, C.J.M. (2007) The role of ideology in terrorists' target selection, *Terrorism and Political Violence*. 10, 2, 53–85.

Drisko, J.W. and Maschi, T. (2016) *Content analysis*. Pocket guides to social work research methods. New York: Oxford University Press.

Drmola, J., Bastl, M. and Mares, M. (2015) Modeling Hacktivism Using System Dynamics, *Journal of Applied Security Research*. 10, 2, 238–48.

Duff, L. and Gardiner, S. (1996) Computer Crime in the Global Village: Strategies for Control and Regulation — in Defence of the Hacker, *International Journal of the Sociology of Law*. 24, 2, 211–28.

van Eck, N.J. and Waltman, L. (2014) Visualizing Bibliometric Networks. In Ding, Y., Rousseau, R., and Wolfram, D. (eds.) *Measuring Scholarly Impact*. [Online]. Cham: Springer International Publishing. pp. 285–320.

Edyvane, D. and Kulenovic, E. (2017) Disruptive Disobedience, *Journal of Politics*. 79, 4, 1359–71.

Ellis, J., Fisher, D., Longstaff, T., Pesante, L. and Pethia, R. (1997) Report to the President's Commission on critical infrastructure protection, *Electronic Version] http://www. cert. org/pres_comm/cert. rpcci. ex. sum. html# edu (Accessed on April 1, 2008)*.

Elo, S. and Kyngäs, H. (2008) The qualitative content analysis process, *Journal of Advanced Nursing*. 62, 1, 107–15.

Embar-Seddon, A. (2002) Cyberterrorism: Are We Under Siege?, *American Behavioral Scientist*. 45, 6, 1033–43.

Emery, N.E. (2005) The Myth of Cyberterrorism, *Journal of Information Warfare*. 4, 1, 80–9.

Enslin, P. and Hedge, N. (2018) On Peer Review as the 'Gold Standard' in Measuring Research Excellence: From Secrecy to Openness?, *Journal of Philosophy of Education*. 52, 3, 379–96.

Epiphaniou, G., French, T. and Maple, C. (2014) The DarkWeb: Cyber-Security Intelligence Gathering Opportunities, Risks and Rewards, *Journal of Computing and Information Technology*. 22, LISS 2013, 21.

Eroukhmanoff, C. (2017) Securitisation theory. In *International relations theory*. 104: E-International Relations Publishing. p.

Fahmy, C. and Young, J.T.N. (2017) Gender Inequality and Knowledge Production in Criminology and Criminal Justice, *Journal of Criminal Justice Education*. 28, 2, 285–305.

Farmer, F. (2022) *Cybercrime Vs Hacktivism: Do we Need a Differentiated Regulatory Approach?* Ph.D. [Online]. England: University of Exeter (United Kingdom).

Felson, M. (2000) The routine activity approach as a general crime theory, *Criminological perspectives: essential readings*. 2,160–7.

Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M. and Inácio, P.R.M. (2014) Security issues in cloud environments: a survey, *International Journal of Information Security*. 13, 2, 113–70.

Field, A. (2009) The 'New Terrorism': Revolution or Evolution?, *Political studies review*. 7, 2, 195–207.

Fierke, K.M. (2015) *Critical approaches to international security*. John Wiley & Sons.

Fine, G.A. and Sandstrom, K. (1993) Ideology in Action: A Pragmatic Approach to a Contested Concept, *Sociological Theory*. 11, 1, 21.

Finklea, K.M. and Theohary, C.A. (2012) *Cybercrime: Conceptual Issues for Congress and US Law Enforcement*

Firinci Orman, T. (2016) " Paradigm " as a Central Concept in Thomas Kuhn's Thought, *International Journal of Humanities and Social Sciences*. 6,.

Fisher, B.S., Vander Ven, T.M., Cobane, C.T., Cullen, F.T. and Williams, N. (1998) Trends in multiple-authored articles in criminology and criminal justice: A comparative analysis, *Journal of Criminal Justice Education*. 9, 1, 19–38.

Fitri, N. (2011) Democracy discourses through the Internet communication: Understanding the hacktivism for the global changing, *Online Journal of Communication and Media Technologies*. 1, 2, 1–20.

Fletcher, G.P. (2006) The indefinable concept of terrorism, *Journal of international criminal justice*. 4, 5, 894–911.

Foltz, C.B. (2004) Cyberterrorism, computer crime, and reality, *Information Management and Computer Security*. 12, 2, 154–66.

Fowler, K. (2016) An Overview of Data Breaches. In Fowler, K. (ed.) *Data Breach Preparation and Response*. [Online]. Boston: Syngress. pp. 1–26.

Franklin, J., Paxson, V., Perrig, A. and Savage, S. (2007) An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of the 14th ACM conference on Computer and communications security*. [Online]. 28 October 2007 Alexandria Virginia USA: ACM. pp. 375–88.

Frantz, A. and Franco, M. (2005) A semantic web application for the air tasking order. In *10th International Command And Control Research And Technology Symposium Experimentation Track*. [Online]. 2005 p.

Freshwater, D., Sherwood, G. and Drury, V. (2006) International research collaboration: Issues, benefits and challenges of the global network, *Journal of Research in Nursing*. 11, 4, 295–303.

Frumkin, L.A., Morrison, J.F. and Silke, A. (2023) *A Research Agenda for Terrorism Studies*. Edward Elgar Publishing.

Fuchs, C. (2009) Information and Communication Technologies and Society, *European Journal of Communication*. 24, 1, 69–87.

Fuchs, C. (2013) The Anonymous movement in the context of liberalism and socialism, *Interface: a journal for and about social movements*. 5, 2, 345–76.

Fuentes, M.A. (2015) Performance Constellations: Memory and Event in Digitally Enabled Protests in the Americas, *Text and Performance Quarterly*. 35, 1, 24–42.

Fuller, S. (2001) Discussion note: Is there philosophical life after Kuhn?, *Philosophy of science*. 68, 4, 565–72.

Gaibulloev, K. and Sandler, T. (2019) What we have learned about terrorism since 9/11, *Journal of Economic Literature*. 57, 2, 275–328.

Gallagher, C. and McQuinn, C. (2021) *Dark web 'dump sites' being monitored for HSE data after hack*. [Online]. 18 May 2021. The Irish Times.

Gambetta, D. and Hertog, S. (2007) Engineers of Jihad: The Curious Connection between Violent Extremism and Education, *The American Journal of Islam and Society*. 37,1–2.

Garcia, H. and Belim, C. (2016) 'To be or not to be a cyberterrorist', that is the question!: The political communication of al-Qaeda and Islamic state on social networks, *Trípodos*. 39, 13–34.

Gardner, B. (2014) Threat. In Gardner, B. and Thomas, V. (eds.) *Building an Information Security Awareness Program*. [Online]. Boston: Syngress. pp. 9–13.

Garfield, E. (1955) Citation indexes for science: A new dimension in documentation through association of ideas, *Science*. 122, 3159, 108–11.

Garfield, E. (1972) Citation Analysis as a Tool in Journal Evaluation: Journals can be ranked by frequency and impact of citations for science policy studies., *Science*. 178, 4060, 471–9.

Garfield, E. (2006) On the origins of bibliometrics, *Scientometrics*. 68, 1, 109–33.

Garvey, W.D. and Griffith, B.C. (1979) Scientific communication as a social system, *Communication: The essence of science*. 148–64.

Gaudette, T., Scrivens, R., Davies, G. and Frank, R. (2021) Upvoting extremism: Collective identity formation and the extreme right on Reddit, *New Media & Society*. 23, 12, 3491–508.

Gentner, D. and Collins, A. (1981) Studies of inference from lack of knowledge, *Memory & Cognition*. 9, 4, 434–43.

George, J.J. and Leidner, D.E. (2019) From clicktivism to hacktivism: Understanding digital activism, *Information and Organization*. 29, 3, UNSP 100249.

Gerring, J. (2012) *Social science methodology: A unified framework*. 2nd edition. Cambridge University Press.

Giacomello, G. (2004) Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism, *STUDIES IN CONFLICT & TERRORISM*. 27, 5, 387–408.

Gibbs, J.P. (1989) Conceptualization of terrorism, *American sociological review*. 329–40.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan, J. (2017) Terrorist Use of the Internet by the Numbers, *Criminology & Public Policy*. 16, 1, 99–117.

Glänzel, W. (2012) Bibliometric methods for detecting and analysing emerging research topics, *El Profesional de la Informacion*. 21, 2, 194–201.

Glänzel, W. and Lange, C.D. (2002) *A distributional approach to multinationality measures of international scientific collaboration*

Glänzel, W. and Schoepflin, U. (1994) Little scientometrics, big scientometrics... and beyond?, *Scientometrics*. 30, 2–3, 375–84.

Gofas, A. (2012) *'Old' vs. 'New' Terrorism: What's in a Name?*

Goldman, Z.K., Maruyama, E., Rosenberg, E., Saravalle, E. and Solomon-Strauss, J. (2017) Terrorist use of virtual currencies, *Washington DC: Center for a New American Security, May*. 3,.

Gomez, M.A. and Whyte, C. (2021) Breaking the myth of cyber doom: Securitization and normalization of novel threats, *International Studies Quarterly*. 65, 4, 1137–50.

González-Alcaide, G., Melero-Fuentes, D., Aleixandre-Benavent, R. and Valderrama-Zurián, J.-C. (2013) Productivity and Collaboration in Scientific Publications on Criminology, *Journal of Criminal Justice Education*. 24, 1, 15–37.

Goodchild, J. (2022) *WannaCry 5 years on: Still a top threat*. [Online]. 19 May 2022. CSO Online.

Goode, E. (2004) Is the sociology of deviance still relevant?, *The American Sociologist*. 35, 4, 46–57.

Goode, L. (2015) Anonymous and the Political Ethos of Hacktivism, *Popular Communication*. 13, 1, 74–86.

Goodman, S.E., Kirk, J.C. and Kirk, M.H. (2007) Cyberspace as a medium for terrorists, *TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE*. 74, 2, 193–210.

Goodwin, J. (2005) A Theory of Categorical Terrorism Social Scientific Analyses of Terrorism, *Social Forces*. 84, 4, 2027–46.

Gordon, A. (2004) The Effect of Database and Website Inconstancy on the Terrorism Field's Delineation, *Studies in Conflict & Terrorism*. 27, 2, 79–88.

Gordon, A. (2010) Can terrorism become a scientific discipline? A diagnostic study, *Critical Studies on Terrorism*. 3, 3, 437–58.

Gordon, G. and Neumann, Y. (1979) A Three Facet Model of Scientific Development, *Public Administration Review*. 39, 2, 134–40.

Gordon, S. and Ford, R. (2002) Cyberterrorism?, *Computers & Security*. 21, 7, 636–47.

Gordon, S. and Ford, R. (2006) *On the definition and classification of cybercrime*.

Gorge, M. (2007) Cyberterrorism: hype or reality?, *Computer Fraud and Security*. 2007, 2, 9–12.

Grant, P.R. (1991) Ethnocentrism Between Groups of Unequal Power Under Threat in Intergroup Competition, *The Journal of Social Psychology*. 131, 1, 21–8.

Gray, P.H. and Meister, D.B. (2003) Introduction: fragmentation and integration in knowledge management research, *Information Technology & People*. 16, 3, 259–65.

Greene, A. (2017) Defining Terrorism: One Size Fits All?, *International and Comparative Law Quarterly*. 66, 2, 411–40.

Griffith, B.C. (1974) Mapping the Scientific Literature. In *Perspectives in Information Science*. Springer. pp. 457–81.

Gross, M.L., Canetti, D. and Vashdi, D.R. (2016) The psychological effects of cyber terrorism, *Bulletin of the Atomic Scientists*. 72, 5, 284–91.

Gross, M.L., Canetti, D. and Vashdi, D.R. (2017) Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes, *Journal of Cybersecurity*. 3, 1, SI, 49–58.

Gruber, T. (1993) *What is an Ontology*. [Online].

Guice, J. (1998) Looking Backward and Forward at the Internet, *The Information Society*. 14, 3, 201–11.

Gupta, B.B. and Badve, O.P. (2017) Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment, *Neural Computing and Applications*. 28, 12, 3655–82.

Gusenbauer, M. (2019) Google Scholar to overshadow them all? Comparing the sizes of 12 academic search engines and bibliographic databases, *Scientometrics*. 118, 1, 177–214.

Habib, R. and Afzal, M.T. (2019) Sections-based bibliographic coupling for research paper recommendation, *Scientometrics*. 119, 2, 643–56.

Haggard, S. and Lindsay, J.R. (2015) *North Korea and the Sony hack: Exporting instability through cyberspace*

Haggbloom, S.J., Warnick, R., Warnick, J.E., Jones, V.K., Yarbrough, G.L., Russell, T.M., Borecky, C.M., McGahhey, R., Powell, J.L., Beavers, J. and Monte, E. (2002) The 100 Most Eminent Psychologists of the 20th Century, *Review of General Psychology*. 6, 2, 139–52.

Haghani, M., Kuligowski, E., Rajabifard, A. and Lentini, P. (2022) Fifty years of scholarly research on terrorism: Intellectual progression, structural composition, trends and knowledge gaps of the field, *International Journal of Disaster Risk Reduction*. 68,102714.

Hai-Jew, S. (2015) Action Potentials: Extrapolating an Ideology from the Anonymous Hacker Socio-Political Movement (A Qualitative Meta-Analysis), *Information Science Reference*. 812–69.

Hampson, N.C. (2012) Hacktivism: A new breed of protest in a networked world, *BC Int'l & Comp. L. Rev.* 35,511.

Hansen, J.V., Lowry, P.B., Meservy, R.D. and McDonald, D.M. (2007) Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection, *DECISION SUPPORT SYSTEMS*. 43, 4, 1362–74.

Hansen, L. and Nissenbaum, H. (2009) Digital disaster, cyber security, and the Copenhagen School, *International studies quarterly*. 53, 4, 1155–75.

Harker, J.L. and Saffer, A.J. (2018) Mapping a subfield's sociology of science: A 25-year network and bibliometric analysis of the knowledge construction of sports crisis communication, *Journal of Sport and Social Issues*. 42, 5, 369–92.

Hechter, M. (1978) Group Formation and the Cultural Division of Labor, *American Journal of Sociology*. 84, 2, 293–318.

van Heerden, R.P., Irwin, B., Burke, I.D. and Leenen, L. (2012) A Computer Network Attack Taxonomy and Ontology:, *International Journal of Cyber Warfare and Terrorism*. 2, 3, 12–25.

Hegghammer, T. (2013) The future of terrorism studies, *Talk at Intelligence, National Security, and War*.

Henschke, A. (2021) Terrorism and the internet of things: cyber-terrorism as an emergent threat. In *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Springer International Publishing Cham. pp. 71–87.

Henschke, A., Reed, A., Robbins, S., and Miller, S. (eds.) (2021) *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Advanced Sciences and Technologies for Security Applications. [Online]. Cham: Springer International Publishing.

Hershman, T. (2001) Israel Discusses the 'Inter-fada'. *Wired*. [Online].

Hewitt, S. (2008) *The British War on Terror: Terrorism and Counter-Terrorism on the Home Front Since 9-11*. Continuum.

Himma, K.E. (2007) *Internet security: Hacking, counterhacking, and society*. [Online]. Jones & Bartlett Learning.

Hirsch, P.M. and Levin, D.Z. (1999) Umbrella Advocates Versus Validity Police: A Life-Cycle Model, *Organization Science*. 10, 2, 199–212.

Hitzler, P., Krötzsch, M., Parsia, B., Patel-Schneider, P.F. and Rudolph, S. (2009) OWL 2 web ontology language primer, *W3C recommendation*. 27, 1, 123.

Hodgson, G.M. (2019) Taxonomic definitions in social science, with firms, markets and institutions as case studies, *Journal of Institutional Economics*. 15, 2, 207–33.

Hodgson, J.S. and Tadros, V. (2013) The Impossibility of Defining Terrorism, *New Criminal Law Review: An International and Interdisciplinary Journal*. 16, 3, 494–526.

Hoffman, B. (1999) Terrorism Trends and Prospects, *Countering the new terrorism*.

Hoffman, B. (2006) *Inside Terrorism*. REV-Revised, 2. [Online]. Columbia University Press.

Hoffman, B. (2017) *Inside terrorism*. Columbia university press.

Hogge, B. (2010) *Open Data Study: New Technologies*. [Online].

Holbrook, D. and Horgan, J. (2019) Terrorism and Ideology, *Perspectives on Terrorism*. 13, 6.

Hollinger, R.C. and Lanza-Kaduce, L. (1988) The Process of Criminalization: The Case of Computer Crime Laws*, *Criminology*. 26, 1, 101–26.

Holt, T.J. (2007) Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures, *Deviant behavior*. 28, 2, 171–98.

Holt, T.J. (2010) Examining the role of technology in the formation of deviant subcultures, *Social Science Computer Review*. 28, 4, 466–81.

Holt, T.J. (2012) Exploring the Intersections of Technology, Crime, and Terror, *Terrorism and Political Violence*. 24, 2, 337–54.

Holt, T.J. and Bossler, A.M. (2014) An Assessment of the Current State of Cybercrime Scholarship, *Deviant Behavior*. 35, 1, 20–40.

Holt, T.J., Burruss, G.W. and Bossler, A.M. (2010) Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World, *Journal of Crime and Justice*.

Holt, T.J., Chermak, S.M., Freilich, J.D., Turner, N. and Greene-Colozzi, E. (2022) Assessing Racial and Ethnically Motivated Extremist Cyberattacks Using Open Source Data, *Terrorism and Political Violence*. 0, 0, 1–14.

Holt, T.J., Freilich, J.D. and Chermak, S.M. (2017) Exploring the Subculture of Ideologically Motivated Cyber-Attackers, *Journal of Contemporary Criminal Justice*. 33, 3, 212–33.

Holt, T.J. and Kilger, M. (2012) Examining Willingness to Attack Critical Infrastructure Online and Offline, *Crime & Delinquency*. 58, 5, 798–822.

Holt, T.J., Kilger, M., Chiang, L. and Yang, C.-S. (2016) Exploring the Correlates of Individual Willingness to Engage in Ideologically Motivated Cyberattacks, *Deviant Behavior*. 38, 3, 356–73.

Holt, T.J., Lee, J.R., Freilich, J.D., Chermak, S.M., Bauer, J.M., Shillair, R. and Ross, A. (2020) An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks, *Terrorism and Political Violence*. 34, 7, 1305–20.

Holt, T.J., Stonhouse, M., Freilich, J. and Chermak, S.M. (2019) Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups, *Terrorism and Political Violence*. 1–22.

Homolar, A. and Rodríguez-Merino, P.A. (2019) Making sense of terrorism: a narrative approach to the study of violent events, *Critical Studies on Terrorism*. 12, 4, 561–81.

Hood, W.W. and Wilson, C.S. (2001) *The Literature of Bibliometrics, Scientometrics, and Informetrics*

Horgan, J. (2008) From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism, *The ANNALS of the American Academy of Political and Social Science*. 618, 1, 80–94.

Horgan, J. and Boyle, M.J. (2008) A case against 'Critical Terrorism Studies', *Critical Studies on Terrorism*. 1, 1, 51–64.

Horridge, M. (2011) *A Practical Guide To Building OWL Ontologies Using Prot´eg´e 4 and CO-ODE Tools Edition 1.3* 109.

Horton, J. (1978) Policing the Crisis: Mugging, the State, and Law and Order, Hall, S., Critcher, C., Jefferson, T., Clarke, J., and Roberts, B. (eds.) *Crime and Social Justice*. 12, 59–63.

Hosford, K. (2021) Hacker Generations, Subcultures and Hat Colours: A More Practical Approach to Classification. In *Cybercrime in Action an International Approach to Cybercrime*. 1st edition. [Online]. Ch. 9: Nobel. p.

Hosford, K., Aqil, N., Windle, J., Gundur, R.V. and Allum, F. (2021) Who researches organised crime? A review of organised crime authorship trends (2004–2019), *Trends in Organized Crime*.

Hossová, M. (2018) Fake news and disinformation: Phenomenons of post-factual society, *Media Literacy and Academic Research*. 1, 2, 27–35.

Hout, M.C.V. and Bingham, T. (2013) 'Silk Road', the virtual drug marketplace: A single case study of user experiences, *International Journal of Drug Policy*. 24, 5, 385–91.

Hoyningen-Huene, P. (1993) *Reconstructing scientific revolutions: Thomas S. Kuhn's philosophy of science*. [Online]. University of Chicago Press.

Hua, J. and Bapna, S. (2012) How Can We Deter Cyber Terrorism?, *Information Security Journal: A Global Perspective*. 21, 2, 102–14.

Hua, J., Chen, Y. and Luo, X. (Robert) (2018) Are we ready for cyberterrorist attacks?-Examining the role of individual resilience, *Information and Management*. 55, 7, 928–38.

Huang, R. (2014) RQDA: R-based qualitative data analysis, *R package version 0.2–7*.

Hudson, B. (2008) Difference, diversity and criminology: The cosmopolitan vision, *Theoretical Criminology*. 12, 3, 275–92.

Hughes, B. (2016) *Defying the IRA?: Intimidation, coercion, and communities during the Irish Revolution*. [Online]. Liverpool University Press.

Hummel, K. (2016) *How Terrorists Use Encryption*. [Online]. 16 June 2016. Combating Terrorism Center at West Point.

Hunter, L., Albert, C., Garrett, E. and Rutland, J. (2022) Democracy and cyberconflict: how regime type affects state-sponsored cyberattacks, *Journal of Cyber Policy*. 7,1–23.

Hunton, P. (2009) The growing phenomenon of crime and the internet: A cybercrime execution and analysis model, *Computer Law and Security Review*. 25, 6, 528–35.

Hurley, L.A., Ogier, A.L. and Torvik, V.I. (2013) Deconstructing the collaborative impact: Article and author characteristics that influence citation count, *Proceedings of the American Society for Information Science and Technology*. 50, 1, 1–10.

Ibrahim, S.A. (2019) Regulating cryptocurrencies to combat terrorism-financing and money laundering, *Stratagem*. 2, 1.

Iqbal, M. (2003) Defining cyberterrorism, *J. Marshall J. Computer & Info. L.*

Iqbal, S., Hassan, S.-U., Aljohani, N.R., Alelyani, S., Nawaz, R. and Bornmann, L. (2021) A decade of in-text citation analysis based on natural language processing and machine learning techniques: an overview of empirical studies, *Scientometrics*. 126, 8, 6551–99.

Isenberg, D. (2000) Electronic Pearl Harbor? More hype than threat, *Retrieved May*. 31,2001.

Jackson, R. (2007) Constructing Enemies: 'Islamic Terrorism' in Political and Academic Discourse, *Government and Opposition*. 42, 3, 394–426.

Jackson, R. (2012) Unknown knowns: the subjugated knowledge of terrorism studies, *Critical Studies on Terrorism*. 5, 1, 11–29.

Jackson, R., Smyth, M.B. and Gunning, J. (2009) Critical terrorism studies: A new research agenda. In *Critical Terrorism Studies: A New Research Agenda*. [Online]. p.

Jacobsen, J.T. (2022) Cyberterrorism: Four Reasons for Its Absence—So Far, *Perspectives on terrorism*. 16, 5, 62–72.

Jacobson, M. (2010) Terrorist Financing and the Internet, *Studies in Conflict & Terrorism*. 33, 4, 353–63.

Jaishankar, K. (2018) *Cyber Criminology As An Academic Discipline: History, Contribution And Impact*

Jangada Correia, V. (2022) An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Science*. 3, 1, 84.

Janis, I.L. and Fadner, R.H. (1943) A coefficient of imbalance for content analysis, *Psychometrika*. 8, 2, 105–19.

Jansen, R.S. (2011) Populist mobilization: A new theoretical approach to populism, *Sociological theory*. 29, 2, 75–96.

Jarneving, B. (2007) Bibliographic coupling and its application to research-front and other core documents, *Journal of Informetrics*. 1, 4, 287–307.

Järvinen, P. (2007) Action research is similar to design science, *Quality & quantity*. 41,37–54.

Jarvis, L. and Macdonald, S. (2014) Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon, *Perspectives on Terrorism*. 8, 2, 52–65.

Jarvis, L. and Macdonald, S. (2015a) Responding to cyberterrorism: Options and avenues, *Geo. J. Int'l Aff.*

Jarvis, L. and Macdonald, S. (2015b) What is cyberterrorism? Findings from a survey of researchers, *Terrorism and Political Violence*. 27, 4, 657–78.

Jarvis, L., Macdonald, S. and Nouri, L. (2014) The Cyberterrorism Threat: Findings from a Survey of Researchers, *Studies in Conflict and Terrorism*. 37, 1, 68–90.

Jarvis, L., Macdonald, S. and Whiting, A. (2016a) Analogy and authority in cyberterrorism discourse: An analysis of global news media coverage, *GLOBAL SOCIETY*. 30, 4, 605–23.

Jarvis, L., Macdonald, S. and Whiting, A. (2016b) Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat, *European Journal of International Security*. 2, 1, 64–87.

Jassawalla, A.R. and Sashittal, H.C. (1998) An Examination of Collaboration in High-Technology New Product Development Processes, *Journal of Product Innovation Management*. 15, 3, 237–54.

Jayaswal, V., Yurcik, W. and Doss, D. (2002) *Internet hack back: Counter attacks as self-defense or vigilantism?* In 2002 IEEE. pp. 380–6.

Jewkes, Yvonne, and Majid Yar, Eds. (2013) Jewkes2010. *Handbook of Internet crime.* Willan.

Jick, T.D. (1979) Mixing Qualitative and Quantitative Methods: Triangulation in Action, *Administrative Science Quarterly*. 24, 4, 602–11.

Jin, S. and Yeung, D.S. (2004) *A covariance analysis model for DDoS attack detection*. In 2004 IEEE. pp. 1882–6.

Jones, A. (2005) Cyber terrorism: Fact or fiction, *Computer Fraud & Security*. 2005, 6, 4–7.

Jordan, T. (2001) *Mapping hacktivism: Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) And cyber-wars*

Jordan, T. (2002) *Activism! Direct action, Hacktivism and the future of society*. [Online]. London, UK: Reaktion.

Jordan, T. (2007) Online Direct Action: Hacktivism and Radical Democracy, *Radical democracy and the Internet: interrogating theory and practice*. 73–88.

Jordan, T. (2017) A genealogy of hacking, *Convergence-the International Journal of Research into New Media Technologies*. 23, 5, 528–44.

Jordan, T. and Taylor, P. (1998) A Sociology of Hackers, *The Sociological Review*. 46, 4, 757–80.

Jordan, T. and Taylor, P.A. (2004) *Hacktivism and Cyberwars: Rebels with a cause?* 193.

Juliadotter, N.V. and Choo, K.-K.R. (2015) CATRA: Conceptual cloud attack taxonomy and risk assessment framework. In Ko, R. and Choo, K.-K.R. (eds.) *The Cloud Security Ecosystem*. [Online]. Boston: Syngress. pp. 37–81.

Just, J. (2015) *Jihad 2.0: the impact of social media on the Salafist scene and the nature of terrorism*. Anchor Academic Publishing.

Kalyvas, S.N. (2004) The Paradox of Terrorism in Civil War, *The Journal of Ethics*. 8, 1, 97–138.

Karagiannopoulos, V. (2018a) Contemporary Norms and Law and Hacktivism, *Living with Hacktivism: From Conflict to Symbiosis*. 91–142.

Karagiannopoulos, V. (2018b) *Living With Hacktivism*. [Online]. Cham: Springer International Publishing.

Karystianis, G., Simpson, P., Lukmanjaya, W., Ginnivan, N., Nenadic, G., Buchan, I. and Butler, T. (2023) Automatic Extraction of Research Themes in Epidemiological Criminology From PubMed Abstracts From 1946 to 2020: Text Mining Study, *JMIR Formative Research*. 7, 1, e49721.

Katz, J.S. and Martin, B.R. (1997) What is research collaboration?, *Research Policy*. 26, 1, 1–18.

Kavada, A. (2015) Creating the collective: social media, the Occupy Movement and its constitution as a collective actor, *Information, Communication & Society*. 18, 8, 872–86.

Kelly, B.B. (2012) Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' Can and Should Influence Cybersecurity Reform, *Boston University Law Review*. 92, 5, 1663–711.

Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World, *Orbis*. 59, 1, 111–28.

Kerr, K. (2004) Putting cyberterrorism into context. *Auscert. org*. [Online].

Kessler, M.M. (1963) Bibliographic coupling between scientific papers, *American documentation*. 14, 1, 10–25.

Kharasch, E.D., Avram, M.J., Clark, J.D., Davidson, A.J., Houle, T.T., Levy, J.H., London, M.J., Sessler, D.I. and Vutskits, L. (2021) Peer Review Matters: Research Quality and the Public Trust, *Anesthesiology*. 134, 1, 1–6.

Kilger, M. (2015) Integrating human behavior into the development of future cyberterrorism scenarios, *2015 10th International Conference on Availability* .

King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B. and Sample, C. (2018) Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment, *Frontiers in psychology*. 9,39–39.

Klein, A.G. (2015) Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press, *Communication Monographs*. 82, 3, 379–401.

Klona, M., Menzies, J. and Zutshi, A. (2021) Mapping terrorism in the academic landscape of business field of study: a bibliometric study of the past 30 years, *International Journal of Conflict Management*. 32, 5, 791–825.

Koehler, D. (2017) *Right-Wing Terrorism in the 21st Century*. [Online].

Kokol, P. and Vošner, H.B. (2019) Historical, descriptive and exploratory analysis of application of bibliometrics in nursing research, *Nursing Outlook*. 67, 6, 680–95.

Koops, B.-J. (2010) The Internet and its Opportunities for Cybercrime, *SSRN Electronic Journal*.

Krapp, P. (2005) Terror and Play, or What Was Hacktivism?, *Grey Room*. 21, 70–93.

Krippendorff, K. (1980) Validity in Content Analysis, *Computerstrategien für die Kommunikationsanalyse*. 69–112.

Krippendorff, K. (1989) *Content Analysis*

Krippendorff, K. (2018) *Content analysis: An introduction to its methodology*. Sage publications.

Kristofferson, K., White, K. and Peloza, J. (2020) The Nature of Slacktivism: How the Social Observability of an Initial Act of Token Support Affects Subsequent Prosocial Action (vol 40, pg 1149, 2014), *Journal of Consumer Research*. 46, 5, 1003–1003.

Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R. and Roks, R.A. (2019) Money talks *money laundering choices of organized crime offenders in a digital age*, *Journal of Crime and Justice*. 42, 5, 569–81.

Kuhn, T.S. (1970) *The structure of scientific revolutions*. International encyclopedia of unified science. Foundations of the unity of science, v. 2, no. 2. [2d ed., enl. Chicago: University of Chicago Press.

Kuhn, T.S. (1977) *The Essential Tension: Selected Studies in Scientific Tradition and Change*. [Online]. Chicago, IL: University of Chicago Press.

Kupchik, S. (2022) *Conti's Hacker Manuals: Read, Reviewed & Analyzed*. [Online]. 5 April 2022.

Kutlaca, M., van Zomeren, M. and Epstude, K. (2020) Friends or foes? How activists and non-activists perceive and evaluate each other, Wisneski, D. (ed.) *PLOS ONE*. 15, 4, e0230918.

Kwon, K.H. and Shakarian, J. (2018) Black-Hat Hackers' Crisis Information Processing in the Darknet: A Case Study of Cyber Underground Market Shutdowns. In Wellman, B., Robinson, L., Brienza, C., Chen, W., and Cotten, S.R. (eds.) *Studies in Media and Communications*. [Online]. Emerald Publishing Limited. pp. 113–35.

Kyngäs, H., Mikkonen, K., and Kääriäinen, M. (eds.) (2020) *The Application of Content Analysis in Nursing Science Research*. [Online]. Cham: Springer International Publishing.

von Lampe, K. (2003) Organising the nicotine racket: Patterns of cooperation in the cigarette black market in Germany, *Criminal finances and organising crime in Europe*. 41–66.

von Lampe, K. (2008) Organised crime research in Europe: development and stagnation, *European crime-markets at cross-roads: Extended and extending criminal Europe. Nijmegen: Wolf Legal Publishers*. 17–41.

von Lampe, K. (2015a) *Definitions of organized crime* 1–42.

von Lampe, K. (2015b) *Organized crime: analyzing illegal activities, criminal structures, and extra-legal governance*. Sage Publications.

von Lampe, K. (2017) The interdisciplinary dimensions of the study of organized crime, *Transnational Organized Crime*. 9, 3, 3–21.

Landreth, B. (1985) *Out of the Inner Circle - A Hacker's Guide to Computer Security | Office of Justice Programs*. [Online]. 1985.

Lange, L. (1997) *The Rise of the Underground Engineer - White Paper*. [Online]. 22 September 1997. TechSearch.

Lavorgna, A. (2015) Organised crime goes online: realities and challenges, *Journal of Money Laundering Control*. 18, 2, 153–68.

Lawson, S. (2013) Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats, *Journal of Information Technology & Politics*. 10, 1, 86–103.

Lawson, S.T., Yeo, S.K., Haoran Yu and Greene, E. (2016) The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In *2016 8th International Conference on Cyber Conflict (CyCon)*. [Online]. May 2016 Tallinn, Estonia: IEEE. pp. 65–80.

Leahey, E. and Moody, J. (2014) Sociological innovation through subfield integration, *Social Currents*. 1, 3, 228–56.

Ledingham, R. and Mills, R. (2015) A preliminary study of autism and cybercrime in the context of international law enforcement, *Advances in Autism*. 1, 1, 2–11.

Lee, K., Kim, J., Kwon, K.H., Han, Y. and Kim, S. (2008) DDoS attack detection method using cluster analysis, *Expert systems with applications*. 34, 3, 1659–65.

Lee, S. and Bozeman, B. (2005) The Impact of Research Collaboration on Scientific Productivity, *Social Studies of Science*. 35, 5, 673–702.

Lehto, M. (2022) Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection*. Springer. pp. 3–42.

Lemke, R., Johnson, L.M. and Jenks, D. (2015) Perceptions of the trend of collaborative publications: Results from a survey of criminal justice and criminology department chairs, *Journal of Criminal Justice Education*. 26, 1, 1–21.

Leukfeldt, E.R., Kleemans, E.R. and Stol, W.P. (2017a) A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists, *Crime, Law and Social Change*. 67, 1, 21–37.

Leukfeldt, E.R., Kleemans, E.R. and Stol, W.P. (2017b) Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis, *Crime, Law and Social Change*. 67, 1, 39–53.

Leukfeldt, E.R., Lavorgna, A. and Kleemans, E.R. (2017) Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, *European Journal on Criminal Policy and Research*. 23, 3, 287–300.

Leukfeldt, E.R. and Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, *Deviant Behavior*. 37, 3, 263–80.

Levesque, M. (2006) 00009. *Hacktivism: The How and Why of Activism for the Digital Age*. Weiss, J., Nolan, J., Hunsinger, J., and Trifonas, P. (eds.). [Online]. Dordrecht: Springer.

Levine, R.A. and Campbell, D.T. (1972) 00000. *Ethnocentrism: Theories of conflict, ethnic attitudes, and group behavior*. New York: Wiley.

Levitt, G. (1986) Is terrorism worth defining, *Ohio NUL Rev.* 13,97.

Levy, S. (2010) Citationkey:Levy2010. *Hackers: Heroes of the computer revolution*. 1st ed. Sebastopol, CA: O'Reilly Media.

Lewkowicz, D.J. (2001) The concept of ecological validity: What are its limitations and is it bad to be invalid?, *Infancy*. 2, 4, 437–50.

Li, X. (2013) Hacktivism and the first amendment: Drawing the line between cyber protests and crime, *Harv. JL & Tech.* 27,301.

Libicki, M.C. (2009) *Cyberdeterrence and cyberwar*. RAND corporation.

Libicki, M.C. (2012) *Crisis and escalation in cyberspace*. Rand Corporation.

Libicki, M.C. (2015) *Sharing information about threats is not a cybersecurity panacea*

Lindgren, S. and Lundstrom, R. (2011) Pirate culture and hacktivist mobilization: The cultural and social protocols of #WikiLeaks on Twitter, *New Media & Society*. 13, 6, 999–1018.

Lindsay, J.R. (2014) The impact of China on cybersecurity: Fiction and friction, *International Security*. 39, 3, 7–47.

Lindsay, J.R. (2015) Exaggerating the Chinese Cyber Threat, *Quarterly Journal: International Security. Retrieved from https://www. belfercenter. org/sites/default/files/legacy/files/linsday-china-cyber-pb-final. pdf*.

Lindsay, J.R. (2017) Restrained by design: the political economy of cybersecurity, *Digital Policy Regulation and Governance*. 19, 6, 493–514.

Liu, A. (2004) *The laws of cool: Knowledge work and the culture of information*. [Online]. University of Chicago Press.

Liu, S. and Chen, C. (2013) The differences between latent topics in abstracts and citation contexts of citing papers, *Journal of the American Society for Information Science and Technology*. 64, 3, 627–39.

Loader, B.D. and Thomas, D. (2013) *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.

Lock, I. and Seele, P. (2015) Quantitative content analysis as a method for business ethics research, *Business Ethics: A European Review*. 24, S1, S24–40.

Lokot, T. (2017) Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism, *Irish Studies in International Affairs*. 28,99–116.

Lugg, C.A. (2017) Educating for political activism and subversion: the role of public educators in a Trumpian age, *International Journal of Qualitative Studies in Education*. 30, 10, 965–70.

Luiijf, E. (2014) Definitions of cyber terrorism. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier. pp. 11–7.

Lukman, E. (2013) *Uh Oh! Indonesia's President Dissed as His Website Gets Hacked*. [Online]. 10 January 2013. Tech in Asia.

Luong, H.T. (2023) Foundations and trends in the darknet-related criminals in the last 10 years: a systematic literature review and bibliometric analysis, *Security Journal*.

Lynch, J. (2018) Not Even Our Own Facts: Criminology in the Era of Big Data, *Criminology*. 56, 3, 437–54.

Lynch, O., Ahmed, Y., Russell, H. and Hosford, K. (2020) 00000. *Reflections on Irish Criminology: Conversations with Criminologists*. [Online]. Palgrave Macmillan.

Macdonald, S., Jarvis, L. and Chen, T. (2013) A Multidisciplinary Conference on Cyberterrorism: Final Report, *The cyber terrorism project, Swansea*.

Macdonald, S., Jarvis, L., Chen, T. and Lavis, S. (2013) *Cyberterrorism: A survey of researchers*. Cyberterrorism project research ….

Macdonald, S., Jarvis, L. and Lavis, S.M. (2019) Cyberterrorism Today? Findings From a Follow-on Survey of Researchers, *Studies in Conflict & Terrorism*. 1–26.

Macdonald, S., Jarvis, L. and Nouri, L. (2015) State Cyberterrorism: A Contradiction in Terms?, *Journal of Terrorism Research*. 6, 3, 62.

Machado, M.B. (2015) Between control and hacker activism: the political actions of Anonymous Brasil, *Historia Ciencias Saude-Manguinhos*. 22,.

Maggi, F., Balduzzi, M., Flores, R., Gu, L. and Ciancaglini, V. (2018) Investigating Web Defacement Campaigns at Large. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ASIACCS '18. [Online]. 29 May 2018 New York, NY, USA: Association for Computing Machinery. pp. 443–56.

Magnone, E. (2014) The extreme case of terrorism: a scientometric analysis, *Scientometrics*. 101,179–201.

Maier, D., Maier, A., Aşchilean, I., Anastasiu, L. and Gavriş, O. (2020) The Relationship between Innovation and Sustainability: A Bibliometric Review of the Literature, *Sustainability*. 12, 10, 4083.

Majchrzak, A., Faraj, S., Kane, G.C. and Azad, B. (2013) The Contradictory Influence of Social Media Affordances on Online Communal Knowledge Sharing, *Journal of Computer-Mediated Communication*. 19, 1, 38–55.

Majumder, A., Routh, M. and Singha, D. (2019) A conceptual study on the emergence of cryptocurrency economy and its nexus with terrorism financing. In *The Impact of Global Terrorism on Economic and Political Development*. Emerald Publishing Limited. pp. 125–38.

Malešević, S. (2006) *Identity as ideology: understanding ethnicity and nationalism*. Basingstoke: Palgrave Macmillan.

Manion, M. and Goodrum, A. (2005) *Terrorism or civil disobedience*. 2. [Online]. azumisan.asuscomm.com.

Mansfield-Devine, S. (2015) The Ashley Madison affair, *Network Security*. 2015, 9, 8–16.

Marple, H. (2018) Parasite, pirate, and Robin Hood: Sci-Hub is disrupting the world of academic publishing, *The iJournal: Student Journal of the University of Toronto's Faculty of Information*. 3, 2.

Martin, G., Ghafur, S., Kinross, J., Hankin, C. and Darzi, A. (2018) WannaCry—a year on, *BMJ*. k2381.

Martyn, J. (1964) Bibliographic coupling, *Journal of documentation*. 20, 4, 236–236.

Marx, W. and Bornmann, L. (2010) How accurately does Thomas Kuhn's model of paradigm change describe the transition from the static view of the universe to the big bang theory in cosmology?: A historical reconstruction and citation analysis, *Scientometrics*. 84, 2, 441–64.

Maskaliunaite, A. (2002) *Defining Terrorism in the Political and Academic Discourse* 15.

Matusitz, J. (2008) Cyberterrorism: Postmodern State of Chaos, *Information Security Journal: A Global Perspective*. 17, 4, 179–87.

Matusitz, J. and Breen, G.-M. (2011) A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism, *Journal of Human Behavior in the Social Environment*. 21, 2, 109–29.

Matusitz, J. and Minei, E. (2009) Cyberterrorism: Its Effects on Health-Related Infrastructures, *Journal of Digital Forensic Practice*. 2, 4, 161–71.

Mayer Lux, L. (2018) Defining cyberterrorism, *Revista Chilena de Derecho Y Tecnologia*. 7, 2, 5–25.

McCain, K.W. (1990) Mapping authors in intellectual space: A technical overview, *Journal of the American Society for Information Science (1986-1998)*. 41, 6, 433.

McCarthy, M.T. (2015) Toward a Free Information Movement, *Sociological Forum*. 30, 2, 439–58.

McCusker, R. (2006) Transnational organised cyber crime: distinguishing threat from reality, *Crime, Law and Social Change*. 46,257–73.

McGuigan, A.S. (2019) *Hacking Back: Justifiable or Vigilantism*

McKelvey, F. (2015) We Like Copies, Just Don't Let the Others Fool You: The Paradox of The Pirate Bay, *Television & New Media*. 16, 8, 734–50.

McQuade, S.C. (ed.) (2009) *Encyclopedia of cybercrime*. Westport, Conn: Greenwood Press.

McQuire, M. and Dowling, S. (2013) *Cyber crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75*. [Online].

McTavish, D.G. and Pirro, E.B. (1990) Contextual content analysis, *Quality and Quantity*. 24, 3, 245–65.

Mehrabov, I. (2016) When States Strike Back: Failures of Mediatized Activism in Azerbaijan and Turkey, *Triplec-Communication Capitalism & Critique*. 14, 2, 496–515.

Meland, P.H., Bayoumy, Y.F.F. and Sindre, G. (2020) The Ransomware-as-a-Service economy within the darknet, *Computers & Security*. 92,101762.

Merck, M. (2015) Masked men: hacktivism, celebrity and anonymity, *Celebrity Studies*. 6, 3, 272–87.

Merton, R.K. (1936) The Unanticipated Consequences of Purposive Social Action, *American Sociological Review*. 1, 6, 894.

Merton, R.K. (1942) A note on science and democracy, *J. Legal & Pol. Soc.* 1,115.

Merton, R.K. (1968) *Social Theory and Social Structure*. Simon and Schuster.

Merton, R.K. (1999) Opportunity structure: The emergence, diffusion, and differentiation of a sociological concept, 1930s–1950s. In *The legacy of anomie theory*. [Online]. Routledge. pp. 3–78.

Meserve, J. (2001) *New 'Injustice' virus spreads political message*. [Online]. 20 March 2001. Computerworld.

Mezei, K. (2018) Cyberterrorism and the terrorist use of the Internet, *Law Series of the Annals of the West University of Timisoara*.

Mihas, P. (2019) 00000. *Learn to Use an Exploratory Sequential Mixed Method Design for Instrument Development*. [Online]. 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications, Ltd.

Miller, C. (2020) *How Taiwan's 'civic hackers' helped find a new way to run the country*. [Online]. 27 September 2020. The Guardian.

Miller, J.H. and Page, S.E. (2007) Social science in between, from complex adaptive systems: An introduction to computational models of social life, *Introductory Chapters*.

Miller, T., Staves, A., Maesschalck, S., Sturdee, M. and Green, B. (2021) Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems, *International Journal of Critical Infrastructure Protection*. 35,100464.

Millington, C. (2024) Bad history: a historian's critique of Rapoport's "four waves of modern terrorism" model, *Critical Studies on Terrorism*. 1–18.

Milone, M.G. (2002) Hacktivism: Securing the National Infrastructure, *Information and Organization*. 29,32.

Montasari, R. (2023) *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National*

Cybersecurity. Advances in Information Security. [Online]. Cham: Springer International Publishing.

Morozov, E. (2009) Foreign Policy: Brave New World of Slacktivism. *NPR*. 19 May.

Morrison, J.F. (2016) Trust in me: Allegiance choices in a post-split terrorist movement, *Aggression and Violent Behavior*. 28,47–56.

Morrison, J.F. (2022) Talking Stagnation: Thematic Analysis of Terrorism Experts' Perception of the Health of Terrorism Research, *Terrorism and Political Violence*. 34, 8, 1509–29.

Mott, G. (2016) Terror from behind the keyboard: conceptualising faceless detractors and guarantors of security in cyberspace, *Critical Studies on Terrorism*. 9, 1, 33–53.

Mulkay, M.J. (1975) Three Models of Scientific Development, *Sociological Review*. 23, 3, 509–26.

Mumtaz, A.A. and Sultan, A.-D. (2011) Literature on terrorism: A bibliometric analysis of articles published during 1981-1990, *Malaysian Journal of Library & Information Science*. 16, 2, 33–43.

Munn, Z., Peters, M.D.J., Stern, C., Tufanaru, C., McArthur, A. and Aromataris, E. (2018) Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach, *BMC Medical Research Methodology*. 18, 1, 143.

Musen, M.A. (2015) The Protégé Project: A Look Back and a Look Forward, *AI matters*. 1, 4, 4–12.

Nakov, P., Schwartz, A. and Hearst, M. (2004) *Citances: Citation sentences for semantic analysis of bioscience text*

Neagu, F.S. and Savu, A. (2019) The costs of cyberterrorism for the national economy: United States of America vs Egypt, *Sciendo*. 13, 1, 983–93.

Nelson, M.S., Wooditch, A. and Gabbidon, S.L. (2014) Is Criminology Out-of-Date? A Research Note on the Use of Common Types of Data, *Journal of Criminal Justice Education*. 25, 1, 16–33.

Neuendorf, K.A. (2002) *The Content Analysis Guidebook Thousand Oaks: Sage*

Neuendorf, K.A. (2011) Content Analysis: A Methodological Primer for Gender Research, *Sex Roles*. 64, 3–4, 276–89.

Neufeld, D. (2020) Computer crime motives: Do we have it right?, *Sociology Compass*. 17, 4, e13077.

Newman, J., Cherney, A. and Head, B.W. (2016) Do Policy Makers Use Academic Research? Reexamining the "Two Communities" Theory of Research Utilization, *Public Administration Review*. 76, 1, 24–32.

Nissenbaum, H. (2004) Hackers and the contested ontology of cyberspace, *New Media & Society*. 6, 2, 195–217.

Nissenbaum, H. (2005) Where computer security meets national security, *Ethics and Information Technology*. 7,61–73.

Norris, P. (2007) *Political Activism: New Challenges, New Opportunities*. Boix, C. and Stokes, S.C. (eds.). [Online]. Oxford University Press.

Noy, N.F. and McGuinness, D.L. (2002) *Ontology Development 101: A Guide to Creating Your First Ontology* 25.

Noyons, E.C.M., Moed, H.F. and Van Raan, A.F.J. (1999) Integrating research performance analysis and science mapping, *Scientometrics*. 46, 3, 591–604.

Nurse, J.R.C. and Bada, M. (2019) *The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations*. In [Online]. pp. 690–715.

Offermann, P., Blom, S., Schönherr, M. and Bub, U. (2010) Artifact Types in Information Systems Design Science – A Literature Review. In Winter, R., Zhao, J.L., and Aier, S. (eds.) *Global Perspectives on Design Science Research*. Lecture Notes in Computer Science. [Online]. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 77–92.

Olsen, M.E. (1973) A model of political participation stratification, *Journal of Political & Military Sociology*. 183–200.

O'Malley, G. (2013) Hacktivism: cyber activism or cyber crime, *Trinity CL Rev.* 16,137.

Omand, D. (2018) The threats from modern digital subversion and sedition, *Journal of Cyber Policy*. 3, 1, 5–23.

Onat, I., Bastug, M.F., Guler, A. and Kula, S. (2022) Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison, *Behavioral Sciences of Terrorism and Political Aggression*. 1–17.

Osareh, F. (1996) Bibliometrics, Citation Analysis and Co-Citation Analysis: A Review of Literature I, *Libri*. 46, 3.

O'Shaughnessy, N.J. and Baines, P.R. (2009) Selling terror: The symbolization and positioning of Jihad, *Marketing Theory*. 9, 2, 227–41.

Ottis, R. and Lorents, P. (2010) *Cyberspace: Definition and implications*. In 2010 Academic Conferences International Limited. p. 267.

Page, M.J., Moher, D., Brennan, S. and McKenzie, J.E. (2023) The PRISMATIC project: protocol for a research programme on novel methods to improve reporting and peer review of systematic reviews of health evidence, *Systematic Reviews*. 12, 1, 196.

Paisley, W. (1972) The Role of Invisible Colleges in Scientific Information Transfer, *Educational Researcher*. 1, 4, 5–19.

Palmer, D. (2019) *WannaCry ransomware is still infecting PCs - and some victims are still trying to pay the ransom*. [Online]. 20 September 2019. ZDNET.

Panetta, L. (2012) Defending the National From Cyber Attacks. In *Presentation to Business Executives for National Security*. p.

Parker, T. and Sitter, N. (2016) The Four Horsemen of Terrorism: It's Not Waves, It's Strains, *Terrorism and Political Violence*. 28, 2, 197–216.

Pasadeos, Y., Phelps, J. and Kim, B.-H. (1998) Disciplinary impact of advertising scholars: Temporal comparisons of influential authors, works and research networks, *Journal of Advertising*. 27, 4, 53–70.

Pasculli, L. (2020) *The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory* 2,.

Pastrana, S., Hutchings, A., Caines, A. and Buttery, P. (2018) Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum. In Bailey, M., Holz, T., Stamatogiannakis, M., and Ioannidis, S. (eds.) *Research in Attacks, Intrusions, and Defenses*. Lecture Notes in Computer Science. [Online]. Cham: Springer International Publishing. pp. 207–27.

Paterson, T. and Hanley, L. (2020) Political warfare in the digital age: cyber subversion, information operations and 'deep fakes', *Australian Journal of International Affairs*. 74, 4, 439–54.

Patro, S.G.K. and sahu, K.K. (2015) Normalization: A Preprocessing Stage, *IARJSET*. 20–2.

Payne, B.K. and Hadzhidimova, L. (2020) Disciplinary and interdisciplinary trends in cybercrime research: An examination, *International Journal of Cyber Criminology*. 14, 1, 81–105.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007) A Design Science Research Methodology for Information Systems Research, *Journal of Management Information Systems*. 24, 3, 45–77.

Peretti, K. and Slade, J. (2014) State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction, *The SciTech Lawyer*. 10, 2.

Peretti, K.K. (2008) Data breaches: What the underground world of" carding" reveals, *Santa Clara Computer & High Tech. LJ*. 25,375.

Perez, E. and Prokupecz, S. (2015) *Paris attackers likely used encrypted apps, officials say | CNN Politics*. [Online]. 17 December 2015.

Perkins, R.C., Howell, C.J., Dodge, C.E., Burruss, G.W. and Maimon, D. (2022) Malicious Spam Distribution: A Routine Activities Approach, *Deviant Behavior*. 43, 2, 196–212.

Peters, H.P.F. and Van Raan, A.F.J. (1991) Structuring scientific activities by co-author analysis, *Scientometrics*. 20, 1, 235–55.

Phillips, B.J. (2023) How Did 9/11 Affect Terrorism Research? Examining Articles and Authors, 1970–2019, *Terrorism and Political Violence*. 35, 2, 409–32.

Piat, C. (2019) Slacktivism: Not Simply a Means to an End, but a Legitimate Form of Civic Participation, *Canadian Journal of Family and Youth / Le Journal Canadien de Famille et de la Jeunesse*. 11, 1, 162–79.

Pisciotta, A.W. (1981) Theoretical Perspectives for Historical Analyses, *Criminology*. 19, 1, 115–30.

Plotnek, J.J. and Slay, J. (2021) Cyber terrorism: A homogenized taxonomy and definition, *Computers & Security*. 102,102145.

Polat, B., Bakiroğlu, C.T. and Sayin, M.E.D. (2013) Hactivism in Turkey: The case of Redhack, *Mediterranean Journal of Social Sciences*. 4, 9, 628–36.

Pollitt, Mark.M. (1998) Cyberterrorism—fact or fancy?, *Computer Fraud & Security*.

Pool, R. and Custers, B. (2017) The police hack back: Legitimacy, necessity and privacy implications of the next step in fighting cybercrime, *European journal of crime, criminal law and criminal justice*. 25, 2, 123–44.

Post, J.M. (1990) *Terrorist psycho-logic: Terrorist behavior as a product of psychological forces.*

Potter, W.J. and Levine-Donnerstein, D. (1999) Rethinking validity and reliability in content analysis, *Journal of Applied Communication Research*. 27, 3, 258–84.

Presbey, G.M. (1992) *Hannah Arendt on Power, Consent, and Coercion*

Price, J.H. and Murnan, J. (2004) Research limitations and the necessity of reporting them, *American journal of health education*. 35, 2, 66–7.

Prieto-Diaz, R. (2003) A faceted approach to building ontologies. In *Proceedings Fifth IEEE Workshop on Mobile Computing Systems and Applications*. [Online]. October 2003 pp. 458–65.

Pritchard, A. (1969) Statistical bibliography or bibliometrics, *Journal of documentation*. 25, 4, 348–9.

van Raan, A. (1999) Advanced bibliometric methods for the evaluation of universities, *Scientometrics*. 45, 3, 417–23.

Rae, M. (2021) Analyzing the NFT mania: Is a JPG worth millions? In *SAGE Business Cases*. SAGE Publications: SAGE Business Cases Originals. p.

Raj, K. (2007) *Relocating modern science: circulation and the construction of knowledge in South Asia and Europe, 1650-1900*. Springer.

Raley, R. (2009) *Tactical media*. U of Minnesota Press.

Rapoport, D.C. (2003) The Four Waves of Rebel Terror and September 11, *The New Global Terrorism: Characteristics, Causes, Controls*. 8, 1, 36–52.

Rawat, R. (2023) Logical concept mapping and social media analytics relating to cyber criminal activities for ontology creation, *International Journal of Information Technology*. 15, 2, 893–903.

Rawlings, C.M., McFarland, D.A., Dahlander, L. and Wang, D. (2015) Streams of Thought: Knowledge Flows and Intellectual Cohesion in a Multidisciplinary Era, *Social Forces*. 93, 4, 1687–722.

Raymond, E.S. (2003) The jargon file, *The on-line hacker Jargon File*.

Reichertz, J. (2013) *Induction, deduction*. Sage Publications.

Reid, E. (1997) *Evoloution of a Body of Knowledge: An Analysis of Terrorism Research*. pp.91–106.

Reid, E. and Chen, H. (2008) Domain Mapping of Contemporary Terrorism Research. In Chen, H., Reid, E., Sinai, J., Silke, A., and Ganor, B. (eds.) *Terrorism Informatics*. Integrated Series In Information Systems. [Online]. Boston, MA: Springer US. pp. 3–26.

Reid, E., Qin, J., Chung, W., Xu, J., Zhou, Y., Schumaker, R., Sageman, M. and Chen, H. (2004) Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Addressing the Threats of Terrorism. In Chen, H., Moore, R., Zeng, D.D., and Leavitt, J. (eds.) *Intelligence and Security Informatics*. Lecture Notes in Computer Science. [Online]. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 125–45.

Reid, E.F. and Chen, H. (2006) Mapping the contemporary terrorism research domain, *International Journal of Human Computer Studies*. 65, 1, 42–56.

Reid, E.O. (1993) Terrorism research and the diffusion of ideas, *Knowledge and Policy*. 6, 1, 17–37.

Reynolds, P. (2021) *'Wizard Spider': Who are they and how do they operate?*

Rid, T. (2013) *Cyber war will not take place*. Oxford ; New York: Oxford University Press.

Rieck, K., Holz, T., Willems, C., Düssel, P. and Laskov, P. (2008) *Learning and classification of malware behavior*. In 2008 Springer. pp. 108–25.

Riglietti, G. (2016) *Defining the threat: what cyber terrorism means today and what it could mean tomorrow* 8, 3, 8.

Roetzel, P.G. (2019) Information overload in the information age: a review of the literature from business administration, business psychology, and related disciplines with a bibliometric approach and framework development, *Business Research*. 12, 2, 479–522.

Rogers, M.K. (2006) Digital Investigation : A two-dimensional circumplex approach to the development of a hacker taxonomy, *Elsevier*.

Romagna, M. and Leukfeldt, R.E. (2023) Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism, *Journal of Crime and Justice*. 1–19.

Ruscio, J., Seaman, F., D'Oriano, C., Stremlo, E. and Mahalchik, K. (2012) Measuring Scholarly Impact Using Modern Citation-Based Indices, *Measurement: Interdisciplinary Research & Perspective*. 10, 3, 123–46.

Ruth, S. and Stone, S. (2012) A Legislator's Dilemma, *IEEE Internet Computing*. 16, 6, 78–81.

Sageman, M. (2004) *Understanding terror networks*. University of Pennsylvania press.

Sageman, M. (2014) The Stagnation in Terrorism Research, *Terrorism and Political Violence*. 26, 4, 565–80.

Saini, J.K. and Bansal, D. (2021) Detecting online recruitment of terrorists: towards smarter solutions to counter terrorism, *International Journal of Information Technology*. 13, 2, 697–702.

Samoilenko, S.A. (2018) Subversion practices: From coercion to attraction., *Experiencing Public Relations: International voices Routledge, London, UK*. 174–93.

Sampson, J.P. (2012) *Guide to quantitative and qualitative dissertation research*

Samuel, A.W. (2004) *Hacktivism and the future of political participation*. Harvard University.

Sánchez-Cuenca, I. and De la Calle, L. (2009) Domestic terrorism: The hidden side of political violence, *Annual Review of Political Science*. 12,31–49.

Saranya, C. and Manik, G. (2013) A Study on Normalization Techniques for Privacy Preserving Data Mining, *International Journal of Engineering and Technology*. 5, 3.

Sattler (2022) *Historic hacktivism, revenge ransomware, and other cyber attack news related to the Ukraine invasion*. [Online]. 2 March 2022. F-Secure Blog.

Sauter, M. (2013) "LOIC Will Tear Us Apart", *American Behavioral Scientist*. 57, 7, 983–1007.

Sauter, M. (2014) *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet*. Bloomsbury Publishing USA.

Scheuerman, W.E. (2016) Digital disobedience and the law, *New Political Science*. 38, 3, 299–314.

Schildt, H.A., Zahra, S.A. and Sillanpää, A. (2006) Scholarly communities in entrepreneurship research: A co–citation analysis, *Entrepreneurship theory and practice*. 30, 3, 399–415.

Schmelzeisen, L. and Staab, S. (2019) *Learning Taxonomies of Concepts and not Words using Contextualized Word Representations: A Position Paper*. [Online].

Schmid, A.P. (2004a) Frameworks for Conceptualising Terrorism, *Terrorism and Political Violence*. 16, 2, 197–221.

Schmid, A.P. (2004b) Terrorism-the definitional problem, *Case W. Res. J. Int'l L.* 36,375.

Schmid, A.P. (2011) *The Routledge Handbook of Terrorism Research*. 3.

Schmid, A.P. (2014) Comments on Marc Sageman's Polemic "The Stagnation in Terrorism Research", *Terrorism and Political Violence*. 26, 4, 587–95.

Schmid, A.P. (2023) Defining Terrorism, *The Hague: ICCT*.

Schmid, A.P. and Jongman, A.J. (1984) *Political terrorism: A research guide to concepts, theories, data bases and literature*. North-Holland Amsterdam.

Schmid, A.P. and Jongman, A.J. (1988) Political Terrorism: A New Guide to Actors, *Authors, Concepts, Data Bases*.

Schrock, A.R. (2016) Civic hacking as data activism and advocacy: A history from publicity to open government data, *New Media & Society*. 18, 4, 581–99.

Schuurman, B. (2018) Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship, *Terrorism and Political Violence*. 00, 00, 1–16.

Schuurman, B. (2019) Topics in terrorism research: reviewing trends and gaps, 2007-2016, *Critical Studies on Terrorism*. 12, 3, 463–80.

Schuurman, B. (2020) Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship, *Terrorism and Political Violence*. 32, 5, 1011–26.

Seebruck, R. (2015) A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model, *Digital Investigation*. 14,36–45.

Seglen, P.O. (1997) Why the impact factor of journals should not be used for evaluating research, *BMJ*. 314, 7079, 497.

Shad, M.R. (2019) Cyber Threat Landscape and Readiness Challenge of Pakistan, *Strategic Studies*. 39, 1, 1–19.

Shandler, R. and Gomez, M.A. (2022) The hidden threat of cyber-attacks – undermining public confidence in government, *Journal of Information Technology & Politics*. 20, 4, 359–74.

Shandler, R., Kostyuk, N. and Oppenheimer, H. (2023) Public Opinion and Cyberterrorism, *Public Opinion Quarterly*. 87, 1, 92–119.

Sharma, H.P. (2007) Download plus citation counts - A useful indicator to measure research impact [1], *Current science*. 92,.

Shenk, D. (1997) 01222. *Data smog: Surviving the information glut*. HarperCollins Publishers.

Shichor, D. (1982) An analysis of citations in introductory criminology textbooks: A research note, *Journal of Criminal Justice*. 10, 3, 231–7.

Shiffrin, R.M. and Börner, K. (2004) Mapping knowledge domains, *Proceedings of the National Academy of Sciences*. 101, suppl_1, 5183–5.

Shinder, D.L. and Tittel, E. (2002) *Scene of the cybercrime: computer forensics handbook*. Syngress Shinder books. Rockland, Mass: Syngress Publ.

Shneider, A.M. (2009) Four stages of a scientific discipline; four types of scientist, *Trends in Biochemical Sciences*. 34, 5, 217–23.

Sieber, U. (2006) *International Cooperation against Terrorist Use of the Internet*

Siedlecki, S.L. (2020) Understanding descriptive research designs and methods, *Clinical Nurse Specialist*. 34, 1, 8–12.

Silic, M. and Lowry, P.B. (2021) Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes, *Information Systems Frontiers*. 23, 2, 329–41.

Silke, A. (2001) The Devil You Know: Continuing Problems with Research on Terrorism, *Terrorism and Political Violence*. 13, 4, 1–14.

Silke, A. (2003) Becoming a terrorist, *Terrorists, victims and society: Psychological perspectives on terrorism and its consequences*. 29,53.

Silke, A. (2004) The road less travelled: Recent trends in terrorism research. In *Research on Terrorism*. Routledge. pp. 206–33.

Silke, A. (2006) The impact of 9/11 on research on terrorism. In *Mapping terrorism research*. Routledge. pp. 90–107.

Silke, A. (2008) *Research on Terrorism: A Review of the Impact of 9/11 and the Global War on Terrorism*. In pp. 27–50.

Silke, A. (2009) Contemporary terrorism studies: issues in research. In *Critical terrorism studies*. [Online]. Routledge. pp. 48–62.

Silke, A. and Schmidt-Petersen, J. (2017) The Golden Age? What the 100 Most Cited Articles in Terrorism Studies Tell Us, *Terrorism and Political Violence*. 29, 4, 692–712.

Simpson, G.G. (1961) Principles of animal taxonomy. In *Principles of Animal Taxonomy*. Columbia University Press. p.

Simpson, P.L., Guthrie, J., Jones, J. and Butler, T. (2021) Identifying research priorities to improve the health of incarcerated populations: results of citizens' juries in Australian prisons, *The Lancet Public Health*. 6, 10, e771–9.

Small, H. (1973) Co-citation in the scientific literature: A new measure of the relationship between two documents, *Journal of the American Society for information Science*. 24, 4, 265–9.

Small, H. and Griffith, B.C. (1974) The structure of scientific literatures I: Identifying and graphing specialties, *Science studies*. 4, 1, 17–40.

Smith, B., Yurcik, W. and Doss, D. (2001) *Ethical Hacking: The Security Justification*

Smith, B.L. and Damphousse, K.R. (2006) *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic,*

Smith, T.B., Mao, R., Korotchenko, S. and Krohn, M.D. (2023) Partners in Criminology: Machine Learning and Network Science Reveal Missed Opportunities and Inequalities in the Study of Crime, *Journal of Quantitative Criminology*.

Smith, T.E. (2015) Binary Terror: The Reality of Terrorism in a Virtual World, *American Intelligence Journal*. 32, 2, 131–8.

Snider, K.L., Shandler, R., Zandani, S. and Canetti, D. (2021) Cyberattacks, cyber threats, and attitudes toward cybersecurity policies, *Journal of Cybersecurity*. 7, 1, tyab019.

de Solla Price, D.J. and Beaver, D. (1966) Collaboration in an invisible college., *American psychologist*. 21, 11, 1011.

Solomon, R. (2017) Electronic protests: Hacktivism as a form of protest in Uganda, *Computer Law & Security Review*. 33, 5, 718–28.

Sorell, T. (2015) Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous, *Journal of Human Rights Practice*. 7, 3, 391–410.

Sovacool, B.K., Kester, J., Noel, L. and de Rubens, G.Z. (2019) Energy Injustice and Nordic Electric Mobility: Inequality, Elitism, and Externalities in the Electrification of Vehicle-to-Grid (V2G) Transport, *Ecological Economics*. 157,205–17.

Stalans, L.J. and Finn, M.A. (2016) Understanding How the Internet Facilitates Crime and Deviance, *Victims & Offenders*. 11, 4, 501–8.

Stamm, E. (2015) We Are All Anonymous: Beyond Hacktivist Stereotypes, *Spectra*. 4, 2.

Stern, J. (2014) Response to Marc Sageman's "The Stagnation in Terrorism Research", *Terrorism and Political Violence*. 26, 4, 607–13.

Stockdale, K.J. and Sweeney, R. (2022) Whose voices are prioritised in criminology, and why does it matter?, *Race and Justice*. 12, 3, 481–504.

Stoehrel, R.F. and Lindgren, S. (2014) For the Lulz: Anonymous, Aesthetics and Affect, *TripleC*. 12, 1, 238–64.

Stohl, M. (2007) Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?, *Crime, Law and Social Change*. 46, 4, 223–38.

Straub, V. (2021) Beyond Kinetic Harm and towards a Dynamic Conceptualization of Cyberterrorism, *Journal of Information Warfare*. 20, 3, 1–23.

Sullivan, C. (2015) The 2014 Sony Hack and the Role of International Law, *Journal of National Security Law and Policy*. 8, 3, 437–68.

Sun, X., Kaur, J., Milojević, S., Flammini, A. and Menczer, F. (2013) Social Dynamics of Science, *Scientific Reports*. 3, 1, 1069.

Sykes, G.M. (1974) The Rise of Critical Criminology, *J. Crim. L. & Criminology*. 65,206.

Sykes, G.M. and Matza, D. (1957) Techniques of neutralization: A theory of delinquency, *American sociological review*. 22, 6, 664–70.

Symeonidou-Kastanidou, E. (2007) Towards a New Definition of Organised Crime in the European Union, *European Journal of Crime, Criminal Law and Criminal Justice*. 15, 1, 83–104.

Tabah, A.N. (1999) Literature dynamics: Studies on growth, diffusion, and epidemics, *Annual review of information science and technology (ARIST)*. 34,249–86.

Tan, Y., Vuran, M.C. and Goddard, S. (2009) Spatio-Temporal Event Model for Cyber-Physical Systems. In *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*. [Online]. June 2009 Montreal, Quebec, Canada: IEEE. pp. 44–50.

Tanczer, L.M. (2016) Hacktivism and the male-only stereotype, *New Media & Society*. 18, 8, 1599–615.

Tarrant, M., Bray, N. and Katsinas, S. (2018) The invisible colleges revisited: An empirical review, *The Journal of Higher Education*. 89, 3, 341–67.

Tashakkori, A. and Teddlie, C. (1998) 10900. *Mixed methodology: Combining qualitative and quantitative approaches*. Sage.

Taylor, M. (2014) If I Were You, I Wouldn't Start From Here: Response to Marc Sageman's "The Stagnation in Terrorism Research", *Terrorism and Political Violence*. 26, 4, 581–6.

Taylor, M. and Horgan, J. (2006) A Conceptual Framework for Addressing Psychological Process in the Development of the Terrorist, *Terrorism and Political Violence*. 18, 4, 585–601.

Taylor, P.A. (1998) Hackers: Cyberpunks or microserfs?, *Information, Communication & Society*. 1, 4, 401–19.

Taylor, P.A. (2005) From hackers to hacktivists: speed bumps on the global superhighway?, *New Media & Society*. 7, 5, 625–46.

Tenopir, C. and King, D.W. (2000) 00352. *Towards electronic journals: realities for scientists, librarians, and publishers*. Special Libraries Association Washington, DC.

Thomas, D. and Loader, B.D. (2000) Introduction - cybercrime: law enforcement, security and surveillance in the information age, *Cybercrime. Security and Surveillance in the Information Age*. 1–13.

Tilley, N. and Laycock, G. (2018) Developing a knowledge base for crime prevention: lessons learned from the British experience, *Crime Prevention and Community Safety*. 20, 4, 228–42.

Tranfield, D., Denyer, D. and Smart, P. (2003) Towards a methodology for developing evidence-informed management knowledge by means of systematic review, *British journal of management*. 14, 3, 207–22.

Trautman, L.J. and Ormerod, P.C. (2018) Wannacry, ransomware, and the emerging threat to corporations, *Tenn. L. Rev.* 86,503.

Travaglino, G.A. (2019) Support for Anonymous as vicarious dissent: Testing the social banditry framework, *Group Processes & Intergroup Relations*. 22, 2, 163–81.

Trend Micro (2018) *Digital Vandals: Exploring the Methods and Motivations behind Web Defacement and Hacktivism - Security News*. [Online]. 22 January 2018.

Turgeman-Goldschmidt, O. (2008) Meanings that Hackers Assign to their Being a Hacker, *International Journal of Cyber Criminology*. 2, 2, 382–96.

Turkle, S. (2005) *The second self: Computers and the human spirit*. 20th anniversary ed., 1st MIT Press ed. Cambridge, Mass: MIT Press.

Unlu, A. and Gurer, C. (2022) Crime and Violence Studies in the Immigration Field: Interactions between Disciplines and Emerging Concepts, *Journal of Ethnic and Cultural Studies*. 9, 1, 185–205.

UNODC (2012) *The use of the Internet for terrorist purposes*. [Online].

Uschold, M. and King, M. (1995) *Towards a methodology for building ontologies*. [Online]. Citeseer.

Uschold, M., King, M., Moralee, S. and Zorgios, Y. (1998) The enterprise ontology, *The knowledge engineering review*. 13, 1, 31–89.

Van der Bruggen, M. and Blokland, A. (2021) A crime script analysis of child sexual exploitation material fora on the darkweb, *Sexual Abuse*. 33, 8, 950–74.

Van der Hulst, R.C. and Neve, R.J.M. (2008) *High-tech crime*. Boom Juridische uitgevers.

Vander Beken, T., Vandeviver, C. and Daenekindt, S. (2020) A state of affairs of European criminology: an exploration of topics and trends through topic modelling, *SOCARXIV*. 15/06/2020.

Vander Beken, T., Vandeviver, C. and Daenekindt, S. (2021) Two decades of European criminology: Exploring the conferences of the European Society of

Criminology through topic modelling, *European Journal of Criminology*. 18, 4, 463–83.

Veerasamy, N. (2009) Conceptual high-level framework of cyberterrorism, *Journal of Information Warfare*. 8, 1.

Veerasamy, N. (2010) *Motivation for cyberterrorism*. researchspace.csir.co.za.

Veerasamy, N. and Grobler, M. (2010) *Countermeasures to consider in the combat against cyberterrorism*. researchspace.csir.co.za.

Veerasamy, N., Grobler, M. and Solms, B.V. (2012) *Building an ontology for cyberterrorism*. researchspace.csir.co.za.

Veerasamy, N. and Grobler, M.M. (2015) Logic tester for the classification of cyberterrorism attacks, *International Journal of Cyber Warfare and Terrorism*. 5, 1, 30–46.

Von Busch, O. and Palmås, K. (2006) *Abstract hacktivism: the making of a hacker culture*

Waldron, J. (2004) Terrorism and the Uses of Terror, *The Journal of ethics*. 8,5–35.

Wall, D. (ed.) (2001) *Crime and the internet*. New York: Routledge.

Wall, D. (2007) Crime and the Internet. In *Journal of Information Ethics*. p.

Wall, D.S. (2008) Cybercrime and the Culture of Fear: Social science fiction(s) and the production of knowledge about cybercrime, *Information, Communication & Society*. 11, 6, 861–84.

Wallin, J.A. (2005) Bibliometric methods: Pitfalls and possibilities, *Basic and Clinical Pharmacology and Toxicology*. 97, 5, 261–75.

Wang, S. and Zhu, X. (2021) Evaluation of potential cryptocurrency development ability in terrorist financing, *Policing: A Journal of Policy and Practice*. 15, 4, 2329–40.

Waqas, A., Salminen, J., Jung, S., Almerekhi, H. and Jansen, B.J. (2019) Mapping online hate: A scientometric analysis on research trends and hotspots in research on online hate, *PLOS ONE*. 14, 9, e0222194.

Warren, M. and Leitch, S. (2016) The Syrian Electronic Army - a hacktivist group, *Journal of Information Communication & Ethics in Society*. 14, 2, 200–12.

Weber, R.P. (1990) *Basic content analysis*. Sage.

WebTitan (2020) *How Much Money Did WannaCry Make?*. [Online]. 2 July 2020. WebTitan DNS Filter.

Weimann, G. (2004) *Cyberterrorism How Real Is the Threat?*

Weimann, G. (2005) Cyberterrorism: The sum of all fears?, *Studies in Conflict & Terrorism*. 28, 2, 129–49.

Weimann, G. (2008) The Psychology of Mass-Mediated Terrorism, *American Behavioral Scientist*. 52, 1, 69–86.

Weimann, G. (2010) Terror on Facebook, Twitter, and YouTube, *The Brown Journal of World Affairs*. 16, 2, 45–54.

Weimann, G. (2011) Cyber-fatwas and terrorism, *STUDIES IN CONFLICT & TERRORISM*. 34, 10, 765–81.

Weimann, G. (2016) The Emerging Role of Social Media in the Recruitment of Foreign Fighters. In de Guttry, A., Capone, F., and Paulussen, C. (eds.) *Foreign Fighters under International Law and Beyond*. [Online]. The Hague: T.M.C. Asser Press. pp. 77–95.

Weisburd, D., Savona, E.U., Hasisi, B., and Calderoni, F. (eds.) (2020) *Understanding Recruitment to Organized Crime and Terrorism*. [Online]. Cham: Springer International Publishing.

Whittaker, Z. (2019) Two years after WannaCry, a million computers remain at risk. *TechCrunch*. [Online].

Wilson, C. (2015) *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress (CRS Report RL32114)*. Retrieved.

Wilson, C.S. (1999) Informetrics, *Annual Review of Information Science and Technology (ARIST)*. 34,107–247.

Windholz, A. (2019) The Necessity of Sci-Hub and Guerilla Open Access Initiatives, *Perspectives on Scholarly Communication: Volume One*. 148.

Windle, J. (2018) Fundraising, organised crime and financing terrorism. In Silke, A. (ed.) *Routledge Handbook of Terrorism and Counterterrorism*. 1st edition. [Online]. Abingdon, Oxon; New York, NY: Routledge, 2018.: Routledge. pp. 195–206.

Windle, J., Morrison, J.F., Winter, A. and Silke, A. (2018) *Historical perspectives on organized crime and terrorism*. Routledge SOLON explorations in crime and criminal justice histories. Routledge.

Windle, J. and Silke, A. (2019) Is drawing from the state `State of the art'?: A review of organised crime research data collection and analysis, 2004–2018, *Trends in Organized Crime*. 22, 4, 394–413.

de Winter, J.C.F., Zadpoor, A.A. and Dodou, D. (2014) The expansion of Google Scholar versus Web of Science: a longitudinal study, *Scientometrics*. 98, 2, 1547–65.

Winter, T. (2018) *Boston Marathon bomber confessed to FBI agents in handwritten notes*. [Online]. 23 October 2018. NBC News.

Wong, K. (2010) *Patriotic 'Hacktivist' Claims He Took Down Wikileaks Site*. [Online]. 30 November 2010. ABC News.

Wood, F., Ford, N. and Walsh, C. (1994) The effect of postings information on searching behaviour, *Journal of Information Science*. 20, 1, 29–40.

Woodward, V.H., Webb, M.E., Griffin, O.H. and Copes, H. (2016) The Current State of Criminological Research in the United States: An Examination of Research Methodologies in Criminology and Criminal Justice Journals, *Journal of Criminal Justice Education*. 27, 3, 340–61.

Wray, S. (1998) Electronic civil disobedience and the World Wide Web of hacktivism, *Nova Iorque*.

Wray, S. (1999) On electronic civil disobedience, *Peace Review*. 11, 1, 107–11.

Wright, C. (2008) Evolution of Information Systems. In Wright, C. (ed.) *The IT Regulatory and Standards Compliance Handbook*. [Online]. Burlington: Syngress. pp. 25–41.

Wright, R.A. (1998) The most-cited scholars in criminology and criminal justice textbooks, 1989 to 1993, *The Justice Professional*. 10, 3, 309–22.

Wu, L., Peng, Q. and Lembke, M. (2023) Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database, *International Journal of Cybersecurity Intelligence & Cybercrime*. 6, 1, 5–28.

Yannakogeorgos, P.A. (2014) Rethinking the threat of cyberterrorism, *Cyberterrorism*.

Yar, M. (2005a) Computer Hacking: Just Another Case of Juvenile Delinquency?, *The Howard Journal of Criminal Justice*. 44, 4, 387–99.

Yar, M. (2005b) The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, *European Journal of Criminology*. 2, 4, 407–27.

Yar, M. (2013) *Cybercrime and society*. Sage.

Yar, M. and Steinmetz, K. (2017) *Cybercrime and Society*. June. 1st edition. [Online].

Yar, M. and Steinmetz, K.F. (2019) *Cybercrime and Society*. 2nd edition. SAGE.

Youngman, M. (2020) Building "Terrorism Studies" as an Interdisciplinary Space: Addressing Recurring Issues in the Study of Terrorism, *Terrorism and Political Violence*. 32, 5, 1091–105.

Yunos, Z., Ahmad, R. and Mohd Sabri, N.A. (2015) A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia, *Information Security Journal: A Global Perspective*. 24, 1–3, 15–23.

Zetter, K. (2014) Sony Got Hacked Hard: What We Know and Don't Know So Far. *Wired*. [Online].

Zhang, N. (2014) Web-based backpacking communities and online activism in China: Movement without marching, *China Information*. 28, 2, 276–96.

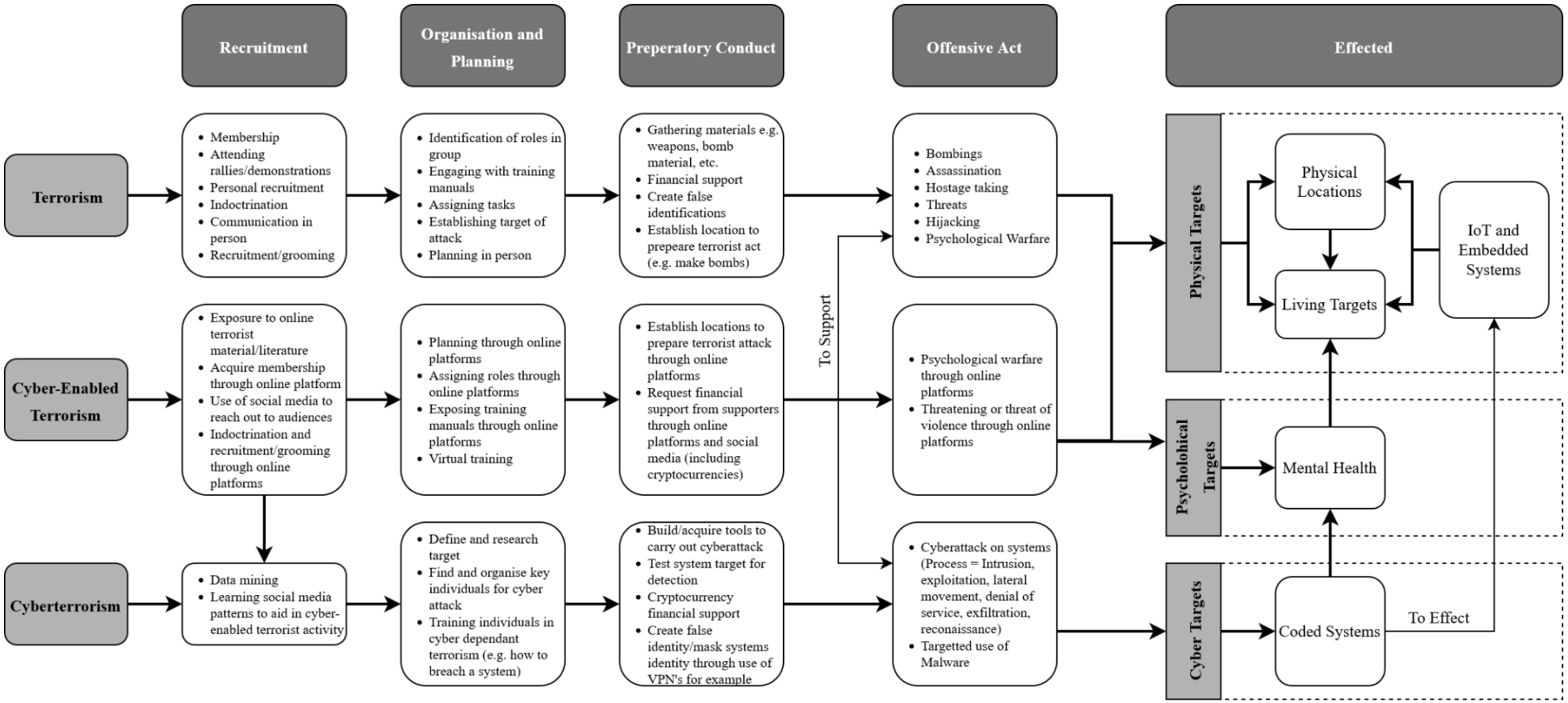
Zuccala, A. (2006) Modeling the invisible college, *Journal of the American Society for information Science and Technology*. 57, 2, 152–68.

Züger, T. (2013) Re-thinking civil disobedience, *Internet Policy Review*. 2, 4.

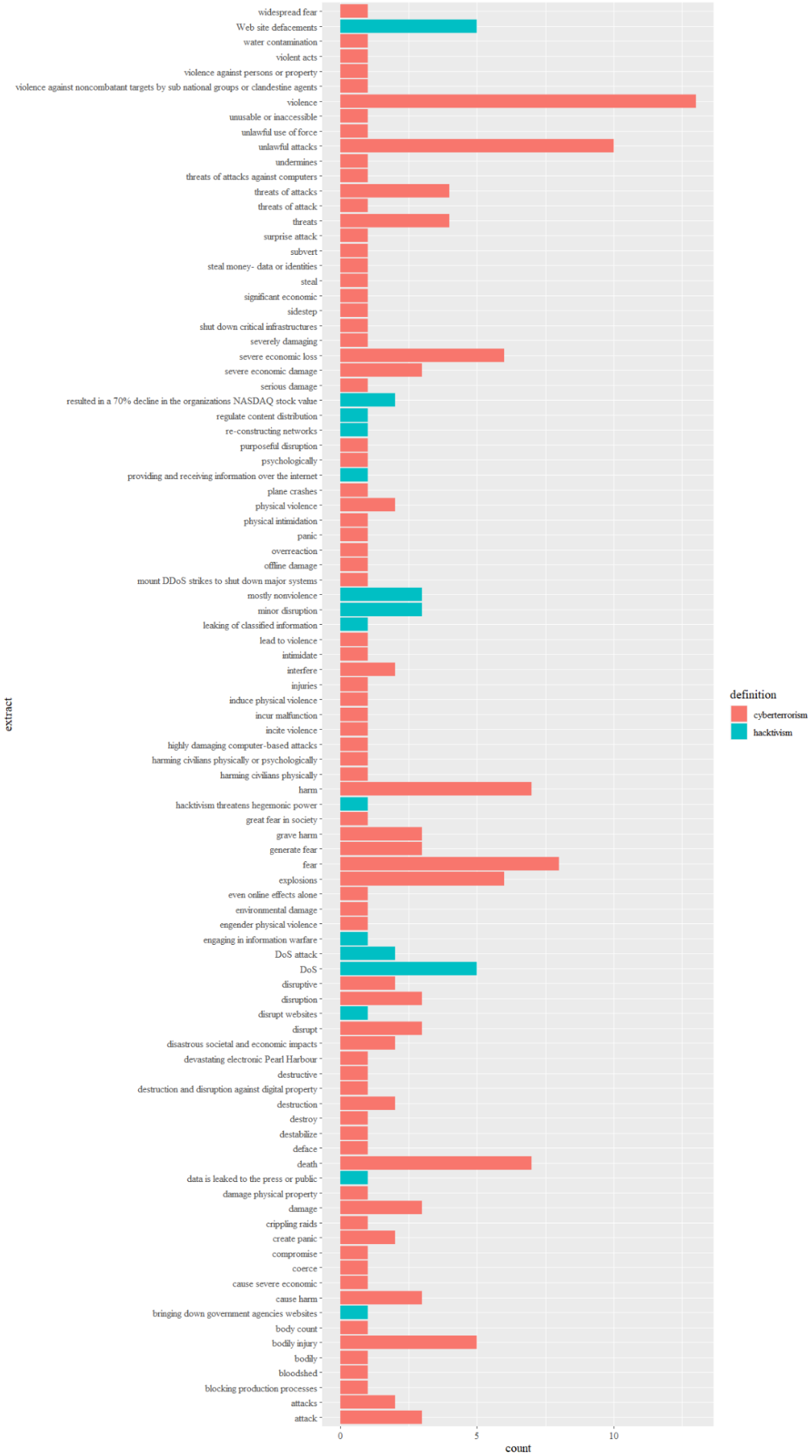
Zupic, I. and Čater, T. (2015) Bibliometric Methods in Management and Organization, *Organizational Research Methods*. 18, 3, 429–72.

Appendix

Appendix: 1 Modified Terrorist Activity Framework (see: Figure 9.2: 97)



Appendix 2: Total Frequency Distribution of Coded Effect Terms (see figure 5.29: 271)



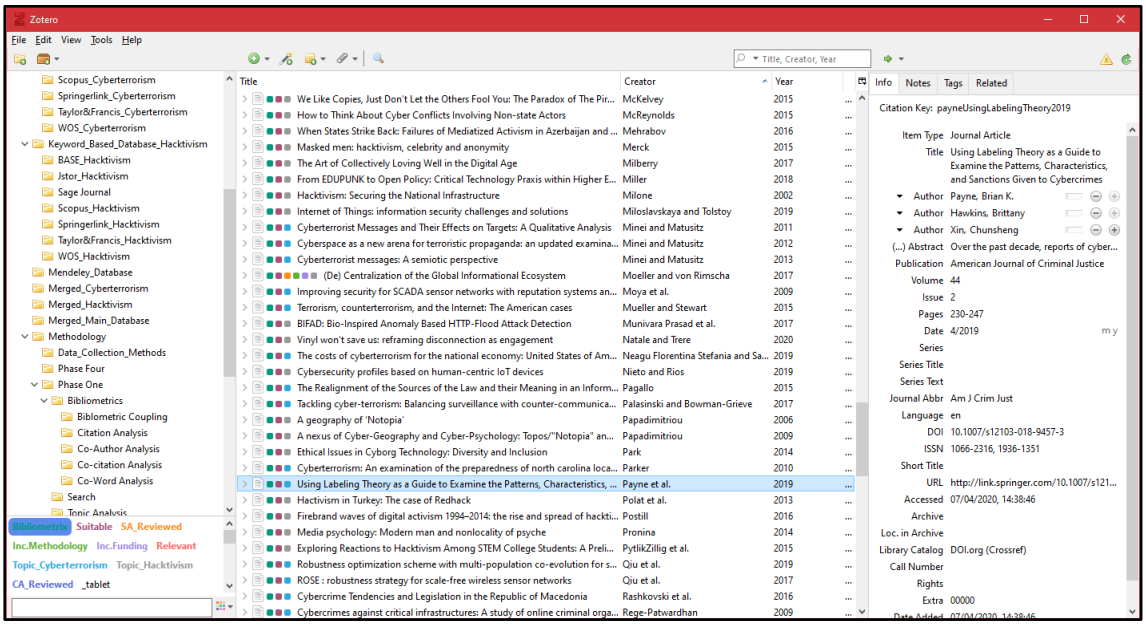
Appendix 3: Example of Bibliographic Database

	A	B	H	I	J	K	L	M	N	O	P	Q	
1	id	definition	year	author	title	gs_citation	refs.denning200	references	journal	url	abstract	issue	vol
2	CERQGQ33	Cyber-Enabled	2003	Anderson, Alison G.	Risk, terrorism, and the internet	39	1		Knowledge, Technol	https://dc	This paper examir	2	
3	HGBQ6RUY	Cyber-Enabled	2015	Argomaniz, Javier	European Union responses to terrorist use of the Internet	45	0	Argomaniz, J., (2011	Cooperation And Conflict		The Internet has l	2	
4	9MPRFEN5	Both	2016	Ayres, Nicholas; Maglaras,	Cyberterrorism targeting the general public through social	14	0	(1990) Computers a	Security And Communication I		Current literature	15	
5	25QKI5E7	Hacktivism	2016	Bakioğlu, Burcu S.	The gray zone: Networks of piracy, control, and resistance	14	0	Beck, U., (1997) The	The Information Soc	https://dc	Taking Operation	1	
6	QE5KXU32	Hacktivism	2016	Beck, Christian	Web of resistance: Deleuzian digital space and hacktivism	24	0	Berlatsky, N., Hashta	Journal For Cultural	https://dc	This article argues	4	
7	LMKWVZ5Y	None	2014	Beyer, Jessica L.	The Emergence of a Freedom of Information Movement: A	118	0	Ahrens, F., U.S. joins	Journal Of Compute	https://w	Online rhetoric al	2	
8	XSAQWQFW	Hacktivism	2014	Bodó, B.	Hacktivism 1-2-3: How privacy enhancing technologies cha	18	0	Adorno, T.W., Horkh	Internet Policy Revie	https://w	This short essay e	4	
9	MAYACSA5	Cyberterrorism	2018	Boys, James D.	The Clinton administration's development and implement	11	0		Intelligence And National Secu		The concept of ar	5	
10	727N3JUJ	Cyber-Enabled	2017	Brantly, Aaron	Innovation and adaptation in jihadist digital security	18	0	Weimann, G., Cyber	Survival		With a small num	1	
11	7MQ6L89R	Cyberterrorism	2006	Brenner, S.W.	Cybercrime, cyberterrorism and cyberwarfare	21	0	Brenner, S.W., Towar	Revue Internationale	https://w	Taxonomy is esse	3	
12	XQD73XMV	None	2013	Brenner, Susan W.	Cyber-threats and the Limits of Bureaucratic Control	29	0		Minnesota Journal C	http://pu	For over half a decade, the auth		
13	F74QFJV2	Hacktivism	2018	Bustard, John D.	Improving Student Engagement in the Study of Profession	11	0	Alinsky, S., (2010) Ru	Science And Enginee	https://dc	In spite of the ack	2	
14	4XNDJHG3	Hacktivism	2013	Cammaerts, Bart	Networked Resistance: The Case of WikiLeaks	48	0	Ackerman, J.M., San	Journal Of Computer-Mediate		In this article, Wil	4	
15	JV48IBJ7	None	2006	Carducci, Vince	Culture Jamming: A Sociological Perspective	251	0	(2005) Adbusters, , I	Journal Of Consume	https://dc	'Culture jamming	1	
16	33KUJXML	Both	2012	Cassim, Fawzia	Addressing the spectre of cyber terrorism: a comparative p	22	1		Potchefstroom Elect	http://hdl	This article looks	2	
17	JKIIK8PM	Cyberterrorism	2008	Cavelty, Myriam Dunn	Cyber Terror: Looming Threat or Phantom Menace? The Fr	179	1		Journal Of Informati	10.1300/J	For some years, e	1	
18	8HXTXTET	Hacktivism	2017	Chandler, David	Securing the Anthropocene? International policy experime	32	0		Security Dialogue	https://dc	This article analys	2	
19	6YLFS8XW	None	2008	Choo, Kim-Kwang Raymonc	Organised crime groups in cyberspace: a typology	167	0	Abelson, J., Breach c	Trends In Organized	https://dc	Three categories	3	
20	CBRMLKAL	Cyber-Enabled	2008	Choo, Kim-Kwang Raymonc	Criminal Exploitation of Online Systems by Organised Crim	128	0	Ahmad, R., Slashing	Asian Journal Of Cri	https://dc	This article consic	1	
21	6VSMZ57V	Cyberterrorism	2011	Chu, Hai-Cheng; Deng, Der-	Potential cyberterrorism via a multimedia smart phone ba	10	0	Ahmed, R., Dharaska	Multimedia Systems		Cyberterrorism ha	4, SI	
22	5IL6BXRB	None	2009	Chu, Hai-Cheng; Deng, Der-	Next Generation of Terrorism: Ubiquitous Cyber Terrorism	13	1	Anson, S., Bunting, S	Journal Of Universal Computer		It is an urgent, im	12	
23	Z68ZW42F	None	2019	Coleman, Gabriella	How has the fight for anonymity and privacy advanced sin	13	0		Media Culture & Soc	https://w	This article exami	4	
24	X7ILWQWY	Hacktivism	2003	Conway, Maura	Hackers as terrorists? Why it doesn't compute	40	0		Computer Fraud An	http://doi	The bulk of this a	12	
25	SMWXUU8K	Cyberterrorism	2003	Conway, Maura	Cyberterrorism: The Story So Far	31	0		Journal Of Informati	https://w	This paper is conc	2	
26	6BJ8V76M	Cyberterrorism	2002	Conway, Maura	Reality bytes: cyberterrorism and terrorist 'use' of the Inte	126	1	Arquilla, J., Ronfledt	First Monday	http://doi	This paper examir	11	
27	KDEENNWA	Cyberterrorism	2011	Conway, Maura	Against Cyberterrorism: Why cyber-based terrorist attacks	45	1	Cavelty, M.D., Cyber	Communications Of	http://doi	Like the 2007 cyb	2	
28	2MW3UW3P	Cyberterrorism	2010	COTTIM, Armando	Cybercrime, Cyberterrorism and Jurisdiction: An Analysis c	14	0		European Journal Of	http://hdl	handle.net/1814/	15118	
29	AY4DC8CB	Cyberterrorism	2015	Cox, Christopher	Cyber Capabilities and Intent of Terrorist Forces	16	0	(2002), http://www.	Information Security	https://doi	org/10.1080/19	43891	
30	FDXGQPGZ	None	2007	Crews, Clyde Wayne	Cybersecurity and Authentication: The Marketplace Role i	12	0		Knowledge, Technol	http://link	springer.com/10.	2	
31	2LTQBBF7	Both	2000	Denning, Dorothy E.	Activism, hacktivism, and cyberterrorism: the Internet as a	734	0	B. Colin., The Future	Computer Security J	https://w	Using news repor	3	
32	6MY9TGKU	Hacktivism	2017	Deseriis, Marco	Hacktivism: On the Use of Botnets in Cyberattacks	34	0	Assange, J., (2012) C	Theory, Culture & Sc	https://dc	This article offers	4	
33	KMK2MNFN	Cyberterrorism	2003	Desouza, K.C; Hensgen, T.	Semiotic emergent framework to address the reality of cyb	52	1	Forno, R., (2000) Shi	Technological Foreca	https://w	The following pap	4	
34	THBSAPAW	Cyberterrorism	2002	EMBAR-SEDDON, AYN	Cyberterrorism: Are We Under Siege?	118	0		American Behaviora	10.1177/(	There is considera	6	
35	PR7HN8IN	Cyberterrorism	2005	Emery, N. E.	The Myth of Cyberterrorism	36	1		Journal Of Informati	https://w	[Media and emer	1	

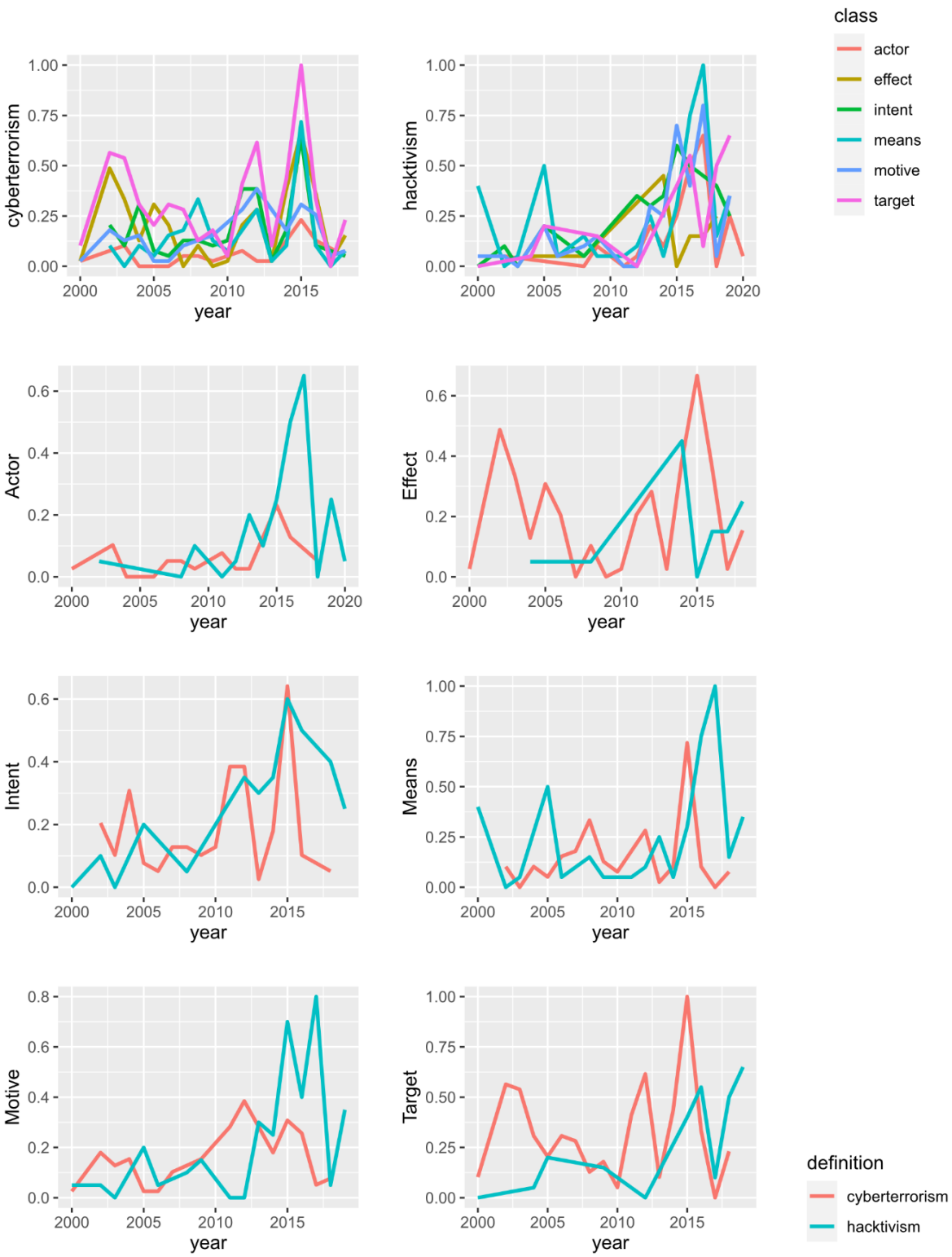
Appendix 4: Example of Definitions Database

	A	C	D	E	F	G	H	I
1	id	definition	unique	type	citation_1	citation_2	citation_3	citation_4
8	3FMR7LUS	Today, cybercriminals have modified Ransomware for different purposes. In addition to a ransom request, they have succeeded in developing Ransomware for the purpose of cyberterrorism and intimidating the political and official authorities through illegal harmful attacks to the computers and databases of official units.	Yes	proposed				
9	IXQFEJVM	To sum up all these it can be said that cyber-terrorism is an aggressive and destructive activity appearing at the meeting point of traditional terrorism and cyberspace. They usually mean attacks and threats against the computer networks and computers as well as against the information flowing or stored on them by which the cyber-terror groups or individuals intend to achieve their political or other goals.	Yes	proposed				
10	FCV4XRD9	These objectives can be social, political, ideological, financial, religious, and so on. Because our dependence on electronic networking has inflated considerably, cyberterrorism has become a serious threat to both public and private infrastructures (Axelrod, 2009; Matusitz, 2008).	No	consolidated	Axelrod, 2009	Matusitz, 2008		
11	AY4DC8CB	Therefore, in order to qualify as cyber terrorism, an act must be committed which furthers the goals of terrorism using or targeting the medium of cyber space.	Yes	proposed				
12	VBSDU96Q	Their weapons include viruses, Trojan horses, and other types of malicious software. Generally, a cyberterrorist has the same goal as a conventional terrorist: to coerce people or their government to achieve specific political, ideological, or similar objectives (Clem et al. 2003, p. 272).	No	qouted	Clem et al. 2003			
13	TVXQVTMQ	The very definition of cyberterrorism refers to Internet use, technology, and computer-based networks against critical infrastructures (Conway, 2002; Matusitz, 2008a, 2008b).	No	consolidated	Conway, 2002	Matusitz, 2008a, 2008b		
14	7L7BFP2V	The U.S. National Conference for State Legislatures (NCSL) defined "cyberterrorism" as "The use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically."8	No	qouted	U.S. National Conference for State Legislatures (NCSL)			
15	LAIB44Y7	The threat of cyber terrorism is more dangerous than that of common information security attacks (Rogers, 1999; Verton, 2003).	No	consolidated	Rogers, 1999	Verton, 2003		
16	TNZ5X8LM	The term cyberterrorism refers to all acts that combine forms of terrorism and cyberspace. It was first introduced by Colin (1997).	No	qouted	Collin, 1997			

Appendix 5: Example of Zotero Database



Appendix 6: Overview of Taxonomic Classification Distribution



Appendix 7: Taxonomy Network Distribution of Classifications and Terms

