The Digitalised Terrorism Ecology: A Systems Perspective

Nixon Muganda Ochara
Research Professor, School of Management Sciences, University of Venda, Thohoyandou, South Africa; and Research Associate, LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://orcid.org/0000-0001-5736-7901

Nancy Achieng Odhiambo
Doctoral Candidate, Department of Business Information Systems, School of Management Sciences, University of Venda, Thohoyandou, South Africa
https://orcid.org/0000-0002-3123-7305

Armstrong Kadyamatimba
Dean and Professor, School of Management Sciences, University of Venda, Thohoyandou, South Africa
http://orcid.org/0000-0002-9638-0858

Abstract
This study uses a systematic review methodology to interpret existing literature on the digital dimensions of contemporary terrorism and counter-terrorism. Using the theory of synergetics as a guiding analytical framework, the study conducts meta-synthesis of relevant literature, including application of soft systems methodology (SSM), in order to generate conceptualisation of a digitalised terrorism ecology. This ecology comprises five interacting sub-systems: open digital infrastructure; digital information ecology; digital terrorism enactment; digital capabilities; and digital enslavement.

Keywords
digital technologies, digitalisation, terrorism, counter-terrorism, synergetics, soft systems methodology (SSM), sociomateriality, digitalised terrorism ecology, open digital infrastructure, digital information ecology, counter power, digital terrorism enactment, digital enslavement

DOI: https://doi.org/10.23962/10539/29196

Recommended citation
Ochara, N. M., Odhiambo, N. A., & Kadyamatimba, A. (2020). The digitalised terrorism ecology: A systems perspective. *The African Journal of Information and Communication (AJIC), 25*, 1-19. https://doi.org/10.23962/10539/29196

1. Introduction

Countering terrorism remains a priority for national governments throughout the world. The Global Terrorism Index (GTI) report of 2018 reported that deaths from terrorism events fell by 27% between 2016 and 2017, a third consecutive year of decline. However, the same GTI report stated that every region of the world had recorded a higher average impact of terrorism in 2017 compared to 2002. Evidence also suggests that the nature of terrorism is becoming increasingly complex. For instance, while the dominant view of global terrorism is that it is largely fuelled by Muslim extremism, the 15 March 2019 attack on two Muslim mosques in New Zealand pointed to the increasing prominence of far-right movements as a source of terrorism (Hawi, Osborne, Bulbulia, & Sibley, 2019). Such instances involving right-wing extremists suggest the changing nature of terrorism, with drivers anchored not only in religion, but also in culture, the economy, politics, globalisation, and various forms of media (Sirgy, Estes, El-Aswad, & Rahtz, 2019).

While the nature of the terrorism ecosystem has been changing, research and counter-terrorism responses have retained a strong focus on Al-Qaeda and jihadist terrorism generally; have remained event-driven; and have under-emphasised the roles of digital technologies, state-sponsored terrorism, and right-wing extremists (Asongu, Nnanna, Biekpe, & Acha-Anyi, 2019; Schuurman, 2019). This under-emphasis on the actual current dynamics of terrorism provided the justification for this study, which sought to develop a nuanced understanding of the contemporary terrorism ecology, with particular attention to the ecology's digital dimensions.

McLuhan, writing in the 1960s (see McLuhan, Gordon, Lamberti, & Scheffel-Dunand, 2011), foresaw that technological ecosystems are not passive containers, and are, rather, active processes that reshape people and technologies alike. This insight is particularly meaningful in our contemporary world, in which, in July 2019, it was estimated that more than 4.33 billion people (approximately 56% of the world's population) were active internet users (Statista, 2019). Such pervasiveness of digital technologies cannot help but have a reshaping dynamic in human life.

Digital ecology approach

We adopted a digital ecology approach for this study (see García-Marco, 2011), which is an approach that can unravel and capture the complexity of the various interacting sub-systems and processes that characterise terrorism's macro-systems. The digital ecology approach evolved from the notion of information ecology, and is a systems approach that seeks to understand the ways in which societies and their knowledge and communication are being shaped by digital technologies. The approach has been used, inter alia, to analyse the evolution of the World Wide Web (Huberman, 2003), digital libraries (García-Marco, 2011), social communities on the internet (Finin et al., 2008), and e-government (Ochara, 2014). Our study applied the digital ecology approach in order to develop an understanding of how digitalisation is influencing the structuring of terrorism ecologies.

Theory of synergetics

We used the theory of synergetics (Haken, 1984) as a structuring device for our study. Synergy, in the systems theory context, denotes a conceptual or mathematical product of causes (or factors), and is used in many sciences as a general model to account for non-linear change (Schmitt, Eid, & Maes, 2003). According to Haken (1984), the five core properties of the theory are:

- order parameters (macroscopic patterns);
- control parameters;
- internal and external system constraints;
- internal and external parameters and system elements; and
- environment.

As will be seen below, we used these five core properties of synergetics as the main tools for structuring our research and findings.

2. Research methodology

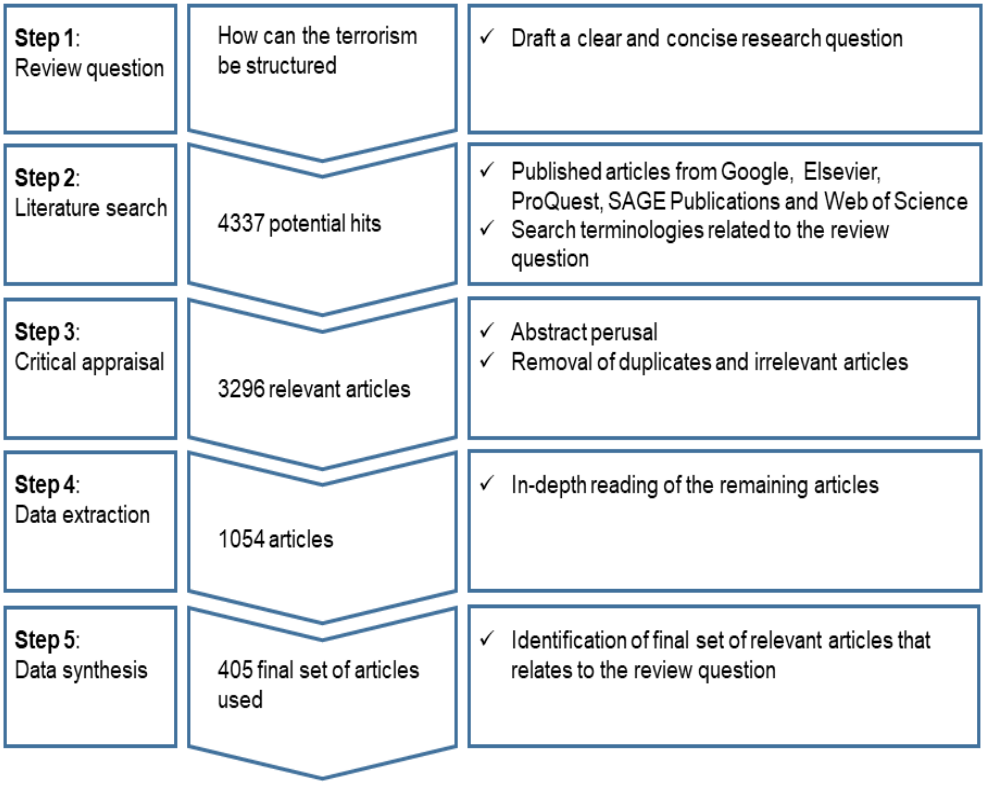
We used the systematic literature review method in order to identify the most relevant literature on how digitalisation interweaves with terrorism and counter-terrorism. Both peer-reviewed sources (e.g., journal articles, scholarly books), and non-peer-reviewed sources (non-scholarly books, media articles, blogs, reports, websites and videos) were used as data sources for the systematic literature review. We used scholarly electronic databases such as Elsevier, ProQuest, SAGE Publications and Web of Science for peer-reviewed content, and Google for non-peer-reviewed sources. Table 1 presents the key search terms that were used.

Table 1: Key search terms

Terrorism	Extremism	Ideology AND Terrorism
Counter-Terrorism	Radicalization	Definition of Terrorism
Religion AND Terrorism	Policies AND Terrorism	Technology AND Terrorism
Root Causes of Terrorism	Forms of Terrorism	Counter-Terrorism AND Technology
Radicalization AND Terrorism	Poverty AND Terrorism	Terrorism AND Facebook
Terrorism AND modus operandi	Governance AND Terrorism	Terrorism AND Twitter
Terrorism AND Internet	Terrorism AND YouTube	Terrorism AND Social Media
Counter-Terrorism AND Twitter	Counter-Terrorism AND Training	Counter-Terrorism AND Social Media
Research AND Terrorism	Europe AND Terrorism	Terrorism AND USA
Africa AND Terrorism	Human Rights and Terrorism	Terrorism Organizations
Terrorism AND ISIS	Terrorism AND Al-Qaeda	Terrorism AND Osama
Terrorism AND Al-Shabaab	Terrorist Groups	Terrorism AND Propaganda
Terrorism AND Recruitment	Terrorism AND Training	Counter-Terrorism AND Organisational Culture
Counter-Terrorism AND Collaboration	Terrorism AND Media	Counter-Terrorism AND Institutional Rivalry
Counter-Terrorism AND Organisational Structure	Counter-Terrorism AND Policy	Counter-Terrorism AND Human Rights
Community Policing AND Terrorism	Terrorism and Boko Haram	Counter-Terrorism AND Boko Haram
Counter-Terrorism AND Media	Counter-Terrorism AND Facebook	Counter-Terrorism AND YouTube

The search focused mainly on English-language content published since 11 September 2001, the date of the "9/11" terrorist attacks in the United States that fundamentally changed both academic and non-academic treatments of the topic of terrorism. Our search produced 4,337 documents. We applied an inclusion and exclusion process through which we removed duplicates, scanned through the titles and abstracts of the identified documents, and checked through the references sections of the identified documents to identify whether more documents could be included in the list. This process resulted in a final dataset of 405 documents (see Figure 1).

Figure 1: Process followed to identify the 405 documents



Meta-synthesis

We then evaluated the articles via meta-synthesis, a qualitative methodology for synthesising outcomes of several studies that are similar in topic or outcome measure (see Park & Gretzel, 2007). Informed by Ochara's (2013) guidelines for application of theory in research, our meta-synthesis was focused on dividing the 405 documents according to their relevance to the five components of the theory of synergetics (Haken, 1984) outlined above: order parameters (macroscopic patterns); control parameters; internal and external system constraints; internal and external parameters and system elements; and environment.

Thematic analysis

All 405 documents were then subjected to thematic analysis, a qualitative technique that consists of delineating the data according to its thematic patterns and then assigning codes to the themes (see Alhojailan, 2012). For this thematic analysis, we used the NVivo software, and applied the CATWOE soft systems methodology (SSM). CATWOE is a mnemonic representation of six elements that, when

considered, can aid conceptualisation of problems, and responses to problems (Checkland, 1981, pp. 224–225):

- customers;
- actors;
- transformation;
- worldview;
- owners; and
- environmental constraints.

We chose an SSM methodology because such methodologies are suitable for addressing real-world, complex, and poorly-structured problems—and terrorism is a problem of that sort. Terrorism is often associated with, inter alia, fundamentalism and radicalisation (see Hafez & Mullins, 2015), religious intolerance (see Doosje et al., 2016), and political and civil instability (see Kagwanja, 2006).

Rittel and Webber (1973) refer to certain problems that are unstructured or poorly structured, and that are irregular, complex, novel and adaptive in nature, as "wicked". The problem of terrorism fits this category. Such problems require that they first be clearly defined and structured before a resolution can be proposed (Dunn, 2015), and SSM tools help in the process of defining and structuring problems.

3. Findings

Meta-synthesis results

Table 2 shows the distribution of the 405 documents when we delineated them according to their relevance to the five components of the theory of synergetics.

Table 2: Data categorisation in terms of theory of synergetics

Components	First-order themes	No. of articles
Order parameters (macroscopic patterns)	✓ dominant ideology ○ philosophy ○ root causes ✓ policies ✓ open models of information-sharing ○ collaboration ○ sharing economy ✓ open technology platforms	94
Control parameters	✓ regional economic imbalance ○ poverty and grievances ○ extremism ✓ poor governance ✓ technology (media and internet)	73

Internal and external system constraints	✓ institutional rivalry ✓ organisational perspectives ○ norms and values ○ roles and responsibilities	18
Internal and external parameters and system elements	✓ complexity of inter-organisational cognitive behaviour ✓ complexity of cross-organisational competencies ✓ collective intelligence ✓ open governance models ○ collaboration ○ transparency ✓ participation	71
Environment	✓ definitions of terrorism ✓ multiple agencies ✓ changing modes of attack ✓ improved access to, and availability of, technology	149

The distribution of these articles was considered sufficient to allow for the SSM approach to be applied.

Thematic analysis results

Braun, Clarke, and Terry (2014) call for three steps to be followed when conducting thematic analysis of data: familiarisation, generation of initial codes, and theme search. We applied the six elements (presented above) of the CATWOE SSM in performing these three steps. We produced a thematic word cloud visualisation (Figure 2) based on the initial thematic "nodes" generated by the NVivo qualitative data analysis software.

Figure 2: Thematic word cloud

Our thematic analysis also produced a table summarising high-level themes (Table 3) in terms of the six CATWOE categories, with the focus of the thematic analysis being the digitalised terrorism ecosystem.

Table 3: Second-order themes identified in terms of CATWOE

C	Customers	government, state, community, individuals, terrorists, Al-Qaeda, ISIS, people, public, group, organisations, society, companies, human, university, international, countries
A	Actors	technology, social media, Twitter, Facebook, computer and internet, community, government, websites, organisations, video, system, digital, political, police, press, human, university, media, social, computer, people, individuals, society, community
T	Transformation	policy, strategy, communication, frameworks, analysis, content, activities, technologies, data, work
W	Worldview	Islamic, political, national, privacy, rights, counter-terrorism, surveillance, terrorism
O	Owners	technology, social media, Twitter, Facebook, computer and internet, government, community, organisations, videos, journalists, companies, system, digital, police, press, university, media, information, social, online, computer
E	Environmental constraints	support, attacks, material, violence, services, intelligence, effective, strategy, threat, techniques, news, approach, information, terror, privacy, enforcement, program, cyber terrorism, war, AI, struggle, propaganda

In a CATWOE SSM analysis, *customers* are the beneficiaries or victims affected by the system under consideration (Checkland & Scholes, 1990). What becomes apparent in Table 3 above is the wide range of individuals and groups who are either beneficiaries or victims within the digitalised terrorism ecosystem. In CATWOE, *actors* are the agents who carry out the main activities of a system (Checkland & Scholes, 1990). In Table 3, what is apparent in this category is the dominance of digital technology themes.

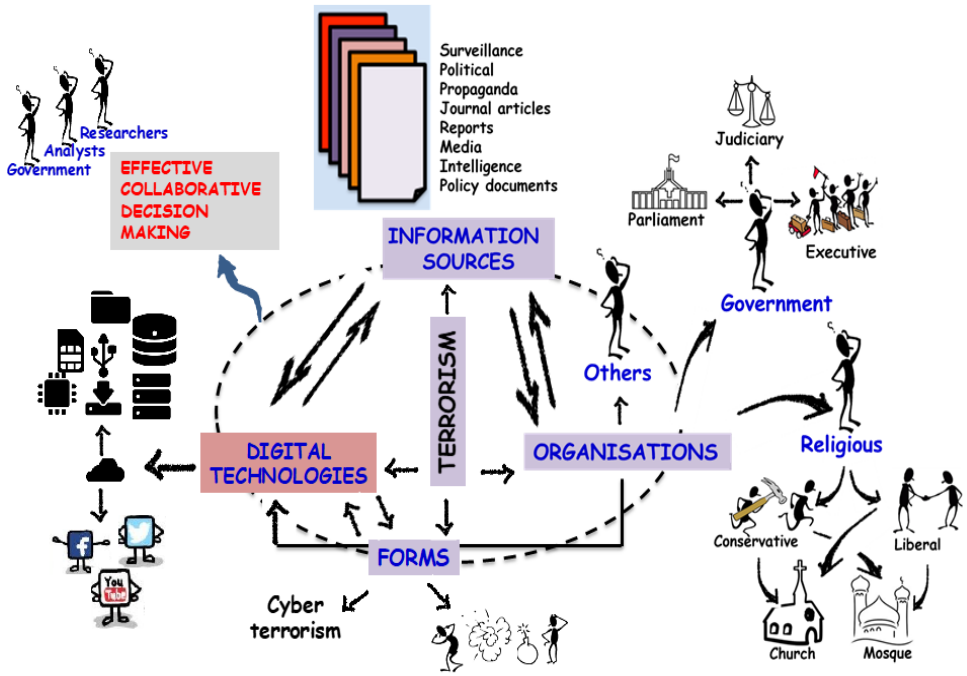
The third aspect of CATWOE, *transformation*, focuses on purposeful activities undertaken by the actors with the aim of solving a problem (Checkland & Scholes, 1990). In the context of the digitalised terrorism ecosystem, we treated transformation as a process, or set of artefacts, that influences the evolution, nature and forms of interactions among the multiple stakeholders in the ecosystem.

The *worldview* in CATWOE is connected to an individual's worldview and beliefs, and gives transformation meaning (Bergvall-Kåreborn, Mirijamdotter, & Basden, 2004). We see in Table 3 that themes related to the ethos of religion, politics, nationalism, digital rights, and responses to the terrorism problem were prevalent

in the 405 documents analysed. The *owners* are those with the power to either stop the transformations or allow them to take place (Checkland & Scholes, 1990). *Environmental constraints* are considered as the internal or external limitations that can hinder transformation (Bergvall-Kåreborn, Mirijamdotter & Basden, 2004). In Table 3, we see a multitude of constraints identified.

This SSM-oriented thematic analysis also produced the "rich picture" shown in Figure 3, which we used as a precursor to the conceptual model based on the theory of synergetics (Figure 4).

Figure 3: Rich picture



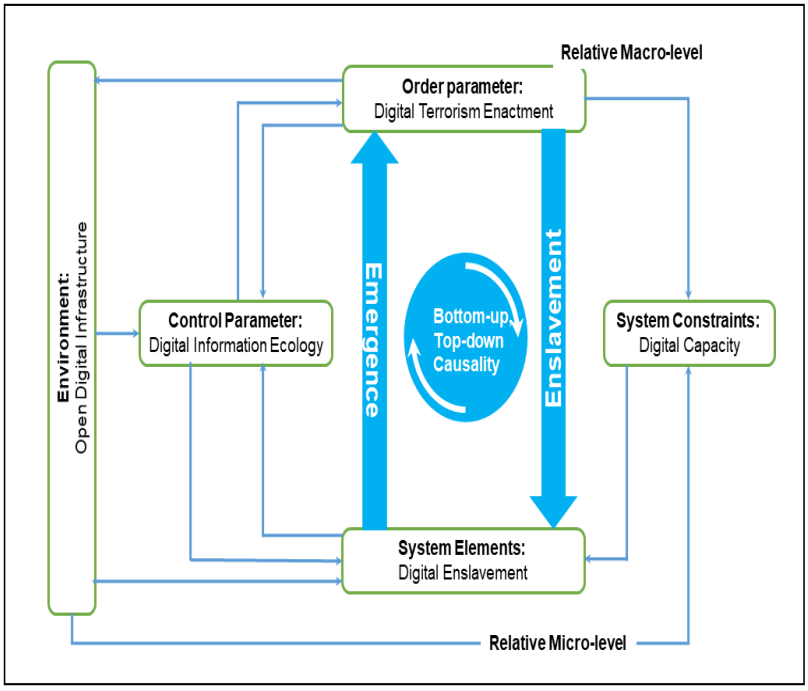
In Figure 3, we see, from a problem-structuring perspective, the pervasive role of digital technology in human systems—a finding that resonates with the sociomateriality literature (see Cecez-Kecmanovic et al., 2014), and with how technology affordances and capabilities play a critical role in agency (Weißenfels, Ebner, Dittes, & Smolnik, 2016). For instance, Daniel, Hartnett, and Meadows (2017) forcefully argue that social media's democratising affordances are evident in the transformation of power structures from top-down to much more bottom-up power.

Figure 3 also accentuates the importance of an understanding of information sources as essential for the development of state understandings of new, varied forms of terrorism, and of evolving state policies and strategies for countering terrorism. With increased online access to information, terrorists can develop counter-strategies to governments' counter-terrorism efforts. In addition, increased online information dissemination has empowered terrorist groupings such as ISIS and Al-Qaeda in their efforts to advance propaganda and recruit new members.

Conceptual model of the digitalised terrorism ecology

Grounded in the theory of synergetics, Figure 4 depicts the *digitalised terrorism ecology* model that we derived from the thematic analysis, with the model set out in terms of the five core properties, as explained earlier, of the theory of synergetics.

Figure 4: Digitalised terrorism ecology



Viewed through the synergetics lens, the documents provided evidence that the structuring process of terrorism starts with an external activation from what we term, in Figure 4, the *digital information ecology*. This digital information ecology context kindles a behavioural change process among terrorism genres at the level of system elements, which in turn leads, or may lead, to the emergence of new terrorism policies (e.g., community policing, counter-terrorism strategies) at the macroscopic level of the order parameter. These new terrorism policies result, in turn, in what we term, in

Figure 4, *digital enslavement* of the system elements (e.g., individual terrorists who feel compelled to adopt particular patterns of behaviour).

4. Analysis

We now analyse the findings of the systematic literature review in terms of components from the theory of synergetics deployed in Figure 4, in the following order:

- environment;
- control parameter;
- order parameter;
- system constraints; and
- system elements.

Environment: Open digital infrastructure

A critical underlying principle for digitalised self-organisation is the openness of systems, which allows for power to be added throughout the environment. In our analysis, the *open digital infrastructur*e is the core construct that undergirds the emergence of terrorism in its current form. Even a casual analysis reveals that in all aspects (severity, magnitude, operations), the "structure" of terrorism has become more complex since its emergence in the 1960s and 1970s. We attribute this dramatic change in the nature of terrorism to the advent of the internet infrastructure (Denning, 2010; Benson, 2014), due in large part to its characteristic openness, which enhances networking and increases terrorism capability.

The identification above of the central role of digital technologies confirms the dominant view that the emergence of wider digital sociomaterial infrastructures such as the internet are reshaping society (Merali, 2006), with implications for increased global terrorism (Gillespie, Osseiran, & Cheesman, 2018). Therefore, we view the current sociomaterial digital infrastructure as the environmental nexus that continues to "structure" the terrorism ecology.

The open nature of digital infrastructure is recognised as underpinning newer digitalisation paradigms such as cloud computing, big data, transparent computing, and nomadic computing (Odero, Ochara, & Quenum, 2017). To understand the nature of the influence of open digital infrastructure on terrorism ecologies, we adopt the perspective of technology affordance to reify the potentials of the emerging features of such newer digital technologies and infrastructures. From a relational perspective, based on social interactions that shape and are shaped by the technology and the context (Carugati, Fernández, Mola, & Rossignoli, 2018), the evolving open digital infrastructure for terrorism emphasises the fact that the focus should not be on the features that digital technologies possess, but rather on how actors' goals and capabilities can be related to the inherent potential offered by the features (Autio, Nambisan, Thomas, & Wright, 2018).

Thus, the locus of the environmental aspect of the open digital infrastructure places, at the fore, how open and flexible affordances of digital technologies enable "newer" manifestations of the digital information ecology (the control parameter, as explained below), which occasion change in behaviour within terrorism ecologies. The dominant affordances that facilitate the engagement of terrorism ecologies with the open digital infrastructure as an enabler of the digital information ecology are social media vehicles such as Facebook, Twitter, and Instagram (see the CATWOE and rich picture analyses above), empowered by social software and algorithms, and enabled by smart devices (Tuten & Mintu-Wimsatt, 2018). Certainly, prior research entrenches social media vehicles as the core proxy for open digital infrastructure (Paganini, 2016; Blaker, 2015; Plantin, Lagoze, Edwards, & Sandvig, 2018), with characteristics of the sharing economy and open digital technology platforms influencing contemporary information ecologies of terrorists. The sharing economy, or gig economy, is seen as the most predominant contemporary organising principle influencing how human beings share knowledge and assets, enabled by the increased connectivity, scale, speed, and transparency of the internet (Burtch, Carnahan, & Greenwood, 2018).

Control parameter: Digital information ecology and digital counterpower

The environmental influence of open digital infrastructure enables the control parameter: the *digital information ecology*. The evolution of the digital information ecology, as a control parameter, can be explained using the concept of digital "counterpower" as used by Castells. According to Castells (2011, p. 773), "[…] wherever there is power, there is counterpower, enacting the interests and values of those in subordinate positions". We use the notion of digital counterpower to interpret the link between the first-order themes that emerged from application of the theory of synergetics and the second-order themes that emerged from application of CATWOE.

The first-order themes that were identified (Table 2) emphasised poor governance and regional economic imbalances that fuel and entrench poverty, grievances, and extremism. Furthermore, technology (particularly digital media and the internet) emerged as a forceful equaliser, empowering billions with access to information. The second-order emergent themes (identified via CATWOE) were strongly linked to the worldview component, which was characterised by "Islamic, political, national, privacy, rights, counter-terrorism, surveillance, terrorism". While the first-order themes were related to "economic imbalances and poor governance", thus pointing to the "root causes" of terrorism (Newman, 2006), the second-order themes pointed to emergent "worldviews" that are increasingly mediated by digital technologies (Bertram, 2016).

The control parameter can thus be viewed through the lens of *digital counterpower,* as a legitimisation tool that links the emergence of terrorism genres to the forceful

mediation of internet sources of information that shape the worldview of the terrorist. As Hajj, McEwan, and Turkington (2019) found out, internet usage influences the information ecology of individuals, thus shaping their worldviews. In our analysis, the terrorist emerges as part of a digital counterpower movement—as a form of political violence, predominantly shaped by the information ecology of the internet as an alternative voice to mainstream worldviews.

Order parameter: Digital terrorism enactment

The first-order themes that emerged from the meta-synthesis for order parameters (Table 2) captured three dominant concepts: dominant ideology (philosophy, root causes); policies; and open models of information-sharing (collaboration, sharing economy, and open technology platforms). The second-order themes (identified via CATWOE) revolved around the notion of transformation. From the methodological perspective of SSM, the notion of transformation focuses on purposeful activities undertaken by actors within a particular ecosystem with the aim of solving a problem (Checkland & Scholes, 1990).

While the control parameter themes, linked to the digital information ecology, were found to be positioned as contributing to a legitimation process in which the notion of digital counterpower is used to rationalise terrorism as an alternative form of political violence, the order parameter themes appear to capture *digital terrorism enactment*, i.e., the mobilisation activities of terrorism and counterterrorism. Mobilisation, in the manner used by Swanson and Ramiller (1997), serves the dynamic function of activating, motivating and structuring the forces that emerge to support the material realisation of new acts of terrorism. Mobilisation implies that actors (both terrorists and counter-terrorism agencies) look to the terrorism ecosystem for the resources required to realise their agendas. For instance, both terrorists and counter-terrorism actors are focused on manipulating algorithms that underpin digital information ecology to spread propaganda and enact responses (Ammar, 2019). The emergence, explained above, of digital counterpower as part of the digital information ecology control parameter could be seen to explicate the root causes of terrorism. At the same time, the emergence of alternative worldviews could be seen as structuring the digital terrorism enactment order parameter. It is this latter perspective that envisions the emergence of terrorism and counter-terrorism through various transformation activities objectified in dominant terrorism ideologies, policies, and strategies.

System constraints: Digital capabilities

Under the CATWOE analysis, we likened the constraining nature of various external and internal systems to "owners", in terms of the Checkland and Scholes (1990) characterisation of owners as those with the power to either stop transformations or allow them to take place. The role of digital technologies in the CATWOE analysis points to the visible role of the relational view of power (Doolin & McLeod, 2012)

as enabling or constraining the digital capabilities of players within the terrorism ecology.

The differentiated *digital capabilities* of counter-terrorism agencies allow, on one hand, a category of these agencies to be efficient in responding to terrorism incidents because they have developed the critical infrastructure, the weaponisation of information, and the targeted use of social media messaging (Omand, 2018). On the other hand, institutional separation in the security sector is deeply entrenched, and is linked to the separation of roles, responsibilities and (digital) resource endowments, which foments institutional competition (Campana & Légaré, 2010). From a terrorism perspective, successful terrorism incidents are in part shaped by their digital capabilities, for instance, their utilisation of the latest communication devices to recruit, share and distribute information, and to mobilise support, particularly through the internet (Carty & Barron, 2019). Thus, for both terrorists and counter-terrorism agencies, digital capability remains a fundamental source of power and counter-power.

System elements: Digital enslavement

The theory of synergetics envisages a dominant order parameter emerging from competing order parameters to "enslave" systems elements (see Figure 4). As this dominant order parameter emerges, the "enslaving" process entrenches system elements through which individuals and collectives (e.g., security agencies, terrorism cells) are both enabled and constrained, by digital capabilities, to participate in an ecology that gives rise to terrorism and counter-terrorism activities. In the case under examination here, the order parameter (digital terrorism enactment) determines the behaviour, via digital enslavement, of the numerous individual elements. For instance, at the macroscopic level of the order parameter, various scholars have claimed that religion, particularly Islamist ideology, is used to foment global terrorism, with the counter-terrorism response undergirded by the belief that Islamist ideology is a root cause of terrorism (Bartolucci, 2019; Schuurman, 2019).

Thus, at the macroscopic order parameter level, a view of terrorism as emanating from Islamic philosophy has stabilised. And we saw in the analysis earlier in this article that the formation of this dominant view of the root causes of terrorism is influenced by open models of information-sharing (collaboration, sharing economy, and open technology platforms). This stabilised narrative of the nature of terrorism structures and influences the behaviour of individual systems elements (such as terrorism cells, counter-terrorism agencies) at the microscopic level, by means of the process we regard as *digital enslavement*.

5. Conclusions

Our systematic literature review has demonstrated that viewing terrorism as separate from the broader digitalisation of society would not only be imprudent but would also constrain societies' ability to counter terrorism effectively. Rather, viewing terrorism as a self-organising digital ecology, comprising a complex web of interacting agents, users, and technologies, allows for better conceptualisation.

Our review resulted in the identification of five key sub-systems interacting within the digitalised terrorism ecology:

- open digital infrastructure;
- digital information ecology and digital counterpower;
- digital terrorism enactment;
- digital capabilities; and
- digital enslavement.

These five sub-systems act to define the sociomaterial nature of the terrorism ecology, influencing the emergence of terrorism and counter-terrorism responses. Viewed in terms of these sub-systems, the digitalised terrorism ecology comprises a complex coexistence of the five sub-systems, centred on the open digital infrastructure, with this infrastructure typified by the "sharing economy" whose modalities are at play within the digital platforms that foment terrorism (Teigland, Holmberg, & Felländer, 2019). This sharing economy has inspired the emergence of the digital information ecology for individuals and collectives, empowering them to consider and appropriate previously unknown worldviews and notions of digital counterpower. The emergence of dominant worldviews, through the process of enactment, then structures and enslaves the emergence of various terrorism and counter-terrorism genres. While the prevailing view is that there is an increase in lone-actor terrorist acts (Sela-Shayovitz & Dayan, 2019), the influence of the digitalised terrorism ecology on individuals and collectives over time needs to be the prime foundation for understanding terrorism.

This study has also provided methodological and theoretical insights. The methodological approach that was adopted demonstrated the possibility of using SSM to inform qualitative thematic analysis. Furthermore, analytical theorising based on synergetics, a theory based on self-organisation, allowed for the unpacking of the complex problem of terrorism from a systems perspective. This combination of SSM and synergetics was found to be of value in furthering our understanding of how the contemporary digital terrorism ecology has emerged. While the claims made in this article are of necessity tentative due to the limits of a meta-synthesis, further empirical research can focus on testing the insights that have emerged.

References

Alhojailan, M. I. (2012). Thematic analysis: A critical review of its process and evaluation. *West East Journal of Social Sciences*, *1*(1), 39–47.

Ammar, J. (2019). Cyber gremlin: Social networking, machine learning and the global war on Al-Qaida- and IS-inspired terrorism. *International Journal of Law and Information Technology, 27*(3), 238–265. https://doi.org/10.1093/ijlit/eaz006

Asongu, S. A., Nnanna, J., Biekpe, N., & Acha-Anyi, P. N. (2019). Contemporary drivers of global tourism: Evidence from terrorism and peace factors. *Journal of Travel & Tourism Marketing*, *36*(3), 345–357. https://doi.org/10.1080/10548408.2018.1541778

Autio, E., Nambisan, S., Thomas, L. D. W., & Wright, M. (2018). Digital affordances, spatial affordances, and the genesis of entrepreneurial ecosystems. *Strategic Entrepreneurship Journal*, *12*(1), 72–95. https://doi.org/10.1002/sej.1266

Bartolucci, V. (2019). The discourse on terrorism of Donald Trump. In J. Kowalski (Ed.), *Reading Donald Trump: A parallax view of the campaign and early presidency* (pp. 127–147). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-93179-1_7

Benson, D. C. (2014). Why the internet is not increasing terrorism. *Security Studies, 23*(2) 293–328. https://doi.org/10.1080/09636412.2014.905353

Bergvall-Kåreborn, B., Mirijamdotter, A., & Basden, A. (2004). Basic principles of SSM modeling: An examination of CATWOE from a soft perspective. *Systemic Practice and Action Research*, *17*(2), 55–73. https://doi.org/10.1023/b:spaa.0000018903.18767.18

Bertram, L. (2016). Terrorism, the internet and the social media advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter violent extremism. *Journal for Deradicalization*, *7*, 225–252.

Blaker, L. (2015). The Islamic State's use of online social media. *Military Cyber Affairs*, *1*(1), 4. https://doi.org/10.5038/2378-0789.1.1.1004

Braun, V., Clarke, V., & Terry, G. (2014). Thematic analysis. In P. Rohleder & A. C. Lyons (Eds.), *Qualitative research in clinical and health psychology* (pp. 95–114). Basingstoke, UK: Palgrave Macmillan.

Burtch, G., Carnahan, S., & Greenwood, B. N. (2018). Can you gig it? An empirical examination of the gig economy and entrepreneurial activity. *Management Science*, *64*(12), 5497–5520. https://doi.org/10.1287/mnsc.2017.2916

Campana, A., & Légaré, K. (2010). Russia's counterterrorism operation in Chechnya: Institutional competition and issue frames. *Studies in Conflict & Terrorism*, *34*(1), 47–63. https://doi.org/10.1080/1057610x.2011.531458

Carty, V., & Barron, F. G. R. (2019). Social movements and new technology: The dynamics of cyber activism in the digital age. In B. Berberglu (Ed.), *The Palgrave handbook of social movements, revolution, and social transformation* (pp. 373–397). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-92354-3_16

Carugati, A., Fernández, W., Mola, L., & Rossignoli, C. (2018). *My choice, your problem ? Mandating IT use in large organisational networks*. *Information Systems Journal, 28*(1), 6–47. https://doi.org/10.1111/isj.12120

Castells, M. (2011). *The rise of the network society: The information age: Economy, society, and culture, volume 1* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Cecez-Kecmanovic, D., Galliers, R. D., Henfridsson, O., Newell, S., & Vidgen, R. (2014). The sociomateriality of information systems: Current status, future directions. *MIS Quarterly*, *38*(3), 809–830. https://doi.org/10.25300/misq/2014/38:3.3

Checkland, P., & Scholes, J. (1990). *Soft systems methodology in action*. Hoboken, NJ: John Wiley & Sons.

Checkland, P. (1981). *Systems thinking, systems practice*. Hoboken, NJ: John Wiley & Sons.

Daniel, E., Hartnett, E., & Meadows, M. (2017). Don't throw rocks from the side-lines: A sociomaterial exploration of organizational blogs as boundary objects. *Information Technology & People*, *30*(3), 542–561. https://doi.org/10.1108/itp-02-2015-0036

Denning, D. E. (2010). Terror's web: How the internet is transforming terrorism. In Y. Jewkes, & M. Yar, (Eds.), *Handbook of internet crime* (pp. 194–213). Milton, UK: Willan Publishing.

Doolin, B., & McLeod, L. (2012). Sociomateriality and boundary objects in information systems development. *European Journal of Information Systems*, *21*(5), 570–586. https://doi.org/10.1057/ejis.2012.20

Doosje, B., Moghaddam, F. M., Kruglanski, A. W., De Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. *Current Opinion in Psychology*, *11*, 79–84. https://doi.org/10.1016/j.copsyc.2016.06.008

Dunn, W. N. (2015). *Public policy analysis: An integrated approach* (6th ed.). Abingdon, UK: Routledge.

Finin, T., Joshi, A., Kolari, P., Java, A., Kale, A., & Karandikar, A. (2008). The information ecology of social media and online communities. *AI Magazine*, *29*(3), 77–92. https://doi.org/10.1609/aimag.v29i3.2158

García-Marco, F. J. (2011). Libraries in the digital ecology: Reflections and trends. *Electronic Library*, *29*(1), 105–120. https://doi.org/10.1108/02640471111111460

Gillespie, M., Osseiran, S., & Cheesman, M. (2018). Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances. *Social Media + Society*, *January-March,* 1–12. https://doi.org/10.1177/2056305118764440

Hafez, M., & Mullins, C. (2015). The radicalization puzzle: A theoretical synthesis of empirical approaches to homegrown extremism. *Studies in Conflict & Terrorism*, *38*(11), 958–975. https://doi.org/10.1080/1057610x.2015.1051375

Hajj, N., McEwan, P. J., & Turkington, R. (2019). Women, information ecology, and political protest in the Middle East. *Mediterranean Politics*, *24*(1), 62–83. https://doi.org/10.1080/13629395.2017.1380116

Haken, H. (1984). Can synergetics be of use to management theory? In H.-U. Gilbert, & J. B. Probst (Eds.), *Self-organization and management of social systems: Insights, promises, doubts, and questions* (pp. 33–41). Berlin: Springer. https://doi.org/10.1007/978-3-642-69762-3_3

Hawi, D., Osborne, D., Bulbulia, J., & Sibley, C. G. (2019). Terrorism anxiety and attitudes toward Muslims. *New Zealand Journal of Psychology*, *48*(1), 80–89.

Huberman, B. A. (2003). *The laws of the web: Patterns in the ecology of information*. Cambridge, MA: MIT Press.

Kagwanja, P. (2006). Counter-terrorism in the Horn of Africa: New security frontiers, old strategies. *African Security Studies*, *15*(3), 72–86. https://doi.org/10.1080/10246029.2006.9627608

McLuhan, M., with Gordon, W. T., Lamberti, E., & Scheffel-Dunand, D. (2011). *The Gutenberg galaxy: The making of typographic man*. Toronto: University of Toronto Press.

Merali, Y. (2006). Complexity and information systems: The emergent domain. *Journal of Information Technology*, *21*(4), 216–228. https://doi.org/10.1057/palgrave.jit.2000081

Newman, E. (2006). Exploring the root causes of terrorism. *Studies in Conflict & Terrorism*, *29*(8), 749–772. https://doi.org/10.1080/10576100600704069

Ochara, N. M. (2014). Towards a regional ontology for e-participation: An ecological view. In P. M. Sebina, K. H. Moahi & K. J. Bwalya (Eds.), *Digital access and e-government: Perspectives from developing and emerging countries* (pp. 60–72). Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-4666-5868-4.ch005

Ochara, N. M. (2013). Linking reasoning to theoretical argument in information systems research. *AIS Electronic Library (AISeL)*, 1–11. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1501&context=amcis2013

Odero, K., Ochara, N. M., & Quenum, J. (2017). Towards big data-driven logistics value chains for effective decision making and performance measurement. In *Proceedings of the 11th European Conference on Information Systems Management (ECISM 2017), Genoa, Italy, 14-15 September*. https://doi.org/10.2139/ssrn.2960510

Omand, D. (2018). The threats from modern digital subversion and sedition. *Journal of Cyber Policy*, *3*(1), 5–23. https://doi.org/10.1080/23738871.2018.1448097

Paganini, P. (2016). The role of technology in modern terrorism. Madison, WI: InfoSec Institute.

Park, Y. A., & Gretzel, U. (2007). Success factors for destination marketing web sites: A qualitative meta-analysis. *Journal of Travel Research*, *46*(1), 46–63. https://doi.org/10.1177%2F0047287507302381

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Rittel, H. W., & Webber, M. M. (1973). 2.3 planning problems are wicked problems. In N. Cross (Ed.), *Developments in design methodology.* Chichester, UK: John Wiley & Sons.

Schmitt, M., Eid, M., & Maes, J. (2003). Synergistic person x situation interaction in distributive justice behavior. *Personality and Social Psychology Bulletin*, *29*(1), 141–147. https://doi.org/10.1177/0146167202238379

Schuurman, B. (2019). Topics in terrorism research: Reviewing trends and gaps, 2007–2016. *Critical Studies on Terrorism*, *12*(3), 463–480. https://doi.org/10.1080/17539153.2019.1579777

Sela-Shayovitz, R., & Dayan, H. (2019). Female Palestinian terrorists: The role of the Intifada period and the terrorism context. *Studies in Conflict & Terrorism*, 1–18. https://doi.org/10.1080/1057610x.2019.1575027

Sirgy, M. J., Estes, R. J., El-Aswad, E.-S., & Rahtz, D. R. (2019). Proposed response: Counterterrorism strategies focusing on the demand side of the terrorism market. In *Combatting Jihadist terrorism through nation-building: A quality-of-life perspective* (pp. 149–173). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-17868-0_8

Statista. (2019). Global digital population as of July 2019 [Web page]. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

Swanson, E. B., & Ramiller, N. C. (1997). The organizing vision in information systems innovation. *Organization Science*, *8*(5), 458–474. https://doi.org/10.1287/orsc.8.5.458

Teigland, R., Holmberg, H., & Felländer, A. (2019). The importance of trust in a digital Europe: Reflections on the sharing economy and blockchains. In A. B. Engelbrekt, N. Bremberg, A. Michalski, & L. Oxelheim (Eds.), *Trust in the European Union in challenging times* (pp. 181–209). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-73857-4_9

Tuten, T., & Mintu-Wimsatt, A. (2018). Advancing our understanding of the theory and practice of social media marketing: Introduction to the special issue. *Journal of Marketing Theory and Practice*, *26*(1–2), 1–3. https://doi.org/10.1080/10696679.2018.1393277

Weißenfels, S., Ebner, K., Dittes, S., & Smolnik, S. (2016). Does the IS artifact matter in sociomateriality research? A literature review of empirical studies. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, 5–8 January. https://doi.org/10.1109/hicss.2016.252