# Distributed Swarming and Stigmergic Effects on ISIS Networks: OODA Loop Model

Ahmad Shehabat[1] & Teodor Mitew[2]

*School of the Arts,English and Media*
*University of Wollongong*
*Australia*

[1]ams591@uowmail.edu.au
[2]tmitew@uow.edu.au

*Received Date: 3/7/2017 Accepted Date: 7/12/2017 Published Date: 28/12/2017*

## ABSTRACT

The stigmergic swarming of digital media environments with propaganda and personal communication made the self-proclaimed Islamic State (also known as ISIS, IS, ISIL and Daesh) one of the strongest terror groups in the world. This study aims to identify the digital manoeuvre warfare tactics deployed by ISIS to survive the degrading operation initiated by its adversaries. In this paper, we emphasise that the information operations of terror organisations are not limited to a certain application or communication platform. Instead, the emergence of anonymous platforms (e.g., Justpase, Sendvid) and encryption communication applications (e.g., Telegram, WhatsApp) has enabled ISIS's information operations and helped the organisation to maintain its networking structure. This paper examines the role played by anonymous platforms in ISIS' operations from an information-

ISSN 1985-563X

centric warfare perspective. The theoretical framework is derived from manoeuver warfare based on John Boyd's OODA loop theory. The data collection involves a digital ethnography approach, concentrated on tracing and observing ISIS' digital activities across anonymous platforms and encrypted communication channels. The study suggests that the failure of ISIS' adversaries in operating inside the OODA loop of ISIS led to the organisation's survival and proliferation of its information operations.

***Keywords:*** *Islamic State, digital media environments, network centric warfare, stigmergy, media manoeuvre warfare, OODA loop.*

## INTRODUCTION

The emergence of digital communication technologies has fundamentally changed the structure and communication dynamics of terror organisations. Hierarchical, centralized organisations have morphed into interconnected, decentralised and distributed networks. This process can also be observed in the logistics of the Islamic State of Iraq and Sham's[1] (ISIS) information operations, propaganda dissemination and personnel communications, which are highly decentralised. To hinder ISIS' communication and disrupt its information operations, the US government declared operation "degrading ISIS's digital capabilities". This operation led to intense information-centric warfare, as ISIS adapted using stigmergic swarming operations to survive the interruption of its information infrastructure. In this paper, we argue that the advent of anonymous sharing platforms (e.g., justpaste.it, sendvid.com), cloud platforms (e.g., google drive, drobox) and encrypted applications (e.g., Telegram, WhatsApp, Signal) along with existing social media platforms (Twitter, Facebook) supplemented ISIS with logistical tools allowing it to maintain its network structure, evade interception, and survive attempts to degrade its information operation capabilities. Ultimately, these new online environments enabled ISIS to launch swarming attacks as part of the information-centric warfare against its adversaries.

[1] Also known as IS, ISIL and Daesh

To analyse information-centric and manoeuvre warfare in the context of this study, we use John Boyd's OODA loop concept (1974) as a theoretical tool allowing us to model the information warfare dynamics in the clash between ISIS and its adversaries. Below, we first examine ISIS and its adversaries' information operations in terms of an OODA loop. Second, we examine the OODA loop model and its role in the information manoeuvre warfare perspective. Finally, we highlight the swarming and stigmergic practices ISIS opted to use to strategically engage in battles in the information domain.

*Network Centric Warfare: ISIS vs the World*

ISIS' declaration of Islamic *Khilafah* in August 2014 fundamentally changed the network architecture of its organisation. The shift from non-state actor to a self-proclaimed quasi-state, and the naming of Mosul as capital city of *Khalif* Abo-Baker Baghdadi required ISIS to centralise at least to a certain extent both its command and control structures and its information operations involving networking, communication, information dissemination, and propaganda. ISIS adversaries (e.g., the US coalition, Shia militias, individual hackers, hacker collectives such as *Anonymous*), attempted to disrupt and disable the communication capabilities of this terror organisation by suspending accounts and associated content on popular social media platforms, hacking of webpages, and disseminating disinformation. However, in order to maintain its network structure[2] and command and control operations (C2),[3] ISIS managed to adapt by manoeuvring its information operations across multiple online platforms, and therefore survive the degrading operation strategy initiated by its adversaries. Nissen has suggested that C2 operations across social media involves "internal communication, information sharing, coordination and synchronisation of actions and facilitates more agile decision-making". [1]

One way to understand the multiple overlapping information warfare operations between ISIS and its adversaries is to employ the Network

[2] Network structure is here understood to include control over: internal information flows, external communication channels, propaganda dissemination channels, and the integrity of propaganda content floating across open channels.

[3] We use command and control according to NATO's taxonomy, where it is known as C2 and stands for "employing of assets and capabilities (people, systems, material and the relationships between them) towards a specific objective or task by organisations" (NATO, 2006, pp. 5-7).

Centric Warfare (NCW) approach. "Network Centric Warfare is the best term developed to date to describe the way we will organize and fight in the Information Age". [2] Within the scope of this study NCW describes well how ISIS maintained their information operations and network structure by dispersing across multiple channels. As Alberts, et al., noted "(NCW) is based upon the experiences of organizations that have successfully adapted to the changing nature of their competitive spaces in the Information Age". [3] It is also important to note that "NCW reflects and incorporates the characteristics necessary for success in the Information Age - the characteristics of agility and the ability to capitalize on opportunities revealed by developing an understanding of the battlespace that is superior to that developed by an adversary". [4] In the context of ISIS, the NCW model sees the emergence of new, distributed, and often open source forms of communication across a variety of public and anonymous platforms. Furthermore, in the context of Boyd's OODA loop (see next subsection), NCW is about leveraging the speed of one's own information network to gain an advantage in manoeuvrability over an enemy, and exploit the ensuing weaknesses in the opponent's networks. Also, it is important to acknowledge that geographically isolated forces are depended on strong networks which are considered the backbone for NCW. [5] ISIS' distributed information network structure, dependent on decentralised C2, has allowed the organisation to manoeuvre across the information battlefield at speed and within a NCW model.

As Cebrowski & Garstka observed, access to necessary information sources, weapons reach, and manoeuvring with accuracy and speed are the facilitating elements to achieve high performance C2 practises. [6] In order to maintain its information operations in the face of a coordinated network degrading campaign, ISIS managed to access and utilise almost every social media and content sharing online platform, constantly disseminating propaganda and manoeuvring its channels to avoid closure. Cebrowski & Garstka predicted that terrorist organisations would take advantage of the emergence of new cloud sharing portals and encrypted applications, suggesting that the high speed and accessibility of internet

technologies enable distribution and creation of content flowing across various information domains online. [7]

The relatively open architecture of sharing portals (e.g., Justpaste.it, share.it), social media platforms (e.g., Twitter, YouTube) and mobile phone applications (e.g., Telegram, WhatsApp) enabled ISIS' information operations to manoeuvre at speed in the information domain. Importantly, the ability of distributed ISIS associates to collaborate on attacks with other distributed nodes of the organisation without involving a central C2 hub allowed the organisation to shift to NCW operations, which "[…] are characterized by information-intensive interactions between computational nodes on the network". [8] As Smith has argued, the ability to rapidly collaborate, produce, analyse, aggregate, disseminate, and access information across networked domains gives terror groups an advantage over their opponents in information warfare. [9] For example, information shared on anonymous platforms can be uploaded and shared across almost every digital domain, including mobile phone applications. Hybrid links of shared information, below referred to as *pheromone trails* (see stigmergic subsection), can be downloaded, edited and shared asynchronously as well as at near-instantaneous speed.

In order to understand the dynamics behind ISIS' migration online we must look at the geographical space and battlefronts they operate across, the large number of combatants joining the organisation, and their political structure. On the one hand, the massive geographical space ISIS controlled in Syria and Iraq made it the largest terror organisation in the world, divided into 23 *Welayats* (provinces). Communication networks were essential to coordinate operations between divided forces across *Welayats.* Therefore, to keep their territory under control, ISIS established a communication hub in every *Welayat,* effectively establishing nodes in the network, to coordinate military action and maintain information operation. In his treatment on Boyd's OODA loop concept Commodore

[4] A German term loosely translated as mission-based tactics, standing for a command philosophy originating with von Moltke, where high operational and tactical flexibility is delegated at the level of frontline unit commanders.

Frans Osinga has argued that the emergence of distributed information networks allows dispersed forces to coalesce and coordinate efforts, as well as adapt new network structures, which in turn require the creation of similar networks to defeat them. [10]

Osinga's observation is immediately applicable to ISIS' operational context, as it illustrates the importance of adapting to a distributed network structure when facing centralised networks organised around hierarchical C2 structures. Distributed information networks are characterised by what Smith calls "self-synchronized" operations with accelerated C2 functions. Smith suggests that "the network would permit us to decentralize or flatten the command structure, taking the control function down to the lowest practicable level of command and shortening the response cycle by removing unneeded levels of command and control". [11] The decentralised structure of ISIS information networks depends heavily on information communicated across networks in just such a self-synchronized manner. As Nissen notes

> non-state actors, who like opposition groups in Syria, have a need for distributing information, internally and externally, and for coordinating and synchronising actions, and in some cases giving commands or direction and guidance to other groups or entities. Particularly when these groups or entities have no formal structure or are dispersed over large geographical areas, social network media can afford them with means and capabilities to conduct C2 activities. [12]

For instance, in November 2016 while under tremendous pressure from coalition forces in the battle of Raqqa (Syria), ISIS managed to take control of Palmyra (Syria). This move could be interpreted as a demonstration that the C2 speed of decentralised networks often allows them to locally overwhelm adversaries with more centralised operational structure. The battle of Al-Bab in Northern Syria (October, 2017- Feb 2017) between Turkish forces and local ISIS forces offers another example

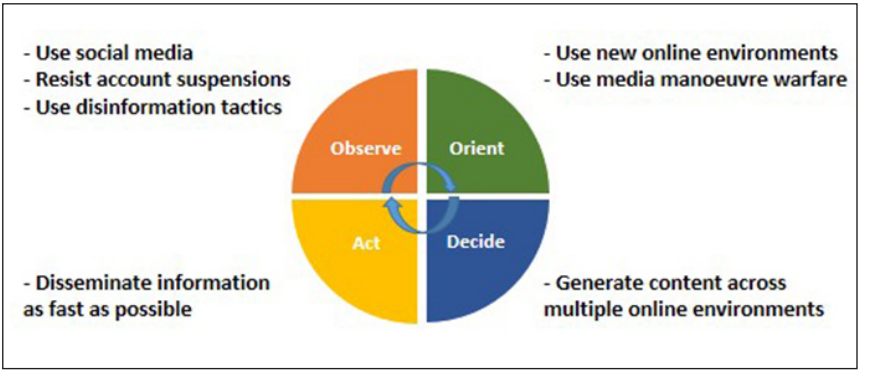
towards this observation. The Turkish forces suffered comparatively serious casualties and losses in military equipment as the speed of ISIS' C2 operations clearly depended on self-synchronized information shared between units operating on the ground.

Cebrowski & Garstka suggest that there are three elements necessary for the C2 speed of decentralised networks in the context of information centric warfare. First, according to them, information superiority is a decisive factor in understanding battlespaces. This can be achieved by adopting fast data gathering networks dependent on powerful sensing and simulation capabilities. The second factor is the speed and precision of effect-based swarming operations (to be discussed in detail later in this article). The third element involves blocking the enemy's operations before they start, otherwise referred to as operating inside the OODA loop of adversaries (see next section). Arguably, the second and third elements were successfully employed by ISIS in their NCW strategy. This resonates with Cebrowski & Garstka's observation that C2 speed is a powerful force multiplier for a weaker combatant in a clash between unequal forces. [13]

In this context, it is important to outline the role of John Boyd's OODA loop model in contemporary thinking on NCW. Mark Safranski identifies three fundamental Boydian ideas influencing NCW strategy: (1) manoeuvre warfare; 2) swarming operations performed by units acting in sync, referred to by Boyd as *auftragstaktik,*[4] and reliant on decentralised C2; and 3) information superiority as a decisive advantage in completing OODA loop cycles accurately and rapidly. [14]

## What is an OODA loop?

The OODA loop is a theory of manoeuvre warfare developed by US fighter pilot Colonel John Boyd during the Korean War, where he succeeded in taking down a number of enemy fighter jets using a high-speed decision making and feedback process. Accordingly, Boyd distilled this process into four stages described as Observe, Orient, Decide, Act (OODA), to be performed continuously in a feedback loop. The outcome of this approach




to get inside the OODA loop of one's opponent by going through the four stages in a faster loop. [16] This means that in the context of the overall dynamics of a complex theatre-wide engagement the organization able to operate in a more decentralised manner, in a pattern consistent with *auftragstaktik,* would likely be able to close its OODA loops faster and likely win. Therefore, the faster a combatant gathers data from the field (observe), and analyses it into meaningful information (orient), the faster their decision-making (decide), which in turn gives them the opportunity to act beyond an opponent's cognitive envelope (act). [17]

Osinga makes this exact point when he writes that "significant operational advantage will accrue to the side that can complete the decision cycle—Observation-Orientation-Decision-Action—in the shortest time span". [18] Importantly, in his PhD Thesis *Science, Strategy and War,* Osinga interprets the OODA loop as a concept operating both at the tactical and strategic levels, allowing units to win individual engagements and armies to win wars. [19] The OODA loop could therefore be understood as a way of operating in conditions of adversity, or, as Boyd puts it in his *Patterns of Conflict,* operating inside an adversary's OODA loop could be described as "observe, orient, decide and act more inconspicuously, more quickly, and with more irregularity". [20] In his unpublished work *Essence of Winning and Losing,* Boyd also makes the point that OODA loops are a fundamental part of decision-making in complex environments, necessary to achieve decisive action at a systemic level. [21]

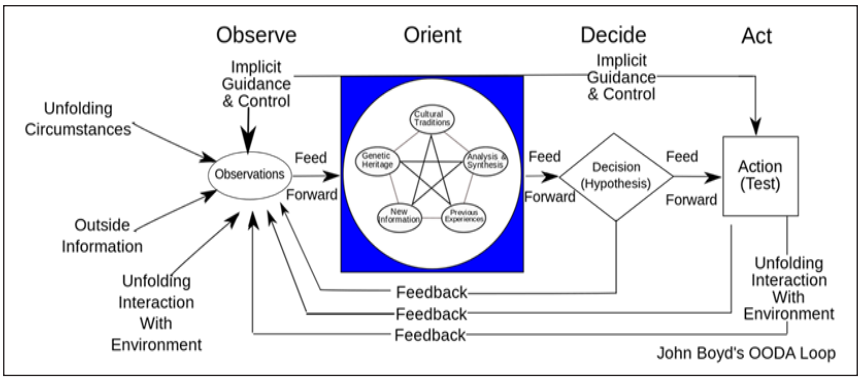



*Figure 1:* A diagram of the OODA process and its feedback loop functions during combat.

As Boyd argues, orientation is a key element of the OODA loop because it involves the processing of observed information and the generation of testable decisions (Figure 1). This makes orientation a fundamental stage in consistently getting inside an adversary's OODA loop, because it is the essential link between two feedback loop stages, observation and decision, and "is shaped by the feedback and other phenomena coming into our sensing or observing window". [22] Importantly, the first two stages of the OODA loop are dependent on sensory perception and the ability to process large amounts of information into a coherent picture of reality. This dependence is both a strength and a weakness. Smith has identified the reliance on sensor-based awareness during the observe stage in combat as a fundamental element of modern warfare, which, while arguably speeding up the first two stages of the loop is also highly fragile in a fog of war situation where field data is incomplete, contradictory, or actively manipulated by the enemy. [23] This is an important consideration in the context of this study.

The concepts of OODA and NCW originate in the domain of manoeuvrer warfare occurring between state actors in the physical world. However, within the scope of this study Boyd's OODA loop model is useful to describe the C2 operations of centralised hierarchical networks (state actors) combating a largely decentralised network (ISIS). Furthermore,

this study applies the OODA loop model to combat occurring primarily in the information domain, as it helps to understand the actions of hierarchical and decentralised networks from NCW perspective. While, as Osinga points out, Boyd "seemed careful never to define" what "operating inside opponents' OODA loops" actually means in practice, Osinga suggests that this can be achieved through destabilising an adversary's capacity to observe and orient in a dynamically changing environment while improving one's own capacity. [24] This point confirms the vulnerability of the first two stages of the OODA loop, and suggests the main vector of attack between state actors and largely decentralised entities such as ISIS.

## Inside ISIS' OODA loop

In examining ISIS' OODA loop it is helpful to consider the role played by the dispersal and decentralisation of its information network topology in the rapid manoeuvring between online platforms and adaptation to NCW. In what follows, this article examines the OODA processes of ISIS and its state adversaries, as well as the former's use of fast adaptation, stigmergy, and swarm operations. The argument put forward is that the speed of the OODA process of ISIS networks has been increased by harnessing anonymous cloud sharing portals and end-to-end encryption applications, giving the organisation a C2 boost which has helped in maintaining ISIS' information operations and allowed the development of new information warfare trajectories. In addition, the largely distributed topology of ISIS' online information warfare networks allowed it to launch distributed swarming operations based on large-scale content distribution while maintaining its network's integrity. This is in line with Arquilla and Ronfeldt's observation that the key aspect of information operations is the securing of internal information flows. [25]

ISIS' OODA loop cycle depended on a large number of smaller operations across online media environments, mirroring what Edward Smith calls "semi-independent operations". [26] Such operations could involve the ad-hoc hijacking of Twitter hashtags using swarming tactics in order to boost the spread of a terror narrative (Figure 2).


*Figure 2:* ISIS used the #shahz al-hemam hashtag, meaning glad tidings, asserting the continuous use of popular social media networks for electronic Jihad. Source: Nashir political service , Telegram channel

These operations are usually masterminded and performed by dispersed individual media jihadists or affiliates, whose role is to repeatedly disseminate information on a large scale (act phase in the OODA cycle). These operations are facilitated by utilizing multiple online media environments in order to overwhelm and disrupt the ISIS opponents' decision-making cycle (the degrading operation against ISIS accounts across popular social media). Based on the above knowledge, the OODA loop of ISIS networks can be described as the following (Figure 3):

**Observe:** In the period of 2013-2015 ISIS adapted to social media and various online environments by copycatting some of al-Qaeda's information operation tactics in utilizing Twitter, YouTube, and Facebook as primary hubs for communication and information dissemination. Other online platforms (e.g. sendvid, dump.to) and end-to-end encrypted applications (e.g. Telegram, WhatsApp) were also used, but played a subservient role in ISIS' information operation strategy. Pro-ISIS digital jihadists involved across these platforms were quick to observe the disruptive effects of the anti-ISIS degrading operation waged by the social media platforms and government agencies. In addition, ISIS affiliates observed the emergence of new information dissemination tools (share.it, Daily Motion, justpaste.it),

enabling them to maintain information operations throughout the disruption phase.

**Orient:** Following on from the first phase, and leveraging the benefits of a largely decentralised network topology, ISIS and its affiliates were quick to grasp the value of relatively new online environments in maintaining network connectivity and information dissemination operations (e.g., justpaste.it, sendvid.com, woodvid.com, dump.to, Telegram, Signal, Top4top, Tumblr, Pinterest).

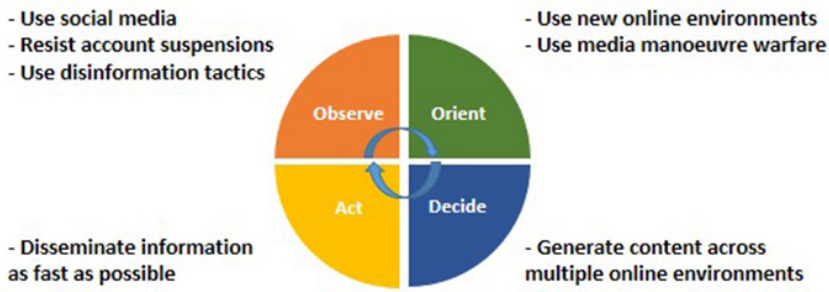



*Figure 3:* ISIS implementation of the OODA loop (image by authors)

In this context, the ability of a decentralised network to rapidly orient itself in the vulnerabilities of new media environments was vital, as it sped up the overall loop cycle leading to the next phase. It also enabled unimpeded information flows between media environments, and the use of multiple environments simultaneously, without losing the coherence of the final information operation objectives. This is an important point as it involves a clear example of the use of auftragstaktik in information warfare, and the leveraging of the dynamics of anonymous and encrypted communication platforms. Therefore, the adoption of new media environments sped up the overall decision-making cycle by creating multi-input information flows continuously feeding into the first two stages of the OODA cycle.

**Decide:** Following feedback from the first two stages of its OODA cycle, and in order to maintain connectivity and information dissemination

operations while the degrading operation against it was underway, ISIS started generating content across multiple online environments. In this context, the existence of anonymous cloud sharing platforms and encrypted applications allowed ISIS to manoeuvre around suppression attempts and maintain fast and continuous decision loop.

**Act:** Finally, the ability to manoeuvre at speed across media environments has had a big impact not only on ISIS' information operations but also on its ability to maintain an effective C2 network structure, allowing the organisation to maintain its OODA loop cycle.

## Inside the OODA loop of ISIS's adversaries

As discussed above, to defeat an adversary (ISIS) in a battle space (the information domain), it is essential to operate inside the loop of its networks and paralyse its information operations. As Boyd argued, to get inside an opponent's loop one has to "[…] change the situation more rapidly than the opponent can comprehend and keep doing it". [27] In interpreting Boyd's thinking on this point, Osinga argues that, because an opponent inevitably relies on information and communication systems, disrupting and destroying those systems can lead to superiority during conflict. [28] That is to say, rapid manoeuvring and changing of the situation on the ground leads to disruption of an opponent's ability to complete the first two stages of the OODA cycle. Furthermore, disruption of these first two stages allows one to get inside an opponent's loop and gain superiority.

In the context of this study, this would involve going through the observe and orient stages faster than the ISIS network by confusing it with rapid changes in the field, as well as disrupting its operations and breaking down its feedback loops. For example, recently the international coalition fighting ISIS succeeded in blocking and otherwise disrupting content linked to ISIS accounts on justpaste.it, in collaboration with the developer of the platform. In other words, and in resonance with Osinga's argument, disrupting ISIS' information flows allows the international coalition to degrade its information operations, destroy or significantly hamper its C2 capabilities, and operate inside ISIS' OODA loop cycle. [29]

Another way of degrading an enemy's initial OODA loop stages involved what Osinga calls a tactic of "interaction and isolation". This aim of this tactic is the complete isolation of opponents from the information domain they operate on. If successful, it will lead to the loss of internal and external cohesion in an adversary's networks by disrupting their information flows. For instance, isolating ISIS from Twitter severely hampered its information operations. As a result, ISIS affiliates initiated operation *#elzam thagrak* (#stay in your domain), intended to maintain internal processes of communication. As Osinga argues, the aim behind this tactic "is to change the opponent from an open into a closed system which slowly suffers the fate of all closed systems". [30] With this in mind, it is important to illustrate the operation of the OODA loop cycle of ISIS adversaries (Figure 4).

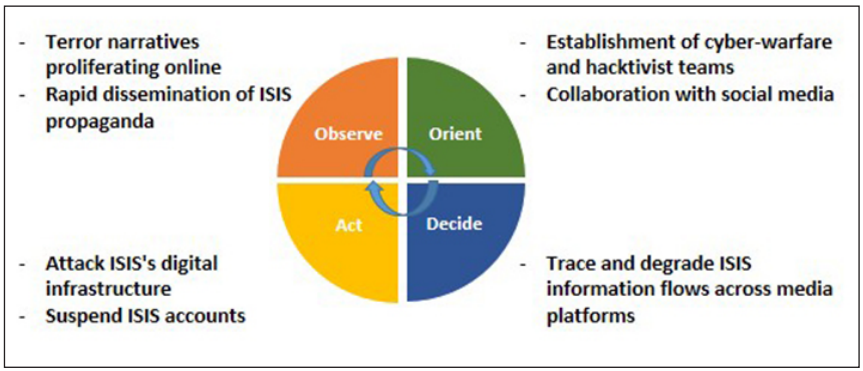



*Figure 4:* Inside the OODA loop of ISIS' adversaries (image by authors)

**Observe:** In this phase, the international coalition fighting ISIS seek to understand its information operations components and objectives. This process includes collecting data to identify the strengths and weakness of terror narratives, the logistics of their proliferation, and potential directions for counter-narrative agendas. This is the phase at which ISIS opponents identified the important logistics role played by popular social media platforms, particularly Twitter and YouTube. For example, in 2015 Jim Berger and Johnathon Morgan monitored ISIS activity on Twitter, suggesting the organisation had almost 90 thousand affiliated accounts. [31]

**Orient:** This phase arguably began with identifying the topology of ISIS-related networks across media platforms, and the dynamics of ISIS information operations. This phase also involves identifying specific actors in the ISIS network, and the types of messages they generate, the process of content generation and dissemination, as well as the role of various information flows in maintaining ISIS' OODA loop cycle. The end of this phase involves identifying potential attack vectors against ISIS networks, and establishing collaboration with social media platforms across whose domain the attacks would have to be performed.

**Decide:** Building on the previous stage, this phase settled on a tactic of quick tracing and identification of ISIS-related network nodes by the information flows they generate and disseminate, followed by immediate disruption. Reminiscent of Osinga's interaction and isolation strategy, this tactic aimed to hinder and suppress terror-related propaganda by disrupting the logistics of its generation and dissemination. Viewed in aggregate, this was systemically waged information warfare, whereby the international coalition managed to inject noise in select ISIS communication networks (mostly across Telegram and Twitter). This involved a number of measures, including inserting disinformation through network infiltration, suspension of select key ISIS accounts, as well as hacking and counter-propaganda operations. As a simple example, ISIS adversaries would join the organisation's Telegram channels and report them to the platform's admins for violations of terms of service, which led to channel suspensions (interaction and isolation).

**Act:** The tactic identified above was followed through in this final phase. This involved the continuous degrading of ISIS' information operations by hacking, disinformation, and tracing the physical locations of key information disseminators acting as network hubs. This 'whack-a-mole' operation was successful in paralysing tens of thousands of ISIS' social media accounts on Twitter and YouTube. For instance, the most prominent pro-ISIS affiliates, Shami Witness and Asawrty Networks, were eliminated permanently after their location was identified by the authorities (Figure 5).


*Figure 5:* Screenshot of Twitter feed of ISIS propagandist Shami Witness (image by Authors).

Overall, examining the information warfare OODA loop cycles of both ISIS and the international coalition combating it, it appears that ISIS was faster in adapting to changing conditions than its adversaries. ISIS, leveraging its decentralised network topology, was able to route around attacks on its information infrastructure by immediately, and often pre-emptively, manoeuvring across to new digital environments. This argument was echoed by Michael Waller, a US military strategist and Secretary of Defence advisor, who argued that jihadi movements including ISIS and Al-Qaeda have "penetrated our own OODA loop and have affected our ability to orient, decide and act". [32]

One conclusion we can draw from this is that the use of social media platforms in waging information centric-warfare was crucial in shortening the OODA loop of ISIS' information generation and dissemination. Continuous reopening of suspended accounts and hijacking of trending Twitter hashtags, among other tactics, gave ISIS a decentralised network advantage against its much more hierarchically organised adversaries. As Nissen argues in his *The Weaponization of Social Media* monograph, "some messaging and content production is also crowd-sourced / crowd distributed (and translated). This indicates IS having access to highly skilled multi-media designers and state-of-the-art software (such as Adobe applications as InDesign, Photoshop etc.) The bottom-line is that IS, when it comes to the strategic utilisation of social media, seems to be in the lead at the moment, although they are increasingly challenged at their own game". [33]

## Swarming and ISIS information operations

Arguably, the resilience of ISIS networks and its survival in the face of massive disruption operations is, at least to a certain extent, due to its adoption of swarming tactics in the information domain. In the midst of the suppression and disruption operations against, ISIS started calling on loosely affiliated collectives of e-jihadists to swarm suddenly hostile social media environments. Meanwhile the US Government used its Cyber Command to run its own swarm attacks countering terrorist propaganda disseminated across social media. Similarly, hacker collectives such as Anonymous established #op_Ice_ISIS in an effort to help the information warfare operations against the terror group.

Swarming is a military tactic based on attacking an enemy from all directions in order to paralyse its decision making process. It can be observed in nature, for example in bee swarms attacking enemies of the hive, and relies on what Libicki calls "the many and the small". [34] In the context of the fight against terrorism, Arquilla and Ronfeldt have pointed out that "swarming is also likely to prove valuable to terrorist and transnational criminal organizations". [35] In his *Brave New War* counter-terrorism expert and military theorist John Robb identifies "massed and dispersed" swarming operations [36]. According to Robb, *massed* swarming resembles the tactics of beehives against attackers, in that the unit starts concentrated only to disperse and swarm the target. Dispersed swarming, on the other hand, is based on small operations by decentralised groups performing specific tasks. Robb illustrates dispersed swarming with the situation in Iraq in 2007, where small guerrilla groups attacked US targets in a wave after wave of swarming operations with next to no coordination apart from the overall mission goal of defeating the US occupation *(auftragstaktik)*. [37]

The swarm activity of ISIS affiliates can be described as a process of spontaneous coordination between mission-affiliated groups in a variety of information warfare tasks. These could involve generating and diffusing information across a wide spectrum of social media, or performing direct attacks against agreed-on targets. For example, ISIS-related Telegram

channels are used to share propaganda videos, publications and personal communication using hybrid links codes leading to anonymous sharing platforms. Nico Prucha has pointed out that ISIS-related Telegram channels were leveraged to maximise the global information impact of the Brussels attack in March 2016. Following the attack, ISIS affiliates operating on Telegram channels related to the terrorist group encouraged followers to hijack trending Twitter hashtags and disseminate information in French and other languages. Followers are encouraged to engage in swarm-like "social media raids" intended to maximise propaganda impact, confuse suppression attempts, and boost the network's flow of information. [38]

The decentralisation of ISIS networks has empowered swarming operation as collectives of e-jihadists carry out ISIS information operations without coordination or an established network centre. Prucha has observed that jihadi tactics during online swarming operations have demonstrated resilience and careful planning. This observation is supported by al-Ghazzi, who describes the swarm as "an army of [IS] supporters who dedicate their time for the defence of the people of jihad". [39]

Above, we pointed out that the effectiveness of ISIS' swarming operations, dependent on self-synchronised semi-independent actors, have sped up its overall C2 capabilities in the context of NCW. Interestingly, this observation is somewhat mirrored by Cebrowski and Garstka, when they note that "information technology is undergoing a fundamental shift from platform-centric computing to network-centric computing". [40] For example, when ISIS appeals to its affiliates to launch swarm attacks on Twitter, the range of tactics includes re-opening of suspended accounts, hijacking of trending hashtags, hacking opponents' accounts, and distribution of propaganda and disinformation aimed at confusing the ISIS adversaries' NCW operations. These swarm operations leverage existing communication channels and are usually self-synchronised in line with the *auftragstaktik* principle.

As Arquilla & Ronfeldt argue, effective swarming tactics depend completely on "robust, rapid communications" [41], while new information technologies "render an ability to connect and coordinate the actions of

widely distributed "nodes" in almost unprecedented ways". [42] Swarming operations are successful when participants "engage adversaries from all directions simultaneously" [43], and a number of ISIS information warfare operations can be categorised this way. Furthermore, swarming is enabled by information circulating freely across the battle spectrum [44], allowing networked actors to defeat adversaries. [45] The continuous re-opening of suspended Twitter accounts associated with ISIS, using fake names, generic emails and hacked phone numbers, is another example of persistent swarming operations in the face of systemic degrading efforts across major social media platforms. Arquilla & Ronfeldt suggest that combating the swarming attacks of an opponent using NCW requires a high level of information security across one's own network. [46] As swarming attacks are by definition highly non-linear and dispersed, poor information security increases the cost of cycling through the first two phases of one's own OODA loop, in effect dooming the effort to failure.

In analysing the coordinated efforts of ISIS affiliates to swarm social media environments in order to gain an advantage in their information operations John Robb has used the concept of *stigmergy* to capture the self-coordination tactics of the swarm. According to Robb, "stigmergy can be used as a mechanism to understand underlying patterns in swarming activity. As such, it can be applied to the understanding of swarming attacks by diverse bands of global guerrillas." [47]

## Stigmergy operations of ISIS networks

The indirect self-coordination between ISIS-related e-jihadists in swarming media environments is a good example of the practice of stigmergy. In this context, Robb describes it as "creating paths for information distribution through self-organised clusters of individuals who have knowledge in access to digital networks". [48] Understanding stigmergy in the context of terrorist operations allows us to understand the mechanics of coordination between decentralised and fully distributed networks for the purpose of disrupting their NCW operations. The notion of stigmergy has its origins in the work of French biologist Pierre-Paul Grasse, who used it to describe "environmental mechanisms for coordinating the

work of independent actors". [49] Etymologically, the term is derived from the Greek words *stigma* ("sign") and *ergon* ("to act") [50], indicating the importance of the semantic payload in the stigmergic process. For example, stigmergy describes the way ants use pheromones to create chemical trails for other ants to follow. While there is no direct communication and coordination between individual ants, the semantic payload of the pheromones acts as the connective tissue forming the edges of the communication network. In a similar mode of operation, ISIS affiliates and sympathisers use hybrid weblog links to establish information paths for others to follow (Figure 6).

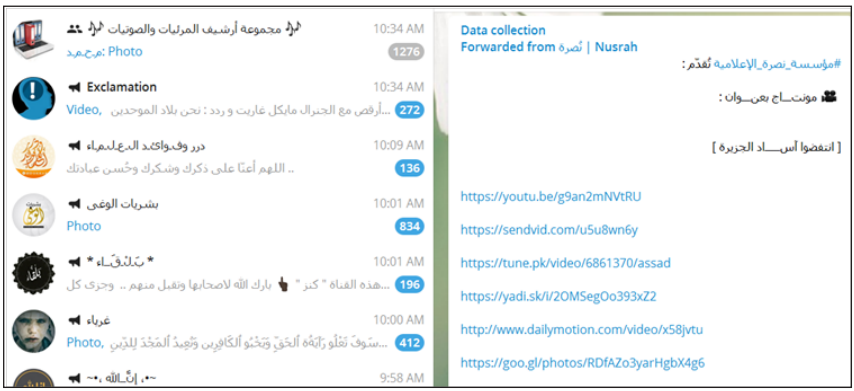



*Figure 6:* Hybrid weblog links to ISIS content disseminated via Telegram (screenshot by Authors).

In the context of this study, we consider stigmergy as an important element affecting the OODA loop speed of ISIS information operations, and the resilience of ISIS C2 functionality even under sustained degrading attacks. Robb breaks down the mechanics of stigmergic coordination in NCW into the following elements: marker-based, sematectonic, quantitative and qualitative.

*Marker-based*

This form of stigmergic coordination involves semantic payload markers, or signs, left by actors to communicate with and influence the actions of other actors. A good example are the short videos left behind

by ISIS-influenced 'lone wolf' attackers, in which they describe their upcoming actions and pledge allegiance to the terror network. Such videos are then distributed across ISIS-related channels and social media, and act as semantic payloads for future attackers. News of the attack presented by mainstream media is also a marker in this context.

*Sematectonic*

This form of coordination is a passive environmental signal affecting all actors in the theatre of operations, because it signifies a change in the underlying conditions of the battle-space. As Robb notes, "stigmergic systems use simple environmental signals to coordinate the actions of independent agents (each with their own decision-making process)". [51] When a vector of attack is blocked by a change in the environment (increase in airport security), this acts as a sematectonic stigmergic signal for the distributed swarm actors to change the vector of attack. For example, the attacks on transportation network hubs such as train stations and airports by ISIS 'lone wolf' or 'wolf pack' operators in 2015-16. In another example, ISIS affiliates interpreted degrading operations against their networks as a sematectonic signal and in an example of manoeuvre warfare urged followers to migrate to the zeronet.io protocol on the BitTorrent network. [52]

*Quantitative*

Quantitative signals can be easily identified and measured as they are scalable and with nonlinear effects. [53] A single attack, and an adversary's response to it, can scale up and generate stigmergic effects globally, which increases non-linearly the costs to defend against it. For example, the 'lone wolf' Nice attack in France, when a terrorist killed 80 people with a delivery truck, generated a strong quantitative stigmergic signal. In the aftermath of the attack France declared a state of emergency, while authorities in a number of Western countries built barricades around New Year's and Christmas celebrations in an effort to cancel this vector of attack. Quantitative stigmergic signals therefore can be very effective in communicating an attack vector, while also increasing non-linearly the costs to defend against such attacks.

*Qualitative*

This form of coordination is a combination of all four stigmergic signals, representing a continuous variation whereby the change in signal represents a change in the semantic payload. A prolonged swarm attack against a target is likely to involve qualitative stigmergic signalling.

Furthermore, ISIS' stigmergic operations can be described through what Marsh and Onof call the agent, environment, and sign feedback loops. [54]

*a) Agents:*

ISIS-related e-jihadists and affiliates operating executing information warfare operations across social media platforms. In this context, ''all that is necessary for stigmergy to occur is for the outcome of the behaviour of the relevant agent to be appropriately affected by previous environmental changes". [55]

*b) Environment:*

The environment is understood as a mediator affording a feedback loop between agents and their surroundings. For example, this can be a social media platform or a distributed protocol such as ZeroNet.io used by ISIS affiliates in their operations. In this context, "stigmergy distinctively relies on the cybernetic relationship of agent – environment – agent - environment through ongoing and mutual modification or conditioning enabled by the rise of computing technologies". [56]

*c) Sign:*

Similar to Robb's marker-based type, this is a collection of semantic trails linked to ISIS content, including direct links to terrorist propaganda dispersed across platforms. The rise of anonymous cloud sharing platforms has created unique stigmergy opportunities for ISIS information warfare, as all uploaded content is immediately transformed and shared as so many pheromone trails that can be easily followed, duplicated and distributed across digital media environments.

In this respect, Marsh and Onof have argued that the cybernetic loop of modification and conditioning of agent-environment-agent-environment is an ongoing part of stigmergy, dissolving group tensions through indirect communication. [57] Arguably, the dynamics of stigmergic operations have allowed ISIS to build resilient networks of information sharing and stigmergic participation.

## ISIS OODA loop dynamics

So far we have examined how ISIS' leveraging of multiple social media platforms and online environments in the context of a short OODA loop and stigmergic swarm tactics has generated powerful NCW effects. As we argued, these effects can be examined by observing the OODA cycles of ISIS and its adversaries. On the one hand, the rise of anonymous cloud sharing platforms and encrypted communication applications has made possible immediate information dissemination coupled with relatively secure information flows. This has increased the information warfare capabilities of ISIS networks by increasing the costs of their disruption and suppression. On the other hand, rapid unimpeded communication and collaboration between ISIS network sympathisers and affiliates is of fundamental importance for the success of the organisation's swarming tactics. These often contradictory tendencies have necessitated that the terror group manoeuver its information operations rapidly between digital environments, and disseminate high volume of information in order to speed up the proliferation of stigmergic signals and shorten its OODA loop cycle between the decide and act phases (Figure 7).

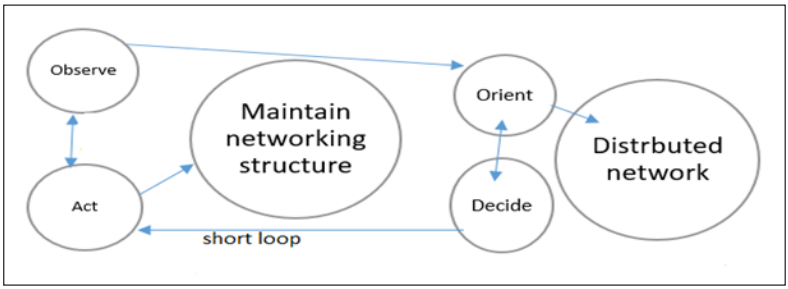



*Figure 7:* The OODA loop of ISIS networks (source: Authors)

Crucially, stigmergic swarming operations are fundamental in maintaining short OODA loops in an environment of active network suppression. These short loops in turn help the network to maintain its internal coherence and adapt to external stimuli. In that context, Osinga's tactic of "interaction and isolation" adapted by ISIS adversaries based on centralised C2 operations appears to have a longer cycle than the short loop of the much more distributed terrorist network.

As argued above, the observe and orient phases in the OODA loop of a decentralised network relying on stigmergy and swarm tactics are fast and agile, allowing the network to rapidly adapt to changing conditions and therefore operate inside the decision cycle of its opponents. As we argued, in the context of swarm operations agility and speed of command and execution are achieved through the self-synchronization of participants using stigmergic communications in an auftragstaktik paradigm. As Cebrowski and Garstka point out,

> Speed of Command is the process by which a superior information position is turned into a competitive advantage. It is characterized by the decisive altering of initial conditions, the development of high rates of change, and locking in success while locking out alternative enemy strategies. It recognizes all elements of the operating situation as parts of a complex adaptive ecosystem and achieves profound effect through the impact of closely coupled events. [58]

Keeping this point in mind, the coordinated degrading operations against ISIS led to the continuous suspension of their social media accounts, and subsequent risks of information flow disruption and network isolation. Accordingly, in adopting swarm tactics ISIS shortened their OODA cycle by relying on stigmergy to compress the time between observe and act phases. That is to say, the adoption of swarm tactics helped ISIS to function effectively in a highly hostile environment, as swarming agents used stigmergic signalling to share information with other affiliates across multiple media environments (Figure 8).

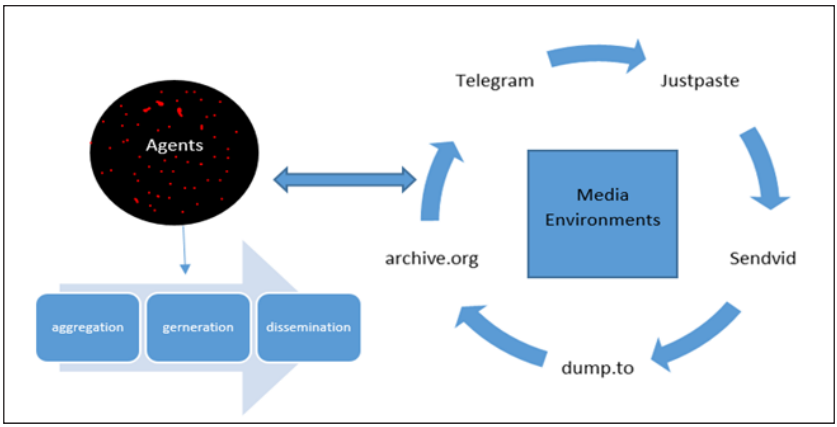



*Figure 8:* ISIS swarming operations (source: Authors)

As shown in Figure 8, ISIS-related agents conducted self-synchronized swarming operations adopting interchangeably the roles of generators, aggregators and disseminators.

*Generators*

We have identified two types of information generators. The first are active agents who are operating inside, or are embedded with, active ISIS combat units recording live footage of ground operations. The second are ISIS affiliates who gather or produce content for propaganda purposes, such as, for example, Asawrty and Shami Witness on Twitter, or the Nasher news, Dabiq, and Amaq channels on Telegram (Figure 9).

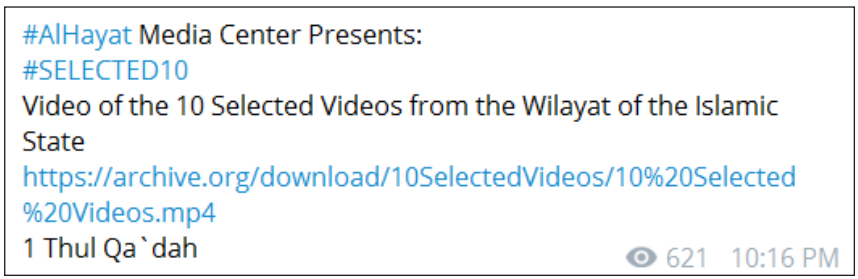



*Figure 9:* Example of the information generator #al-Hayat (screenshot by Authors).

*Aggregators*

This role includes active terrorist combatants and e-jihadists who have responded to the calls of ISIS spokesman abu-Muhammed Adnani that fighting in the media is more important than fighting in the physical war. The role of aggregators is focused on collating content to be included in their propaganda war, and involves a continuous mapping and collection of ISIS-related content appearing across multiple media environments. The aggregate content involves data collected for future retrieval and re-distribution, and data used for immediate propaganda purposes. In that context, aggregators play a pivotal role in sustaining ISIS' propaganda operations and keeping collected data safe to recycle when needed. The 'Nashir political service' channel on Telegram is a good example of the aggregator role among ISIS affiliates (Figure 10).


*Figure 10:* Example of an information aggregator on Telegram (screenshot by Authors)

*Disseminators*

Agents playing the role of disseminators use content from the aggregators and generators to maintain the intensity of ISIS-related terrorist propaganda across media platforms. Self-synchronization during swarm operations is usually the work of disseminators as their activity is concentrated on finding and establishing bridgeheads of information diffusion across media platforms (Figure 11).


*Figure 11:* Example of an information disseminator on Telegram (screenshot by Authors)

As Arquilla & Ronfeldt argue, rapid self-synchronization during swarm operations is "crucially important because swarm forces depend upon uninterrupted flows of information to actualize their potential". [59] In this context, agent collaboration in the roles of information generation, aggregation, and dissemination through self-synchronization in swarming operations seems to have enabled the ISIS terrorist network to run effective NCW. That is, self-synchronisation between ISIS-related affiliates is a primary characteristic of swarm manoeuvring at speed, or, as Cebrowski & Garstka note, "self-synchronization is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up […]" and is enabled by a "high level of knowledge of one's own forces, enemy forces, and all appropriate elements of the operating environment". [60] To this end, this is an example of John Robb's concept of an "Open Source warfare" [61], where the rapid proliferation of communication platforms has facilitated the ability of "non-state networks to challenge the structure and order of nation-states" [62].

## CONCLUSION

In this paper we examined some of the dynamics of information-centric warfare between the ISIS terrorist network and its state and non-state adversaries in the information domain. The study used the OODA loop concept to examine the swarming operations of ISIS and its adversaries, in

order to develop a more granular understanding of the role of the OODA loop cycle in NCW operations. With ISIS' forces dispersed across vast geographic and virtual distances, digital media environments offered the terrorist group unique, secure, and free communication platforms to coordinate attacks and achieve its information operation objectives. Specifically, the rise of anonymous and cloud sharing platforms enabled ISIS to rapidly manoeuvre across digital environments and establish a resilient decentralised communication network. This in turn allowed the terrorist network to weather the massive degrading and disruption operations against it by engaging in swarm tactics and utilising stigmergic communication methods. Our argument concluded that by leveraging swarm tactics and stigmergic communication ISIS often managed to operate inside the OODA loop of its adversaries. That is, the decision-making cycle of ISIS-affiliated e-jihadists was often faster compared to the OODA loop of the centralised networks combating the terror group.

## About the authors

*Ahmad Shehabat (ams591@uowmail.edu.au)*

Ahmad Shehabat is a PhD candidate in the School of the Arts, English and Media at the University of Wollongong. His PhD projects examines the digital media logistics of ISIS networks. His previous research focused on the role of digital media networks during the Arab Spring uprisings.

*Dr Teodor Mitew (tmitew@uow.edu.au)*

Dr Teodor Mitew is a Senior Lecturer in digital media in the School of the Arts, English and Media at the University of Wollongong. His research background is in actor network theory and internet studies. His current projects range across the internet of things, swarm content networks, memetic warfare, object oriented ontology, and smart textiles.

## REFERENCES

[1] Nissen, T. E. (2015). The weaponization of social media: Copenhagen, Denmark: Royal Danish Defense College. P.71

[2] Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). Network centric warfare: Developing and leveraging information superiority.

[3] *ibid,* p.88

[4] *ibid,* p.93

[5] Smith, E. A. (2003). Effects Based Operations: Applying network centric warfare in peace, crisis, and war: DTIC Document.

[6] Cebrowski, A. K., & Garstka, J. J. (1998). *Network-centric warfare: Its origin and future.* Paper presented at the US Naval Institute Proceedings. p.6

[7] *ibid,* p.3

[8] *ibid,* p.3

[9] Smith, 2003, ibid.

[10] Osinga, F. P. (2007). *Science, strategy and war: The strategic theory of John Boyd:* Routledge.

[11] Smith, 2003 , *ibid.*

[12]Nissen, 2015, *ibid* p. 71

[13] Cebrowski & Garstika, 1998, *ibid,* p. 4

[14] Safranski, M. (2008). The John Boyd Roundtable: Debating Science, Strategy, and War. *Ann Arbor Mi: Nimble Books.*

[15] Osinga,2007 *ibid.* p.72.

[16] Osinga, F. (2005). Science, Strategy and War. *Delft, The Netherlands.* p.6

[17] Kopp, C. (2005). Understanding network centric warfare. *Australian aviation,* January/February. p.2

[18] Osinga, 2007, *ibid*

[19] Osinga, 2005, *ibid*

[20] Richards, C. (2012). Boyd's OODA Loop (It's Not What You Think). *Abril de.* p. 9

[21] Boyd, J. R. (1996). The essence of winning and losing. *Unpublished lecture notes.* p.1

[22] *ibid,* p.3

[23] Smith,2003, *ibid.*

[24] Osinga, 2005, *ibid.*

[25] Arquilla, J., & Ronfeldt, D. (2000). Swarming and the Future of Conflict: DTIC Document. p.72

[26] Smith,2003,.p.61 *ibid.*

[27] Richards,2012, p.9 *ibid.*

[28] Safranski, 2008, *ibid.*

[29] Osinga, 2007, *ibid.*

[30] Cited in Safranski, 2008, *ibid.*

[31] Berger, J., & Morgan, J. (2015). The ISIS Twitter Census. *The Brookings Project on US Relations with the Islamic World, Analysis Paper*(20).

[32] Waller, M. (2015). Designing an Information Warfare Campaign Against the Global Jihadi Movement (2014): Threat Knowledge Group. p.30

[33] Nissen, 2015 p. 53, *ibid.*

[34] Cited in Arquilla & Ronfeldt, 2000, p. 22, *ibid.*

[35] Arquilla & Ronfeldt, 2000, p. 43 , *ibid*

[36] Robb, J. (2007). *Brave new war: The next stage of terrorism and the end of globalization:* John Wiley & Sons. p. 122

[37] *ibid,* p.122.

[38] Prucha, N. (2016). IS and the Jihadist Information Highway–Projecting Influence and Religious Identity via Telegram. *Perspectives on Terrorism,* 10(6). p.52

[39] *ibid,* p. 54

[40] Cebrowski & Graska 1998, p.3 *ibid.*

[41] Arquilla & Ronfeldt, 2000, p. vii, *ibid.*

[42] *ibid,* p.4

[43] *ibid,* p.vii

[44] *ibid,* p. 43

[45] *ibid,* p.5

[46] *ibid,* p.67

[47] Robb, J. (2004). The Marines and Stigmergic Awareness. Retrieved from http://globalguerrillas.typepad.com/globalguerrillas/2004/10/journal_the_mar.html

[48] *ibid*

[49] Robb, 2007, p. 124, *ibid.*

[50] *ibid,* p.124

[51] *ibid,* p.124

[52] Liang, C. (2016). Mpping The New Global Criminal-Terrorist Networks. p.86

[53] Robb, 2004, *ibid.*

[54] Marsh, L., & Onof, C. (2008). Stigmergic epistemology, stigmergic cognition. *Cognitive Systems Research,* 9(1), 136-149. p.7

[55] Holland, O., & Melhuish, C. (1999). Stigmergy, self-organization, and sorting in collective robotics. *Artificial life, 5*(2), 173-202. p.174

[56] Marsh, L., & Onof, C. (2008),p.7, *ibid.*

[57] *ibid,* p.14

[58] Cebrowski & Graska 1998,p.6 *ibid.*

[59] Arquilla & Ronfeldt, 2000, p. 67, *ibid.*

[60] Cebrowski & Graska 1998,p.10 *ibid.*

[61] Robb, 2007, p. 16, *ibid.*

[62] *ibid,* p. 17