TACtical Intelligence:

Disrupting the Terrorist Attack Cycle by Analysing Terrorists' Intelligence Operations

July 2021

2486209D
19108591
90652073

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word Count (excluding front and back matter): 20091

Word Count (including front and back matter): 23074

Supervisor: Ken McDonagh

Date of Submission: 20 July 2021

With utmost gratitude to

TD, SD, JA, VN, RP, EDS, KM, DVP, and JAG

whose intelligence, guidance, support, and feedback afforded her the confidence needed for this to succeed.

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu, The Art of War

Table of Contents

Abbreviations

AQ: al-Qaeda[1]

AMISOM: African Union Mission in Somalia

CCA: complex, coordinated attack

CI: counterintelligence

CIA: United States Central Intelligence Agency

FARC: Fuerzas Armadas Revolucionarias de Colombia—Ejército del Pueblo ("Revolutionary Armed Forces of Colombia")

GEOINT: geospatial and satellite imagery intelligence; formerly SIGINT, signals intelligence

HUMINT: human intelligence

IC: intelligence cycle

IED: improvised explosive device

IRA: Irish Republican Army

IS: Islamic State [Daesh][2]

KLA: Ushtria Çlirimtare e Kosovës ("Kosovo Liberation Army“)

LTTE: Tamil̲īl̲a viṭutalaip pulikaḷ ("Liberation Tigers of Tamil Eelam")

MASINT: measurement and signature intelligence

NGOs: non-governmental organisations

NSA: non-state actor(s)

OSINT: open-source intelligence

PIRA: Provisional Irish Republican Army

SAT: Structured Analytic Technique(s)

TAC: terrorist attack cycle

TACtical: author's neologism describing terrorists' intelligence activities during attack planning and preparation

VBIED: vehicular-based improvised explosive device; 'car bomb'

VNSA: violent, non-state actor(s)

VNSA-T: terrorist(s)

[1] Note: This study analyses the broader group known as al Qaeda as under leadership of Osama bin Laden. The study first summarises the organisation's intelligence across all its operational regions; in the second half of its concentrated case study, this narrows to focus on the tactical cell operating in East Africa which instigated the 1998 U.S. Embassy bombings in Kenya and Tanzania.

[2] Note: This study adopts the name "Daesh" to refer to the terrorist organisation also known as "The Islamic State," "ISIS," or "ISIL" and analyses the broader group as under leadership of Abu Bakr al-Baghdadi. The study also first summarises the organisation's intelligence across all its operational regions, and in the second half of its concentrated case study, narrows focus to the tactical cell operating in Europe which instigated the 2015 Paris Attacks.

Towards Understanding the Violent Non-state Actor

On the modern international security stage, wherein the state has a monopoly over political supremacy, considerable resources, and the use of legitimate force, violent non-state actors (VNSAs), including terrorists, are debatably at a discernible competitive disadvantage.

Yet, despite this disadvantage, terrorists can compete with state rivals by circumventing, stressing, or negating the security and intelligence services of the state and by staging attacks, which are perceived to further the pursuit of their *dreams,*—wider aspirations supported by an actor's belief, faith, and confidence—attainable through the completion of intermediary goals. At its root, the terrorist's competition with the state is supported by an intelligence competition, waged as they undertake intelligence activities to understand their adversary's capabilities (which are to be circumvented, stressed, or negated) and vulnerabilities (which are to be exploited) as well as their own capabilities (which are to be developed, expanded, or optimised) and vulnerabilities (which are to be minimised). These intelligence undertakings yield *confidence*—a sense of knowledge, security, certainty, and control over uncertainty and unpredictability—and it is the euphoria of high confidence which lends the rebel a sense of self-assurance, willpower, and resilience to execute attacks and which offers a sense of purpose as a contributor to the success of the dream. Summarised best in a handbook distributed by the Irish Republican Army (IRA), "Good intelligence breeds good morale. And for the guerrilla morale is everything. It is this morale that gives the guerrilla his determination and his daring" (Irish Republican Army (IRA), 1965). To know and to understand the intelligence capacities of terrorist organisations and how these contribute to the terrorist's confidence and conduct in planning and preparing for attacks has relevance for preventing, detecting, or mitigating future acts of terror. However, this intelligence competition between terrorist organisations—seeking to instigate attacks—and their state rivals—seeking to thwart them—is underdeveloped in both academic intelligence and terrorism studies. By overlooking this nexus, these fields are further devoid of the implications the intelligence competition has for understanding and assessing terrorist actors, developing indicators of intent and ability, prioritising the extent of their threat, and preparing crisis management and contingency strategies.

Purpose of the Study

The purpose of this study is thus twofold. First, this research strives to expound upon the nascent academic literature regarding VNSA intelligence by exploring the role and uses of intelligence in the planning and executing phases of an attack. The second is to apply these findings to contribute ideas for counterterrorism efforts by highlighting opportunities where it might be possible to anticipate, detect, or mitigate terrorist attacks. This study is also important as deviating from a state-centric perspective on intelligence underscores the tenet "Security for whom?" This researcher stresses seeking to understand terrorists as intelligence actors might better position state actors in the intelligence competition and orient efforts to pre-empt or address the effects of violence and terror. The following research argues terrorists operationalise intelligence in two ways: to acquire an acute understanding of the capabilities and vulnerabilities of *themselves* and those of their *adversaries*. Exploiting intelligence consequently provides terrorists with a necessary degree of *confidence* that enables them to engage in competition with their adversaries and thus plan and instigate attacks—rational acts of violence undertaken in the wider pursuit of a social or political *dream*.

Research Questions

Two questions underpin the heart of this research:

1. How do terrorist organisations collect and utilise intelligence in preparation for staging attacks?

2. How do these intelligence activities pose challenges for state counterterrorism efforts?

Research Aims

The research aims to analyse the intelligence capabilities and activities of terrorists as they plan, prepare for, and instigate attacks broadly and by highlighting three case studies: al-Qaeda, Daesh, and al-Shabaab. It also aims to offer ideas for frontline counterterrorism and intelligence personnel pertaining to the prevention, detection, and response to terrorist attacks by utilising SATs in an exercise of how planning of a complex, coordinated attack could unfold. Through this work, this research further evaluates the robustness of prevailing intelligence and terrorism theories, chiefly the Intelligence Cycle (IC) and Terrorist Attack Cycle (TAC), and proposes an alternative framework: Terrorist Intelligence and Confidence (TIC).

Scope & Limitations

Spatial and time constraints curtail the scope of analysis to a concentration predominantly on three case groups: al-Qaeda, Daesh, and al-Shabaab. Particulars of case selection are discussed later in the methodology section of this study. In addition, three assumptions underpin the present study. First, terrorists are rational actors, who, in consideration of their emotions, previous experience, perceived inability to communicate, and present circumstances, perceive the decision to evoke violence or terror as a rational choice. Second, because they intend to communicate a broader social or political dream, terrorist attacks are premeditated acts of violence. By this definition, terrorist attacks—especially the complex, coordinated operations covered in this study—require a minimum degree of prior planning and are not random, spontaneous, or unintentional. Last, this research assumes that an attempt to better understand terrorists, including their intelligence capacities, will prove useful for counterterrorism efforts. This assumption does not attest that a better understanding will permit an ability to deter all acts of violence or stop them outright; rather, a better understanding of terrorists, their dreams, purposes, activities, capabilities, and vulnerabilities might engender additional approaches to handling terrorism threats. Data collection for this research is limited to a qualitative review of English/English-translated, open-source material, including declassified/open-access terrorists' works,—including manuals, handbooks, magazines, letters, and notes—terrorists' statements and interviews, court documentation, governmental reviews and investigative reports, newspaper reports, investigative journalism, scholarly articles and research, and books. The two primary case studies—al-Qaeda and Daesh—were chosen explicitly as these organisations have received considerable academic and practitioner inquiry and attention from the media, especially in regard to intelligence, and there is thus a comparatively greater amount of available source material. To reemphasise, however, the quantity of literature on terrorists' intelligence itself is comparatively scant compared to other topics of intelligence and subjects relating to terrorism.

Interestingly, however, facing limited 'intelligence' regarding terrorists' use of intelligence and seeking to extrapolate relevant material from "historical cases" (Gill, 2010, pp. 2-3) to build tentative theories or hypotheses to inform of possible threats or opportunities, this project mirrors the work of an intelligence analyst, who acts similarly "to make sense of and thus actively 'create' the worlds of intelligence and government" (Gill, 2010, pp. 2-3). Limited information and access additionally hint at the most significant caveat of this study: it is ignorance and a lack of understanding of how and why terrorists use intelligence, which paradoxically accentuate this research's main points, being the necessity of utilising intelligence to take informed, appropriate action. Phrased differently, in large due to terrorists' appreciably secretive, decentralised, and impenetrable counterintelligence cultures, developing a verified understanding of their goals, motives, beliefs, choices, and decision-making processes is challenging. However, a modest attempt can result from the study of secondary material and external observations and interpretations of these actors' signals: their overt speech, actions, and behaviours. This caveat can motivate further research, such as through more thorough document analysis or interviews conducted with defectors (for example, see Speckhard & Yayla, 2017). Lastly, it is worth noting two additional points. First, it is acknowledged terrorists do not all possess the same resources, operate in the same ways, nor seek to achieve the same dreams; the same can also be said for nation-states and their security/intelligence mechanisms. Second, terrorists might have adversaries beyond or in addition to states. Nevertheless, in an attempt to understand the terrorist-state intelligence competition as the scope of this research, this researcher argues some conclusions can be made about terrorists' intelligence and their confidence-building mechanisms generally. This is because, as in line with the predominant Realist approach in academic security, intelligence, and political science studies and the modern international system—underscored by Westphalian sovereignty—terrorists have common ground in being at a seeming asymmetric disadvantage, due in large part to the state's monopoly over authority, resources, and the legitimate use of force. Expanding upon these points, this study underscores the terrorist's dream is essential; indeed, terrorists can justify attacks and acts of violence in their struggle to pursue and contribute to its achievement. Lastly, while not minimising their importance, deeper inquiry into the idiosyncrasies between actors' dreams and the dream's influence on tactics or strategy is generally outside the current scope of this study, which concentrates on the role of intelligence in attack planning and preparation.

The structure of this study is as follows: first, a review of the relevant literature to precisely define intelligence and terrorism, both of which remain hotly contested in academic and practitioner circles. Next, the study explores dominant theories within each discipline—for the former, the intelligence cycle and in the latter, the terrorist attack cycle. Each of these theories postulates on the *hows* of their disciplines, that is, *how* intelligence is conducted and utilised and *how* terrorist organisations plan and execute attacks. Recognising the interplay at the intersection of these fields, this study then proceeds with a review of existing scholarship on violent non-state actors' intelligence, including groups such as paramilitaries and insurgencies, accounting for the fact that scholarly inquiry into the nexus of these fields is currently in infancy. From this review, two inchoate theories of VNSA intelligence emerge, which this author evaluates independently and in comparison. Next, this study outlines its methodology in the selection of three case studies and its supposition to test the efficacy of these existing models and theories. Following an in-depth analysis of each case, this study proceeds to synthesise its findings. The results illustrate not only a detailed collection of *how* multiple terrorist organisations undertake intelligence activities but also proposes a nuanced understanding of *how* and *why* intelligence facilitates terrorist organisations in a competition against their rivals. These conclusions are also fruitful for first responders in their crisis management and incidence response plans, which this study strives to support. Accordingly, through the use of Structured Analytic Techniques, this study proceeds to channel the implications of its findings by investigating the possible strategies and outcomes of four terrorist attack scenarios. This study concludes with a proposal for a new framework of terrorists' intelligence and final remarks on the way forward in understanding terrorists' intelligence.

Setting Requirements: Definitions Matter

Intelligence

Before exploring how and why terrorists engage in an intelligence competition with states, it is necessary to define both 'intelligence' and 'terrorism.' No easy feats, definitional debates have long-entertained scholars for much of each respective field's existence. In the intelligence dispute, each writer dissects existing definitions to elucidate subtle nuances in the hopes of crafting *the* definition of intelligence, although thus far, these efforts have been in vain. Indeed, by nurturing and exacerbating these debates, the term has been used simultaneously to refer to products, activities, and organisations, resulting in an unclear classification and purview of 'intelligence' (Warner, 2002). Compounding the lack of consensus and clarity, additional deliberations over whether intelligence is an art or a science has confounded academics, for the answer has ramifications in conceptualising the field and developing theory; the former implies "subjective, intuitive judgment" (Marrin, 2018), whereas the latter entails objectivity dependent on "structured, systematic analytic methods" (Marrin, 2018). In one of the first definition attempts, Sherman Kent, a founding father of intelligence analysis as both a profession and academic discipline, defined the term as "high-level, foreign positive" knowledge, organisation, and activity (1949). In another, oft cited-definition, a pseudonymised CIA official Mr Random adds the element of secrecy to his characterisation and emphasises intelligence is fixated externally, explaining, "Intelligence is the official, secret collection and processing of information on foreign countries to aid in formulating and implementing foreign policy, and the conduct of covert activities abroad to facilitate the implementation of foreign policy" (1958). Lastly, following a comprehensive analysis of seventeen definitions of intelligence, historian Michael Warner develops a definition similar, yet, pared down from Random's definition, concluding "Intelligence is secret, state activity to understand or influence foreign entities" (2002). From these definitions, intelligence can be conceived as a simultaneous product, process, and organisation. Under these notions, intelligence units composed of personnel, equipment, and facilities—the *organisation*—apply a variety of methods to collect, collate, evaluate, and analyse data and information—*the processes*—to produce *products*, which aim to inform on a client's needs (Warner, 2002; Lowenthal, 2020). By informing a client about a given subject matter of interest and illuminating areas where the client can make decisions or take action, intelligence can thus also be "both a *form of* and *resource for* the exercise of power" (Gill, 2018, p. 581).

In line with Realist influence and a state-centric approach, each of these definitions fails to account for fields beyond military and political science where intelligence is applicable, such as business (Breakspear, 2013), medicine (Marrin & Torres, 2017), and history (Marrin, 2017), or additional actors for whom intelligence serves a function or utility such as non-state actors, including businesses (Breakspear, 2013), non-governmental organisations (Gentry, 2016), criminal groups (Kenney, 2008), insurgents (Jackson, 2019; Strachan-Morris, 2019b), or terrorists (Gentry, 2016; Illardi, 2009; Illardi, 2010). Recognising there will be no one-size-fits all definition, as context and priorities differ in the application, for this research, intelligence is thus regarded as the *product of processed and organised knowledge that provides an actor with a baseline understanding of a subject and the confidence to take action through intermediary objectives to pursue their dream*. This definition, while broad, permits for additional nuances and reemphasises the importance of recognising an array of activities—overt and covert—as well as additional intelligence actors, for whom intelligence serves a particular purpose to understand, manipulate, or otherwise engage with their environment, circumstances, or other actors. Intelligence also permits an actor to perceive they have a greater understanding, degree of control, or power over the unknown or unpredictable, thereby breeding confidence to act. Viewed by way of a cost-benefits approach, intelligence serves tactical-, operational-, or strategic- level purposes to illuminate and reduce threats, to take advantage of opportunities, and to guide those in a position to make decisions or take action. While such actions might be suboptimal, when these decisions or actions are taken, they are generally perceived to be more beneficial or favourable than other courses of action, which might be perceived as too costly, risky, or otherwise less favourable towards the actor's dream. Additionally of note, this definition utilises the term '*dream'* to refer to an actor's profoundly broader or ultimate vision—a commitment supported by confidence, belief, or faith—believed to be attainable through accomplishing intermediary goals or objectives.

Terrorism

When defining 'terrorism,' a definitional deliberation has likewise challenged academics and practitioners as the term is both subjective and pejorative, the extent of this contention best illustrated by the cliché "one man's terrorist is another man's freedom fighter" (Laqueur, 1987, p. 302). This cliché underscores the importance of perception in the definitional debacle, but also in wider issues of security, summarised as "Security for whom?"—what is security for one might not be security for another. Walter Laqueur, a life-long scholar of terrorism studies, defines terrorism as "the use or the threat of the use of violence, a method of combat, or a strategy to achieve certain targets… [which] aims to induce a state of fear in the victim, that is ruthless and does not conform with humanitarian rules" (1987, p. 143). In this definition, Laqueur's meaning of 'target' is questionable; while in context it appears to refer to an intention, goal, or dream, the word 'target' can be mistaken to also refer to the recipient(s) of terrorist violence. Furthermore, despite including conformity with humanitarian rules, Laqueur does not detail an explanation of what these rules are, nor does he acknowledge the notion that "humanitarian rules" can fluctuate in contexts or situations. Expanding Laqueur's definition to elucidate both the particular aims of terrorism as well as the constitution of humanitarian law, Bruce Hoffman, a political science and (counter)terrorism analyst and co-founder of the University of St Andrew's Centre for the Study of Terrorism and Political Violence proposes

> Terrorism is ineluctably political in aims and motives, violent—or, equally important, threatens violence, designed to have far-reaching psychological repercussions beyond the immediate victim or target, conducted by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia), and perpetrated by a subnational group or non-state entity (2006).

This definition excludes individuals who might act independently of, be unaffiliated with, or be inspired by an organisation, group, or cell; this definition is additionally questionable when considering the degree to which an "identifiable chain of command" exists. Indeed, in some cells or organisations, to the external observer, a chain of command, structure, or hierarchy might be indistinguishable, whereas the chain of command is clearly recognised by those 'within.' Finally, limiting the perpetrating entity to a "subnational group or non-state entity" risks eclipsing the threat of state-directed or state-sponsored terrorism. A final definition important for this research's purposes, which emphasises operational acts,—*attacks*—terrorism scholars Brent L. Smith, Paxton Roberts, and Kelly R. Damphouse approach the debate by differentiating "terrorism" from "traditional criminality," asserting that in addition to its political or social motives, the former "usually involves considerable planning and preparatory conduct" (2017); consequently, terrorist attacks, contrary to the caricatures proliferated in the media, are rarely spontaneous or opportunistic, nor are they crazed and irrational. For this research, to eschew the confusion over 'targets' as 'victims' or 'dreams,' to capture the premeditation of violence in planning complex coordinated attacks, and to illustrate there is intent and rationality behind sowing terror and fear in a subject and utilising terror in pursuit of an array of possible dreams, the author's following definition of terrorism is applied: *Terrorism refers to the rational, premeditated threat or use of violence to evoke terror and instil fear in a direct or indirect recipient and is intended to communicate or further the pursuit towards a wider social or political dream.*

It is also important to emphasise on the modern security stage, owing to political, legal, and social influences, the Westphalian state enjoys greater access to material resources and a monopoly over the use of legitimate violence. This implies terrorists will engage with their opponents through alternative means, psychologically, for instance, by propagating terror and exercising a monopoly over the element of surprise. The monopoly over surprise entails terrorists can coerce, intimidate, threaten, or persuade their adversaries, or, at a minimum, demonstrate the adversary has weaknesses or can be defeated; attacks thus trigger or expose the weaknesses of the adversary in such a manner that the effects of the attack (for instance, rallying support from sympathisers, forcing the adversary to withdraw from an environment) are favourable to the attackers' dream. Terrorists thus engage in an intelligence competition with their adversaries—a pursuit to understand their opponent's vulnerabilities and capabilities as well as their own vulnerabilities and capabilities. The intelligence competition reveals opportunities and fosters confidence through which terrorists leverage their power to engage in the struggle and assert their control towards the fulfilment of the dream.

Having addressed definitional matters—the '*what'* of intelligence and terrorism—this study now turns to evaluate theoretical models which strive to describe the '*how*,' or the methods and activities of intelligence and terrorist attacks and the extent to which these illustrate the intelligence rivalry. First explained is the traditional Intelligence Cycle (IC), a conceptualisation that, notwithstanding its shortcomings, endures rampantly as a dominant theory of intelligence in traditional political science, military, and security studies; this cyclical framework depicts the 'stages' of intelligence operations and functions. Second is the Terrorist Attack Cycle (TAC), a model which bears similarity to the former and illustrates the 'stages' of how a terrorist conducts an attack. Evaluating the models in tandem, this study evaluates their robustness in a cross-disciplinary approach of "terrorist intelligence." Phrased differently, this research undertakes an effort to gauge the extent to which the functions, methods, and purposes of intelligence as prescribed in the IC are apparent terrorists' intelligence, and further, if the terrorist's intelligence and their competition with state adversaries can be evidenced in the framework of the TAC.

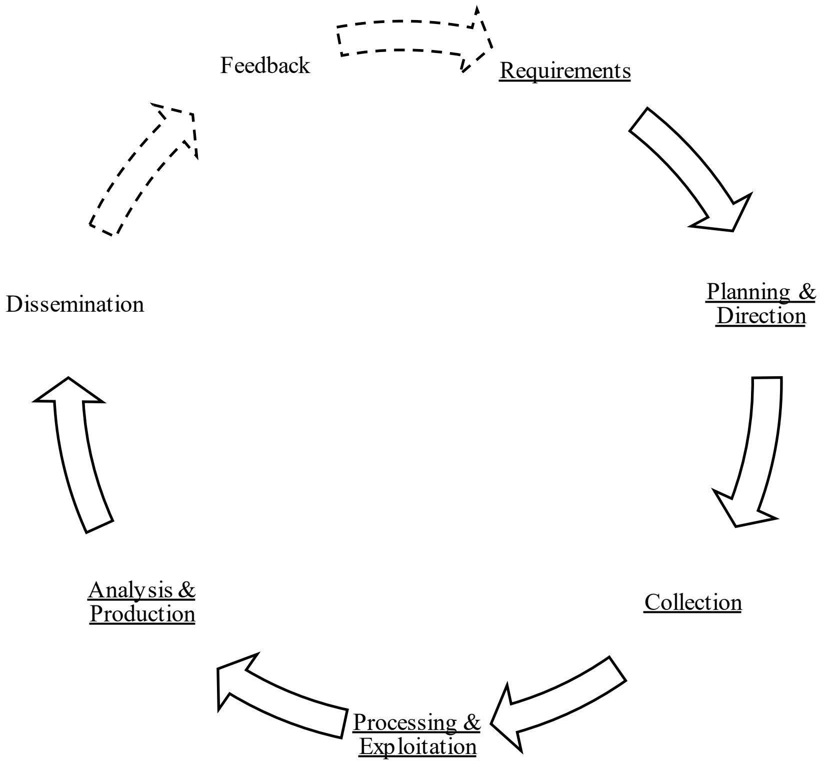
Determining the Direction: A Cyclical Approach

The Intelligence Cycle

To understand the role of intelligence as a confidence-building mechanism that facilitates and supports a terrorist's perceived ability to compete with and stage attacks against the state and in pursuit of a dream, this study explores theory on the functions of intelligence under the traditional intelligence cycle and theory pertaining to the activities undertaken by a terrorist to execute an attack.

Despite lengthy and contentious intelligence debates and receipt of significant academic attention, notably in the post-9/11 milieu, there is a dearth of literature on intelligence theory in terms of breadth; indeed, while new research commonly references intelligence theories, these contributions rely on, expound upon, or debate existing theories, models, and frameworks, as opposed to proposing new conceptualisations (Marrin, 2018). The Intelligence Cycle (IC) is a predominant intelligence theory that attempts to model the activities and functions—the *how*—of intelligence by depicting them in the form of a cyclical process, composed of five (Johnson, 1986) to seven (Lowenthal, 2020) stages. The traditional intelligence cycle is depicted in Fig. 1 below; stages underlined and marked in solid lines are emphasised in this research.

Fig. 1



Source: *Author. Traditional Intelligence Cycle*

The first stage is Requirements, during which a client's priorities and needs or the intelligence problem is identified and defined (Clark, 2017, p. 90). In the second, sometimes omitted, stage, Planning provides direction for the remaining components of the IC, chiefly to guide the collection of relevant information in sufficient quantities, depth, and breadth. This stage can be beneficial in minimising the 'wheat versus chaff' problem, which arises from the collection of more information than is needed, but through which analysts must dig and organise to find the key intelligence that is needed (Lowenthal, 2020, p. 73). The Collection stage of the cycle is often broken down into collection disciplines. Colloquially termed as "INTs" (Lowenthal, 2020, p. 94), these data collection methods range from the overt and nontechnical, such as open-source data (OSINT)—newspapers, academic studies, government publications, industry reports, and court documentation (Gentry, 2018),—to highly technical geospatial and satellite imagery (GEOINT), or signals intelligence (SIGINT)—intercepted signals in telephone communications, emails, or text messages (Gentry, 2018; Johnson, 1986, pp. 7-9),—measurements and signatures (MASINT) used to identify fixed targets, or covert or clandestine methods, such as human-sourced intelligence (HUMINT), often acquired through the use of spies or informants. This stage transitions analysts to the Processing stage, during which raw data is collated and processed through activities including the translations and validation of HUMINT-sourced data or the decryption of codes, signals, or technical texts and images (Lowenthal, 2020, p. 94; Gentry, 2018). During the Analysis stage, recognising smaller bits of intelligence form a bigger picture, the processed material is critically analysed and contextualised to elucidate alternative explanations or hypotheses, and paired with relevant historical or interrelated information to produce a finalised intelligence assessment or *product* (Kerstetter, 1979, p. 110). Dissemination is often the last stage of the cycle, describing the presentation or release of the intelligence *product* to the client or decision-maker. These functions serve to inform on the meaning and significance of a particular matter of interest to a client or decision-maker in a position to take or direct action. To be effective, it is also crucial that the intelligence product be presented in the right form and at the right time and place to be valuable for the client (Breakspear, 2013, p. 681). An additional stage, Feedback, is sometimes added to the traditional cycle (Lowenthal, 2020, p. 77), recognising the importance of intelligence producer-consumer relationships to improve the *organisation, processes, and products* for the next cycle. Accounting for disconnects not limited to differing roles, priorities, and needs, the extent to which feedback even occurs within stakeholders themselves or between stakeholders and one another in practice is debatable (Clark, 2017).

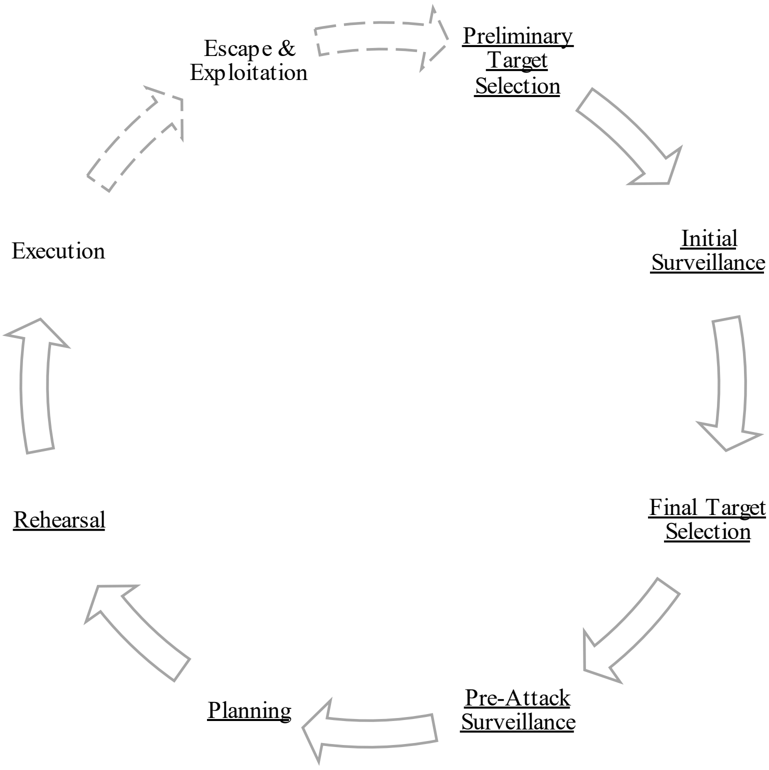
The IC is a convenient and comprehensible model, but its oversimplicity is discommoding, implying two salient shortcomings. First, portraying intelligence as a uni-directional *process* fails to illustrate the following: some stages might occur in a different sequential or multi-directional order than is depicted (Clark, 2017, p. 93); some activities might occur in tandem (such as collection and processing), independently, or not at all (such as a decision-maker's clear dictation of requirements) (Hulnick, 2006, p. 961); and the process might include multiple iterations or "loops" (Clark, 2013, p. 49; Lowenthal, 2020, p. 78) based on changes in requirements, new collection practices, or perceived gaps in analysis. Second, the IC fails to account for additional *procedures* within intelligence, such as counterintelligence (Shulsky & Schmitt, 2002, p. 8; Hulnick, 2006, p. 959), feedback, and even learning. Counterintelligence, or the protection and "preservation of intelligence assets" (Gentry, 2016, pp. 467-468), is offensively or defensively denying or deterring an adversary's attempts for access. For counterintelligence to be effective, the countermeasures must have a precise "understanding or anticipation" (Magee, 2010, p. 511) of self and adversary. 'Understanding of self' in the present research on terrorists includes the appraisal of one's understanding and commitment to the dream and the understanding of one's vulnerabilities (to be minimised) and capabilities (to be expanded, developed, or optimised); 'understanding of adversary' in the context of counterintelligence includes knowledge of the opponent's vulnerabilities (to be exploited) and capabilities (to be minimised, stressed, or negated).

Feedback—a form of self-reflexive critique—is also a critical step to improve the future efficiency or efficacy of intelligence to engender greater benefits to invested stakeholders; this step involves pursuing advantageous progress by streamlining processes, pursuing alternative approaches in recognition of gaps or obstacles, or elucidating 'lessons learned' from failures and successes. This research differentiates *feedback* from *learning* by the distinction that the former seeks development stemming from an understanding of and from *oneself*, whereas the latter pursues development from studying and analysing *others*, including one's allies and opponents.

Terrorist Attack Cycle

With a clearer idea of the methods and functions—the *how*—of intelligence and the inadequacy of the IC broadly, this research evaluates the Terrorist Attack Cycle (TAC), a similar framework that displays the "discernible" (Stratfor, n.d.) serial activities undertaken by a terrorist—the *how*—to orchestrate an attack. Surfacing frequently in U.S. counterterrorism and public safety manuals, the authors of such publications attest the model evinces that several preoperational stages are "often observable and can offer opportunities to identify plots and prevent attacks" (Joint Counterterrorism Assessment Team, n.d.). Fig. 2 below depicts the Terrorist Attack Cycle; stages underlined and marked by solid lines are the focal point of this study.

Fig. 2



Source: *Author. Terrorist Attack Cycle*

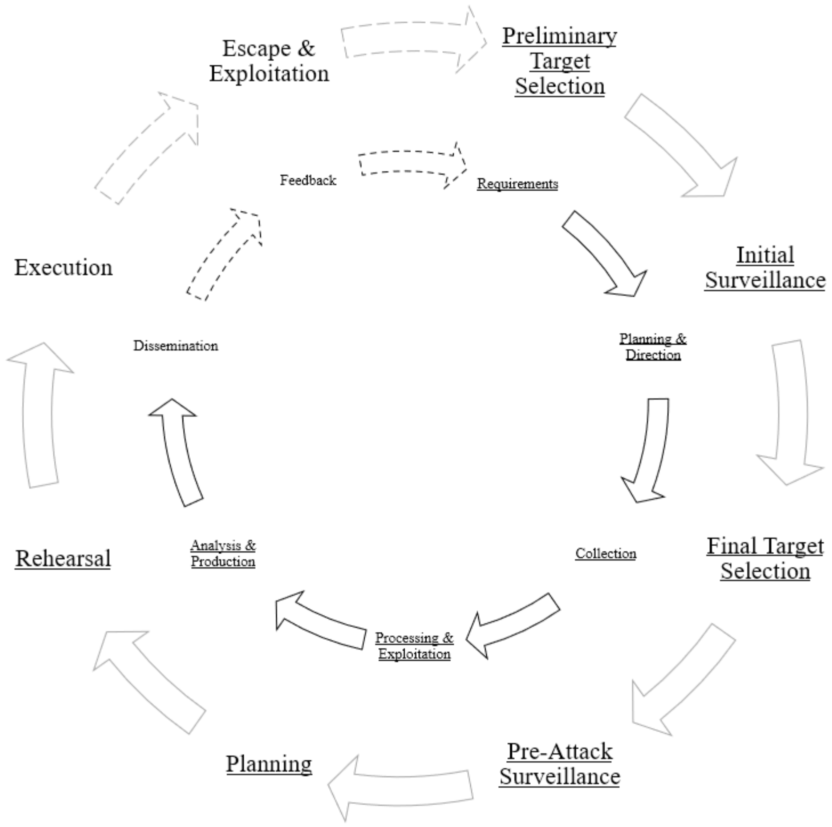
In the first stage of this cycle, Preliminary Target Selection, an actor selects an initial target of attack; choice might be determined by a variety of factors to varying degrees, such as actor *capability,* resources, intent or goal, ideology, or risk appetite. During Surveillance, a terrorist observes and studies their preliminary target. This stage can fall under the scope of 'learning,' which contributes to a terrorist's overall understanding of their adversary's vulnerabilities and capabilities. The third stage of the cycle is Final Target Selection, wherein utilising intelligence from prior surveillance stages, a terrorist concludes their initial target choice remains or is no longer a viable option (Stratfor, n.d., p. 3). Upon confirmation of their target, a terrorist conducts more thorough surveillance, noting particular details that will be relevant to the attack. Noting detail in reconnaissance is important as it enables the planner to develop a strategy of attack that is thorough, realistic, and plausible, and one that furthermore minimises the probability for unintended consequences, undue risk, or unexpected events and effects. During the Planning phase of an attack, an array of activities might occur depending on the type and scale of the intended operation, such as the selection of operatives; procurement of funds or equipment; establishment of front businesses; manufacture or acquisition of weapons; or training in foreign languages, hand-to-hand combat, or specific weapons (Stratfor, n.d., p. 3).

Next, Rehearsal is akin to a ‘dry-run’ of the operation, the purpose for which is to “confirm the validity of the information collected and intelligence derived” (Magee, 2010, p. 520) during surveillance and planning phases. A dry-run confirms an expected ground truth and permits fine-tuning details before execution or the development of contingency plans (Bennett, 2018, p. 198). These preoperational phases terminate with Execution, during which the attack is carried out. Lastly, in the final stage of the TAC, Escape and Exploitation, terrorists exploit the media—the ostensible “oxygen of publicity on which [terrorists] depend” (Thatcher, 1985 as cited in Hoffman, 2006, p. 184) to sensationalise and project their message to a wider audience (Stratfor, 2009, p. 12; Federation of American Scientists, n.d.). Terrorists might also remove themselves from the target site to a third location that offers safety, comfort, or protection.

The TAC offers an expedient lens from which to perceive the complexity engulfed in a terrorist attack; however, if the purpose for the model is to assist first responders in detecting the effectuating pre-attack indicators or preoperational activities (Joint Counterterrorism Assessment Team, n.d.) or to permit a more comprehensive understanding of the factors, considerations, and strategies encompassed in terrorist attacks, it is fruitful to evaluate the cycle’s overall validity and efficacy. Two significant misgivings underpin the TAC. Comparable to the IC, the first criticism is the model’s unidimensional, cyclical representations; indeed, while reasonable to assume “certain types of behaviors occur more frequently at different stages of the planning and preparatory cycle,” (Smith, et al., 2017, p. 68) such as Planning after Target Selection, the degree of uniformity across cases is contested. For example, an expanded arsenal of available matériel, personnel, and funds might imply a broader range of plausible attack targets. Some groups, such as in the case of al-Qaeda (Illardi, 2008), routinely and passively collect information about potential targets from operatives or sympathisers from around the world. Then, depending on the message terrorists intend to convey, one of the targets for which there is already a ‘file’ might be selected for ‘active’ engagement. In this example, much surveillance occurs *before* the identification of targets; only during the planning stages will more detail and precision be sought after. Al-Qaeda has also been known to establish front businesses around the world prior to selecting an attack target with the intention of establishing footholds from which to collect information and conduct additional operations (United States District Court Southern District of New York, 1998; United States Committee on Foreign Relations, 2001). This provokes a second criticism of the TAC. Striving towards a generalised conceptualisation that could be applicable for most terrorist attacks, the over-simplicity of the model fails to account for idiosyncrasies that might influence attack decision-making, planning, preparation, and execution. For instance, dry-runs can be considered imperative to ensure the operation's success; by ensuring a degree of control, power, expectation, and predictability over their expected targets, an operative feels more familiar with themselves, the operation, and the environment, thus boosting their confidence to act. The PIRA regularly ran rehearsals prior to attacks (O'Brien, 2008, p. 36) and their handbook, the Green Book, reiterates rehearsals should be conducted where possible (Irish Republican Army (IRA), 1965). Similarly, al-Qaeda operatives are known to have conducted dry-runs, especially in the lead up to the 9/11 attacks such as by enrolling in flight school and trialling the operation in the days leading up to the attacks (Illardi, 2008; Illardi, 2009; Kean & Hamilton, 2004). Conversely, an actor might perceive rehearsals pose undue risk to exposing the operation and actors to law enforcement, and thus not conduct a thorough run-through. Or, perceiving the window of opportunity to act to be closing, such as a tip-off to law enforcement, a group's sense of urgency to act might transpose this stage, which might have been the case for Aum Shinrikyo, the apocalyptic cult responsible for the 1995 Tokyo subway Sarin attacks (Brackett, 1996). Lastly, escape from the target scene might not be a requirement for the attack's success, such as for acts of suicide terrorism in particular (Hoffman, 2006, p. 132), where terrorists demonstrate the ultimate sacrifice for the dream.

Having appraised the efficacy of each model independently, it is evident there are similarities between the two, yet both apart and in tandem (Fig. 3), there is an appreciable gap regarding the functions of intelligence for terrorists during the preoperational phases of an attack.

Fig. 3.



Source: *Author. Correlations between the Intelligence Cycle (IC) (inner) and the Terrorist Attack Cycle (TAC) (outer)*

Moreover, the models fail to recognise the importance of intelligence as a confidence-building mechanism that allows a terrorist to perceive they have a sufficient understanding of themselves and an adversary, situation, or environment, which enables them to take action. Though these might not be clear, complete, or wholly accurate understandings, intelligence affords the actor a way to perceive they have some degree of control, certainty, or predictability over the outcome of a given operation (Illardi, 2010). Thus, by way of the intelligence that supports a boost in terrorists' confidence, these perceptions are sufficient enough to motivate them to carry out an attack and to persist in the struggle towards their dream.

Collating a Collection: Terrorists' Intelligence

As noted, there is an appreciable lacuna at the nexus of the intelligence and terrorism disciplines; in the academic field of intelligence, exclusive inquiry into NSAs' intelligence has yet to gain much traction, whereas in counterinsurgency literature, "insurgents tend to be treated as something that intelligence acts upon but rarely, if ever, treated as intelligence actors in their own right" (Strachan-Morris, 2019a, p. 980). In the (counter)terrorism discipline, the situation is even more sparse, more oft discussing the characteristics of state intelligence and when and why these organisations and their abilities "fail" in the context of terrorist threats and acts (Wagner, 2007, p. 48; Kerstetter, 1979, p. 111). While an immature subject matter in the academic discourse, some initial case research on VNSAs has been conducted in the form of isolated, actor-specific case studies or hinted at in other studies of terrorists' operational activities. Actors of these case studies include the North Vietnamese in the First (Goshcha, 2007) and Second (Strachan-Morris, 2019b) Indochina Wars, the Maoists in Nepal (Jackson, 2019), the FARC in Colombia (Gentry & Spencer, 2010), the PIRA in Northern Ireland during the Troubles (Illardi, 2010; Illardi, 2010; Bramford, 2005), the Greek Communists during the Greek Civil War (Tantalakis, 2019), the LTTE in Sri Lanka (Joshi, 1996; Thiranagama, 2010), and al-Qaeda (Kenney, 2008; Illardi, 2009; Illardi, 2008). Though disparate circumstances, woven together, these pieces portray a picture of VNSAs' intelligence that can be innovative, sophisticated, and professional, yet can also be devoid of long-term strategy, riddled with counterintelligence paranoia, and crippled by disconnect between top leadership and low-level operatives. A review of these pieces sheds light on some of the similarities and differences between VNSAs' intelligence capabilities and capacities.

Structurally, some groups, such as the PIRA, LTTE, al-Qaeda, and the Maoists demonstrate intricate, formalised intelligence organigrams (O'Brien, 2008; Bramford, 2005; Jackson, 2019; Richards, 2014), compartmentalising labour into divisions or departments such as intelligence, internal security/counterintelligence, reconnaissance and data collection, and special operations. In other groups, such as various Euro-Marxist groups in the 1970s-1980s, these activities were self-contained and self-directed within a small group (O'Brien, 2008). The structural organisation has implications for data collection and amongst many of the groups, HUMINT and OSINT are the overwhelmingly primary forums of intelligence gathering (Jackson, 2019; Monaghan, 2019)—an understandable conclusion as these methods, compared to techniques such as GEOINT or SIGINT, are more accessible from financial, personnel, or maintenance costs perspectives and due to the lower threshold of technical expertise required. Additional studies also concur that although the Internet appears attractive as a trove of information from which one could study their adversary or surveil targets, it has little been exploited as such, as there is nothing comparable to the nuances picked up through first-hand observation; indeed, rather than used for surveillance, during the planning and preparing of attacks, the Internet is more frequently a means to communicate ideological knowledge (United Nations Office on Drugs and Crime, 2012; Holbrook, 2015) and exchange generalised techne (Kenney, 2010). Thus, while the Internet could offer some benefits, recognising attacks are situational and environment-specific, for the terrorist, prioritising on-site surveillance, HUMINT-based intelligence, and know-how acquired through direct exposure or experience reign supreme. Additionally benefiting the terrorist, HUMINT informers need not possess exclusive access to "specific sensitive information," but can routinely pass on more easily observable data (Magee, 2010, p. 513). HUMINT thus, as the oldest intelligence collection discipline, remains the optimal choice from cost, access, and effectiveness points of view. As a contrast, the FARC has acquired and maintained some commercial software for imagery intelligence and "recognises the value of open source information (OSINT) but uses it little" (Gentry, 2016, p. 476).

Building from their gathered intelligence, some groups—such as the Maoists and FARC—demonstrate an understanding of the importance of analysis; however, they possess a "limited understanding of intelligence analytical tradecraft" (Gentry, 2016) by demonstrating favour for military-related, tactical-level information or by employing operatives to perform both activities of data collection and analysis, who then transmit the refined intelligence to a second analytical capability (Jackson, 2019). These bear similarity to the notion of "intelligence politicisation," which describes the distortion of intelligence due to ideological biases and the "tendency for intelligence assessments to be formulated to complement prevailing orthodoxies and predetermined policies" (Jackson, 2010). One intriguing example of this, common between actors including the FARC, Hezbollah, Hamas, and the IRA, is the influence of ideology and/or the dream in biasing or predisposing the VNSA's analytical processes. Hezbollah and Hamas offer an example of how biases and misperception lead to intelligence fallacy. Perceiving the structural transparency of the liberal state to be synonymous with wider transparency, predictability, and certainty, Hamas and Hezbollah developed false impressions and inaccurate intelligence assessments of their adversary, Israel (Bitton, 2019). Confident in their narrowed intelligence assessments and understanding of how Israel would respond to attacks led these groups to mis-calibrate the threshold of violence toleration, much to both groups' detriment, as evidenced in the conflict continuing to the present day (Bitton, 2019). Again on the cross-over of intelligence capabilities and confidence, an interesting takeaway is from the North Vietnamese, who concealed their operational- and strategic– level intelligence weaknesses by maintaining a lengthy struggle grounded in tactical intelligence; it was when their intelligence doctrine and "infrastructure synchronized with the [*sic*] conventional capabilities" that they were able to win the Vietnam war (Strachan-Morris, 2019a; Strachan-Morris, 2019b).

Counterintelligence formalities and practices differ between groups; for instance, some groups are known to have attempted or been successful exercising counterintelligence through the infiltration of their adversary's structure or commands, as known in the cases of Hezbollah and al-Qaeda (Harber, 2009, p. 223). Other groups routinely change their names (Smith, et al., 2017, p. 63) to avoid detection, while others decentralise their structures as a safeguard. The latter was evident in the case of the IRA in the 1970s, an organisation adept in learning from their problems with police penetration in the late 1800s, and accordingly decentralised (Harmon, 2000, p. 2) and engrained counterintelligence practices with rigour, as detailed in the lengthy pages of their manual, the Green Book (Irish Republican Army (IRA), 1965), which reiterates the importance and conduct of counterintelligence practices. Nonetheless, similar among these groups is the recognition that regardless of how it is executed, counterintelligence is essential, to an extreme that even suspicions of infiltration can end abruptly and mercilessly with ex-communication or execution (Jackson, 2019). For the PIRA, counterintelligence was also perceived as an integral component to sustaining group and member confidence as the "means to engage the British with confidence, [and be] reasonably secure in the knowledge that the enemy's security forces were not lying in wait or had covertly interfered with the IRA's equipment or explosives" (Illardi, 2010, p. 2).

These studies capture important insight on VNSA intelligence; however, written as independent studies, they have yet to propose much towards the development of collective VNSA-intelligence theories. The present study seeks to bridge this gap by synthesising information from three case studies, coupled with information known about the other groups. Additionally, taking into account *confidence*—an attribute of VNSA intelligence and commitment to the dream that is salient throughout the above cases—the current research offers a framework that underscores the role of intelligence as a foundational, operational base and confidence-building mechanism from which VNSAs can compete with their state opponents in staging attacks.

Thinking on Theory: An Analysis of Actors

In terms of encompassing theory on VNSA intelligence, in a self-described "preliminary general analysis of a largely neglected aspect of unconventional conflict," conflict historian and terrorism expert J. Bowyer Bell's "The Armed Struggle and Underground Intelligence: An Overview" encapsulates years of formal and informal interviews with VNSAs to detail an account of the VNSA's perception of their goals and utilisation of intelligence to support actions taken in pursuit of their dreams (Bell, 1994). From the onset, Bell stresses that the VNSA's need for intelligence is situational and circumstance-specific; for this reason, what outsiders, including scholars, might strive to conclude as an overarching strategy might be unnecessary or unapparent for the groups themselves (1994). This also complicates the ability to compare groups or pinpoint a precise theory on actors' strategies for intelligence. Prioritised by these individuals is the mandate for tactical or operational level intelligence, a pursuit to acquire "information about the real world, the enemy, its own members, and others. There will be a persistent rebel demand for technical details, tactical intelligence, and counterintelligence but rarely a demand for strategic intelligence" (Bell, 1994, p. 118). Bell elaborates that engagement in the struggle against an adversary *is* the VNSA's strategy; belief in the dream's ultimate success configures the VNSA's reality, such that some operations perceived by external observers to be 'unsuccessful' might still contribute to the rebel struggle and provide the fuel to persist. Furthermore, for some actors, the dream has already been achieved in the future; actions that occur today, including attacks, are preliminary objectives that align with and progress the vision of the future. At the tactical level, therefore, intelligence is the "mundane" details for specific missions, which too, are filtered through the lens of the dream to the extent contradictory or disconfirming evidence is ignored or rejected, regardless of potential detriment to the VNSA, the operation, and/or their cause (Bell, 1994).

One of the first, if not the only, formalised attempts to develop theory on NSA intelligence by comparing multiple groups is former CIA intelligence analyst John A. Gentry's "Toward a Theory of Non-State Actors' Intelligence" (Gentry, 2016). In this paper, Gentry examines the intelligence activities, products, and organisations of non-state actors—the KLA, the FARC, al-Qaeda, and various NGOs—in comparison with nation-states, expounding upon two commonly regarded intelligence activities of state entities—counterintelligence and covert action—justifying his rationale on the basis "non-state actors use these elements of intelligence in very different ways than do states" (Gentry, 2016, p. 467). These and other conclusions are summarised in Fig. 4.

Fig. 4

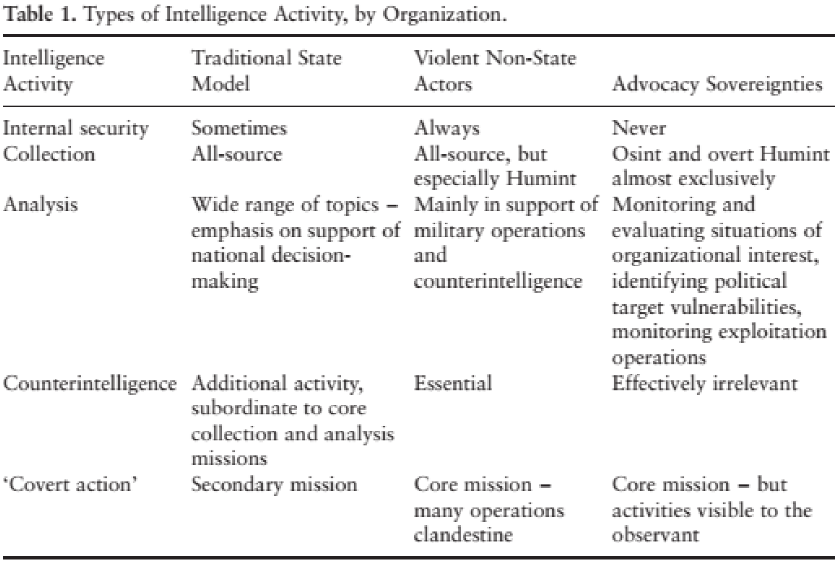


Table 1. Types of Intelligence Activity, by Organization.

Intelligence Activity	Traditional State Model	Violent Non-State Actors	Advocacy Sovereignties
Internal security	Sometimes	Always	Never
Collection	All-source	All-source, but especially Humint	Osint and overt Humint almost exclusively
Analysis	Wide range of topics – emphasis on support of national decision-making	Mainly in support of military operations and counterintelligence	Monitoring and evaluating situations of organizational interest, identifying political target vulnerabilities, monitoring exploitation operations
Counterintelligence	Additional activity, subordinate to core collection and analysis missions	Essential	Effectively irrelevant
'Covert action'	Secondary mission	Core mission – many operations clandestine	Core mission – but activities visible to the observant

Source: *Gentry, J. A., 2016. Toward a Theory of Non-State Actors' Intelligence. Intelligence and National Security, 4, pp. 465-489.*

Gentry defines internal security as "intelligence support to police and other agencies dedicated to protecting governments and citizens from domestic threats of violence" (2016, p. 468). Regarding VNSAs, he contends this function is most apparent in "Successful insurgent groups that become semi-state actors that control appreciable amounts of territory for extended periods" (Gentry, 2016, p. 468). Thus, for Gentry, internal security arises when a VNSA has both territory and prolonged authority over a population, whom they have almost a duty to protect. Bell offers an alternative conclusion, as he asserts for many VNSAs—not limited to the 'successful'—internal security is a strategic means to preserve their faith; concomitant with counterintelligence, it is the duty of each member to remain alert, involved, and suspicious (1994, p. 137). Additionally, despite rigorous counterintelligence practices, leaders of a violent, non-state organisation remain "dubious" (Bell, 1994, p. 135) about internal security, plagued by their paranoia of conspiracy, fear of infiltration, and fear of the power of the state.

While both authors underscore counterintelligence practices are paramount, Bell's and Gentry's explanations of the counterintelligence purpose differ by a slight nuance. Gentry asserts the vitality of counterintelligence as a determinant for the VNSA's survival and writes

"CI is the means by which insurgent groups preserve the faith of their members by ruthlessly enforcing ideological discipline" (Gentry, 2016, p. 473). Bell, on the other hand, asserts a VNSA performs counterintelligence activities "on the basis of limited intelligence data [and] often kills his own first and most passionately, for his own endanger the dream" (Bell, 1994, p. 130). With this viewpoint, the adversary within—the betrayer or apostate—might thus be only a step removed from the supreme enemy, as both parties threaten the achievement and stability of the dream. The subtle nuance lies in the perceived purpose and direct target of counterintelligence. For Gentry, this central purpose of counterintelligence is to target members of the faith, for whom ideological enforcement is a means. Contrastingly for Bell, the central purpose of counterintelligence is to preserve the dream, for which the expulsion, purge, and murder of members is the means. The present study contends both are plausible, perceiving counterintelligence as a technique for terrorists to safeguard their dream and reinforce the ideological faith of their members by exercising methods that threaten harm to or punish those who jeopardise the dream; execution and other dramatic acts are justified to illustrate to other members the consequences of lost faith or treachery.

Bell and Gentry agree that intelligence collection for VNSAs is all-source based and driven predominantly from requirements for operational or attack pursuits; therefore, strategic-level intelligence is rarely in demand (Bell, 1994, p. 119) or relatively weak (Gentry, 2016). Indeed, the lack of 'strategic' intelligence can lead groups to make impulsive decisions or decisions that might later harm their overall cause. While reasonable, such claims are susceptible victims of mirror imaging bias—the imposition of an observer's own views and definitions of 'strategic,' rather than the subject's perspectives. Acknowledging such, this author identifies another point raised, but not fully explored by Bell. This point states, "Tactics become strategy and are focused on persistence and, if possible, escalation through operations" (Bell, 1994). From here, this author contends first that the failure or lack of strategic intelligence exhibited by terrorists might instead be explained by a form of mirror imaging bias in the observer's failure or lack of understanding of what constitutes 'strategic intelligence' for terrorists. For terrorists, facing an asymmetric competition with an adversary, such as a state, who has arguably vaster material resources or even a monopoly over the use of (legitimate) violence (Weber, 2015), strategic intelligence is that which facilitates and supports the ability for the terrorist to persist in their struggle. This said, the strategy *is* the dream, achieved through persistence, and persistence takes the form of attacks; strategic intelligence, therefore, is intelligence that conforms to fit the dream, contributes to the actor's perceivable understanding of their adversary, and affords them the necessary confidence to persist, act, and attack in light of the dream. This also explains Bell's observation that the rebel's "analytical capacity is minimal, and even operational planning is often flawed: no one plans for failure, and often no one even plans for tomorrow" (1994, p. 119). In fact, there is no need to develop plans for failure because in the eyes of the terrorist, again enraptured by the vision of the future, the dream has been achieved; their acts are merely duties in the progression of this dream.

One Step Further: Exploiting the Analysis

The current study thus seeks to expound upon Bell's original work and delve deeper into topics from Gentry's analysis and conclusions, but also acquire a deeper understanding and appreciation for what this author perceives as an 'intelligence competition' between terrorists and their state opponents. By pursuing intelligence—information, methods, and functions—the terrorist is assured of their assessment and understanding of themselves and their adversary. Such reassurance helps the terrorist believe they have a degree of control or predictability over their adversary or a target. Minimising their vulnerabilities, risks, and that which might work against their pursuits, the terrorist is eager to fulfil their dream and convinced in their ability to execute it. These observations thus produce the following supposition:

> *Terrorists operationalise intelligence to develop an understanding of the vulnerabilities and capabilities of themselves and their adversaries; these form a poised understanding, which in turn allows the terrorist to feel more in control and thus more confident when planning for, preparing, and executing attacks.*

This study uses three case studies to determine the tactical and operational intelligence—the *what*—terrorists seek when planning, preparing for, and conducting attacks; the intelligence and intelligence methods and functions—the *how*—they utilise or undertake to inform or support their operations; and the purposes intelligence serves—the *why*—in facilitating their ability to engage with their state adversaries. This research then applies these to evaluate the robustness and explanatory power of the IC and TAC pertaining to terrorists' intelligence endeavours. The three chosen operations needed to fulfil the requirement of being a 'complex, coordinated attack,' defined as

> …a violent assault or series of assaults that employs one or more types of weapons, intends to injure or kill large numbers of people, and meets the following two criteria:

1. Criterion 1: The attack is multi-phased or takes place at multiple sites, or both
2. Criterion 2: The attack must take place within geographic and temporal circumstances that result in unusual strain on command, information sharing/situational awareness, and/or resource allocation (Ryan, 2018, pp. 1-2).

Owing to the number of resources (e.g. personnel, matériel) involved and the multi-phase or multi-locational element, CCAs are judged to require a sophisticated degree of forethought, preparation, and organisation beyond that of an attack by a sole actor or at a single site; for this reason, it is argued in these attacks, it might be more apparent to detect the presence or absence of terrorists' intelligence activities and the intelligence competition between terrorists, state intelligence, and law enforcement prior to and during the attack. To be assured of the ability to evaluate a terrorist organisation's intelligence activities, it was further necessary that the perpetrating group claimed responsibility for the selected attack. Lastly, to maintain some similarity, two points are considered. First, the case study groups selected must all have a broadly similar ideology. While the explicit end goals and tactics differ, maintaining a common thematic dream between the groups allows this research to avoid too much detail analysing the origin and nature of the dreams themselves, which is outside the present scope. Second, in each of the three cases, attacks needed to be claimed or recognised to be engineered and directed with the engagement of parent organisation leadership; attacks that are not *directed*, but rather *inspired* by a formidable organisation or leader might yield different insights and is encouraged as a direction for further research.

With these requirements set, the case studies chosen for the present study are the U.S. embassy bombings in Kenya and Tanzania perpetrated by al-Qaeda (1998), the Paris attacks perpetrated by Daesh (2015), and the Westgate Mall attack perpetrated by al-Shabaab (2013). The former two cases are primary, owing to a higher degree of academic and practitioner inquiry, which translates to a comparably wider breadth of information and knowledge about these groups' structures; capabilities, operations, and *modus operandi*; and spread of global activities and operations. The following case studies are structured to provide a descriptive summary of these actors' intelligence capabilities and activities relating to intelligence collection, analysis, counterintelligence, learning, and feedback. This is accomplished by triangulating data sourced for these studies, including terrorists' publications, court documentation, judiciary reviews and investigations, media reports and investigative journalism, scholarly studies, and books. While 'confidence' might not be clearly articulated, measured, or referred to in the parlance of these sources, this researcher asserts it is nevertheless possible to extract evidence of both terrorists' intelligence endeavours and proxies of confidence, based on their actions and behaviours (or lack thereof) before and during an attack. Understandably, the best way to understand the *hows* and *whys* of terrorists' intelligence is directly from the source, the terrorists themselves. However, gaining first-hand access, such as through interviews, is near-impossible, as groups often operate "underground" (Bell, 1994), maintain strict vetting and security procedures (O'Brien, 2008; Suc, 2017a), and preserve pervasive counterintelligence cultures. Groups additionally often have close-knit familial or friendly ties (Harmon, 2000, p. 2) deeply rooted in established trust (Harber, 2009, p. 229). Indeed, when they fail to exercise these precautions, groups can find themselves infiltrated, their plans revealed, and members arrested, such was the outcome befalling an Islamist cell operating in Barcelona, which, driven by a "proselytising desire" to attract new members, exercised lax security protocols, enabling police to penetrate and expose the cell (Torres-Soriano, 2019). Even defectors, fearing their own safety and wellbeing, are likely reluctant to speak. Case studies are thus beneficial where there is an absence of accepted theory, and by way of a dually abductive and inductive approach, fosters the development of tentative, theoretical models (Gill, 2018, p. 574). The case studies are consequently structured to provide an evaluation of broad, organisation-wide intelligence activities that support an organisation and attack operations as well as an evaluation of intelligence activities specific to the three aforementioned attacks.

Lastly of note, while a clear example of a complex, coordinated attack, the 9/11 attacks perpetrated by al-Qaeda were not chosen by this researcher, as the role of intelligence in this operation has been sufficiently explored by other authors (see Illardi, 2008; Illardi, 2009).

Case-by-Case

Al-Qaeda

Al-Qaeda demonstrated a clear use of intelligence to support the operation's planners' confidence and sense of control as they developed a meticulous plan for U.S. embassy bombings in Nairobi and Dar es Salaam in 1998. During the operation, due to unforeseen circumstances, the execution cell's (henceforth "operatives") level of confidence in their ability to fulfil their duties diminished, and because they lacked sufficient *capability* that would allow them to adapt, the attack was not as successful as al-Qaeda intended. This attack evidences that al-Qaeda's understanding of self is limited and its operatives are the most volatile part of an operation. Indeed, operatives' *competencies* must be well assessed prior to an attack, for misjudgements between expectations and reality can become an organisational vulnerability and threaten the success of an operation. In the embassy bombings, al-Qaeda honed a strong ability to conduct intelligence activities in the interest of knowing its enemy and target to support leaders’ and planners’ confidence in the ability to attack and achieve operational success. Contrasting, the operationalisation of intelligence to know thyself was suboptimal; indeed, in the collection and analysis of its operatives' competencies, the group overestimated these capabilities and enlisted the wrong candidates for the attack. This amounted to blunders during the attack and the failure to achieve certain key objectives.

Understanding bombings in August 1998 requires going back to December 1993, the earliest known date when al-Qaeda members deployed to Kenya (Kean & Hamilton, 2004, p. 68). At this time, and for the next several years that would follow, the collection and analysis of intelligence was vital; indeed, the preeminent duty of members in the region was to establish a foothold in the community—renting property, landing jobs, establishing local businesses, and joining religious, social, and cultural centres (Kean & Hamilton, 2004, p. 69)—through which members could develop an acute understanding of the environment by engaging in the systematic and indiscriminate collection of intelligence on a range of viable targets.

This model al-Qaeda employs—"know thy enemy” (al-Qaeda, n.d., p. 85)—is similar to that of a multinational business interested in entering new markets and a strategy that bin Laden, as a businessman himself, would know well. Indeed, al-Qaeda’s intelligence collectors positioned around the world routinely collect intelligence about their environment’s political and social climates and attractive attack targets to gain a well-informed appreciation of current and future adversarial *vulnerabilities* (to be exploited) and *capabilities* (to be negated or minimised); as put forth in the al-Qaeda-affiliated manual *Declaration of Jihad against the Country’s Tyrants*, these efforts serve as the basis for the design of “good-quality and secure plans” (al-Qaeda, n.d., p. 84). Intelligence collection is both active and passive; the former implying top leadership has pre-identified specific targets for further surveillance whereas the latter entails the solicitation of information on a wider array of possibilities. Intelligence sought intends to provide al-Qaeda with knowledge and an understanding of potential targets and environments, and from these understandings, to choose an opportunity suitable to the organisation’s objectives. This intelligence is exceptional in volume and a precise degree of detail, both of which al-Qaeda perceived as affording the organisation with clearer perceptions of measuring risk (Illardi, 2008, p. 1090), greater certainty and confidence in judgement, and an illusion of near-total control over the success of attacks. Additionally, as the intelligence is current and locally sourced, al-Qaeda leadership has greater reassurance in the timeliness and accuracy of their understandings, even if final decision-making occurs at a spatial distance.

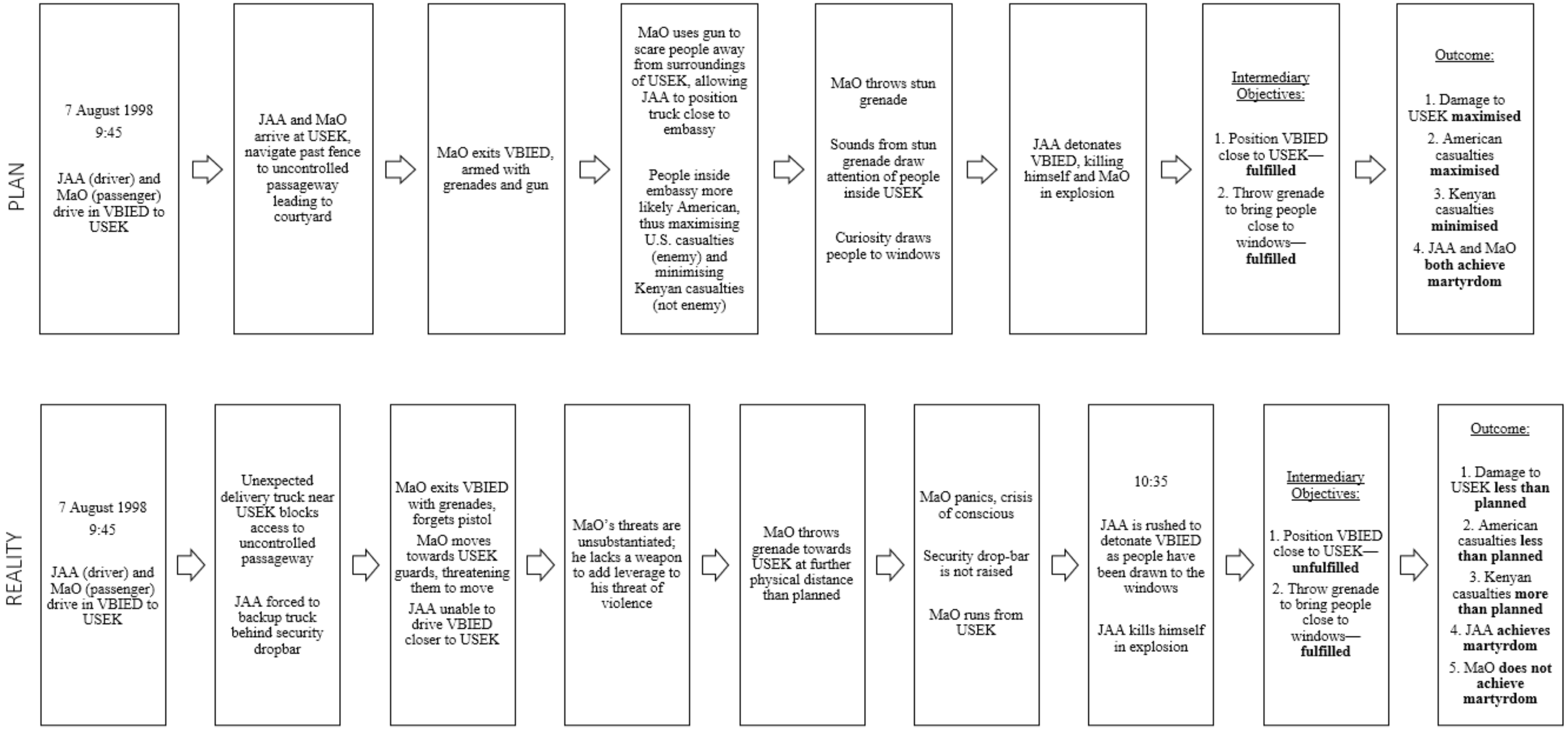
Intelligence collection efforts from 1993-1996 were unspecified, as al-Qaeda had yet to develop a clear picture of the Kenyan market's suitability for attacks. The fact these efforts were led by Ali Mohammed, a former Egyptian army officer who previously lived in the U.S. and served as a U.S. military instructor, highlights a first instance of the intelligence competition and al-Qaeda's endeavours to intimately know and learn from within its enemy. While serving at the Fort Bragg U.S. military base, Mohammed was able to obtain, translate, and distribute U.S. military field manuals to al-Qaeda (Kenney, 2008, p. 141), enabling the organisation to learn from its enemy's training and techniques. Under the command of Mohammed, al-Qaeda members deployed to east Africa for intelligence collection were also instructed to surveil possible targets of strategic and operational interest in particular; these included the U.S. embassy, the U.S. AID building, the U.S. Agricultural Office, the French Cultural Centre, and the French embassy (Illardi, 2008, p. 1079). From the collection of intelligence, members drafted surveillance "casing reports" (Kean & Hamilton, 2004, pp. 68-69; Rabasa, 2006)—voluminous, written assessments of their findings replete with photographs, diagrams, and other schema. The breadth of information sought and depth in the level of detail was encompassing and obsessive—to the extent some information was superfluous or carried little utility (Illardi, 2008, p. 1090). Again, this evidences how al-Qaeda members perceive the uses for and value of intelligence to feel certain and confident in their understanding of their enemy and to minimise the threat of uncertainty or surprise arising during attacks. By January 1994, these casing reports were then presented to top leadership for review (Kean & Hamilton, 2004, p. 68). This analysis stage evaluated the plausibility of each site as a target with the intent to discover the enemy's vulnerabilities, which could then be exploited by the organisation as attack opportunities. Seeing a vulnerability in an uncontrolled passageway near the Kenyan U.S. embassy, bin Laden opted for this target, perceiving it as a strategic site for the placement of a VBIED (Bernarding & Schuster, 2005).

With targets chosen,—the U.S. embassies in Kenya and Tanzania— each operation would consist of two cells: the planners and the operatives. In the pre-operational phases of the attack, the planners were well informed and operationalised a high volume of intelligence to devise precise tactical plans (Bernarding & Schuster, 2005, p. 14). The operatives—those who would execute the attack—were neither selected nor briefed on their assignment until late in the pre-operational phases of the attack. Indeed, for the Kenyan operation, one of the suicide bombers, Mohammed Rashed Daoud al-Owhali, did not arrive in Nairobi until 2 August 1998 (Bernarding & Schuster, 2005, p. 60), five days before the attack. For the Tanzanian operation, through early 1998, al-Qaeda was still seeking attack operatives (Bernarding & Schuster, 2005, p. 15), implying the decision to target the Tanzanian embassy simultaneously occurred after selection of the Kenyan embassy and that the Tanzanian operation would be planned for in less time.

This segregation of members and their degree of operational cognizance is part of a wider strategic intelligence effort to *know thyself*: that vulnerabilities can be minimised and capabilities developed or exploited. Interestingly, this strategy prioritises prolific counterintelligence measures intended to minimise threats from infiltration and exposure, overshadowing the fact the greatest threat to al-Qaeda's operations is the miscalculation of operatives' competence. As demonstrated in the bombings, al-Qaeda's counterintelligence doctrine included limiting the number of people involved in the pre-operational phases, informing its members on a need-to-know basis, and segregating cells based on responsibility (i.e. planning, logistics, operations, intelligence collection); with these practices, leadership felt assured their greatest vulnerabilities—the likelihood of infiltration and/or the exposure of the operation through deliberate or accidental tip-offs to law enforcement—are minimised. With strong counterintelligence, al-Qaeda believed in its control over internal security and operational success, judging its planners and operatives to both be highly *competent. Competence* here refers to the collective of mental intellect, physical abilities, skill and craft, and confidence and the ability to use these qualities to do something successfully and efficiently. Planner competencies include managerial and organisational expertise; therefore, to fulfil their function of *planning* an attack, these actors have detailed knowledge of the whole operation. But while recognising the need to ensure each actor maximises his/her function (al-Qaeda, n.d., p. 76), al-Qaeda's intelligence practices suffered to understand operatives' *competencies* and match operatives with suitable attack opportunities (al-Qaeda, n.d., p. 76); it was the failure to exercise adequate intelligence activities to understand its operatives' competencies that led to failures in the bombings. Operatives' competencies, in contrast with planners', are rooted in loyalty and obedience to operate the attack to fulfil their function, and need not know all the details of the operation. As an operative becomes curious, seeking to know more information about the operation, there is a risk they begin to question or doubt their role as operatives, decreasing their confidence levels. Accurately evaluating operatives' competencies and calibrating the levels of confidence is key to the success of an operation. Indeed, if an operative's competence is lower than was expected during planning, this can trigger a higher error margin, given that objectives will not be attained in an adequate manner. Similarly, if their intelligence competence, in reality, is higher than was expected during planning, this can trigger a higher awareness margin, given that objectives will be cast with doubt, hesitation, and reluctance. To stabilise the operative's confidence, it is necessary to calibrate a balance in helping the operative, informing a sense of importance, providing information, lifting morale, and revitalising confidence, while not allowing the operative to lose faith and deviate from his/her intended purpose in the operation.

In the embassy attacks, al-Qaeda's operationalisation of intelligence engendered an understanding of the enemy—the embassies' vulnerabilities—that allowed them to establish a ground truth, from which a plan for an attack could be drafted. Further, intelligence boosted the planners' confidence in their plans and the degree of control they would possess over the operation's success. Yet, miscalculating understanding of self—their operatives' competencies—resulted in an attack less successful than intended. The graphic below illustrates the attacks against the U.S. embassy in Kenya as envisioned by the planners and as executed by the operatives (Fig. 5).

Fig. 5


PLAN
7 August 1998 9:45 JAA (driver) and MaO (passenger) drive in VBIED to USEK
JAA and MaO arrive at USEK, navigate past fence to uncontrolled passageway leading to courtyard
MaO exits VBIED, armed with grenades and gun
MaO uses gun to scare people away from surroundings of USEK, allowing JAA to position truck close to embassy
People inside embassy more likely American, thus maximising U.S. casualties (enemy) and minimising Kenyan casualties (not enemy)
MaO throws stun grenade
Sounds from stun grenade draw attention of people inside USEK
Curiosity draws people to windows
JAA detonates VBIED, killing himself and MaO in explosion
Intermediary Objectives:
1. Position VBIED close to USEK—**fulfilled**
2. Throw grenade to bring people close to windows—**fulfilled**
Outcome:
1. Damage to USEK **maximised**
2. American casualties **maximised**
3. Kenyan casualties **minimised**
4. JAA and MaO **both achieve martyrdom**
REALITY
7 August 1998 9:45 JAA (driver) and MaO (passenger) drive in VBIED to USEK
Unexpected delivery truck near USEK blocks access to uncontrolled passageway
JAA forced to backup truck behind security dropbar
MaO exits VBIED with grenades, forgets pistol
MaO moves towards USEK guards, threatening them to move
JAA unable to drive VBIED closer to USEK
MaO's threats are unsubstantiated; he lacks a weapon to add leverage to his threat of violence
MaO throws grenade towards USEK at further physical distance than planned
MaO panics, crisis of conscious
Security drop-bar is not raised
MaO runs from USEK
10:35
JAA is rushed to detonate VBIED as people have been drawn to the windows
JAA kills himself in explosion
Intermediary Objectives:
1. Position VBIED close to USEK—**unfulfilled**
2. Throw grenade to bring people close to windows—**fulfilled**
Outcome:
1. Damage to USEK **less than planned**
2. American casualties **less than planned**
3. Kenyan casualties **more than planned**
4. JAA **achieves martyrdom**
5. MaO **does not achieve martyrdom**

Key
JAA: Jihad Ali Azzam – Suicide Bomber; Driver
MaO: Mohamed al-Owhali – Suicide Bomber
VBIED: vehicular-based improvised explosive device
USEK: U.S. embassy in Nairobi, Kenya

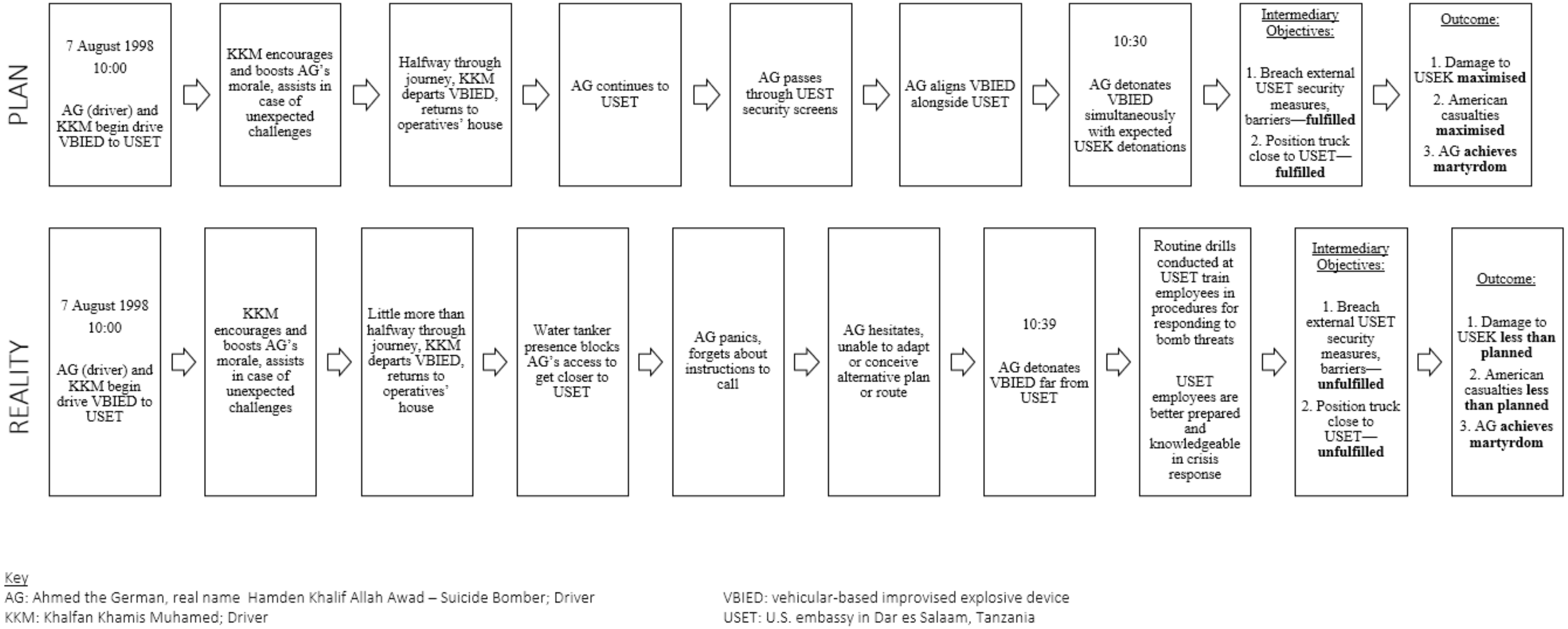
Source*: Author. The Attacks on the Kenyan U.S. Embassy as Planned and Executed*

On the day of the attacks, an unexpected delivery truck beside the embassy blocked the uncontrolled passageway to the embassy and forced operatives Azzam and al-Owhali to back up their VBIED behind a guarded security drop bar (Crowe, et al., 1999). This anomaly permutated the planners' painstakingly developed ground truth expectations and the obstruction resulted in a vicious cycle of lowering confidence and error. To begin, the truck's presence—sparking operational uncertainty—lowered the confidence of the operatives, in particular al-Owhali, who, as a result, mistakenly left his pistol in the truck (Bernarding & Schuster, 2005, p. 61). According to the plan, al-Owhali was meant to use the pistol to clear people from the area (Ressa, 2003, p. 174) to both position the truck closer to the embassy (Crowe, et al., 1999) and to minimise the number of civilian Kenyan casualties (Federal Bureau of Investigation (FBI), 1998), as al-Qaeda held Kenyans were not the enemy, but unfortunate collateral in the attempt to strike its chief enemy—the U.S. As a result of the anomaly, al-Owhali's confidence faltered and his *incapability* prevented him from recovering, readjusting, and retrieving the pistol from the truck to continue the operation as planned. Without the gun to add legitimacy in his threats for the guard to lift the security drop-bar, al-Owhali panicked, throwing his grenade from a distance (United States District Court Southern District of New York, 1998). With this act people would be drawn to the windows by the calamity of the grenade (Wright, 2006)—as intended; however, the truck was still at an unfavourable spatial distance from the embassy. To maximise U.S. casualties from the people drawn to the windows, the thrown grenade triggered an imperative for Azzam to detonate the VBIED quickly, despite the distance. Al-Owhali's failure to carry out his primary duty—making access for the positioning of the VBIED—his capability shortcomings, and diminished confidence in self prompted a crisis of conscience and confidence in the mission. He regarded due to his failure, that by remaining near the embassy, he would be committing *suicide*, not achieving *martyrdom* (Wright, 2006), and, as a result, fled from the site and was not killed when Azzam detonated the VBIED (United States District Court Southern District of New York, 1998). As an additional interesting note, because of the operative's rigid adherence to continue the attack as planned—an *incapability* to adapt—the operatives failed to realise that had they rerouted the VBIED along another street for approximately 50 feet, the vehicle would have been positioned closer to the embassy than it was at the barrier, resulting in equal, if not more, damage than envisioned (Crowe, et al., 1999).

In Dar es Salaam, Tanzania, likely owing to the fact the operation was conceived in less time than the Kenyan operation, the attack's planners failed to accurately gauge both their understanding of their operative's competency (knowledge of self vulnerability) and to collect sufficient intelligence to support their understanding of the embassy's security protocols and procedures (knowledge of adversary capability). While the attack did manifest physical damage, the effect was marginal compared to the organiser's expectations.

Much like the bombings in Nairobi, during the Tanzania attack (see Fig. 6), a water tanker present near the U.S. embassy's perimeter prevented operative Hamden Khalif Allah Awad (also known as Ahmed the German) from positioning his VBIED closer to the embassy, rattling his confidence. Lacking the necessary competence to adapt and regain confidence resulted in an only partially successful attack (United States District Court Southern District of New York, 1998) (Crowe, et al., 1999). For the drive to the embassy, Awad was joined by planner Khalfan Khamis Muhamed, who would accompany him for more than half of the journey, before departing the vehicle to return to the operatives' house to clear evidence (Bernarding & Schuster, 2005). Muhamed's presence served not only to assist in the event something went wrong prior to the execution of the attack, but more importantly to encourage and boost Awad's morale as a valuable, *competent* operative. It is argued had the attack's organisers chosen a more *competent* operative or felt more assured in their judgement of Awad's ability, they would not have perceived the need for Muhamed's support. Awad's confidence following Muhamed's departure faltered, and the aberration of the water tanker challenged Awad with a dilemma: he could either adhere to the plan and detonate from a distance—prioritising the attacks' near-simultaneity and achieving martyrdom—or adapt to the new circumstances, deviating further from the plan by repositioning the VBIED at a different location. Awad opted for the former, detonating the VBIED approximately 35 feet from the compound's outer wall (Crowe, et al., 1999); while causing significant damage, unlike the explosion at the Kenyan embassy, the Tanzanian embassy did not collapse. This attack echoes the same failures suffered by the Kenyan operatives, whose competencies were overestimated during the planning and preparation for the attack. Indeed, lacking sufficient competence, Awad failed to adjust to the changed circumstances and find a way to achieve all the attack's intended objectives—position the VBIED close to the embassy, maximise U.S. casualties, maximise damage, and achieve martyrdom. This is further evidenced in Awad's failure to reach out to the planning team for assistance, despite being left with a cell phone and explicit instructions to call if there were any problems with the mission (Bernarding & Schuster, 2005, p. 61).

Fig. 6


PLAN
7 August 1998 10:00 AG (driver) and KKM begin drive VBIED to USET
KKM encourages and boosts AG's morale, assists in case of unexpected challenges
Halfway through journey, KKM departs VBIED, returns to operatives' house
AG continues to USET
AG passes through UEST security screens
AG aligns VBIED alongside USET
10:30 AG detonates VBIED simultaneously with expected USEK detonations
Intermediary Objectives: 1. Breach external USET security measures, barriers—fulfilled 2. Position truck close to USET—fulfilled
Outcome: 1. Damage to USEK maximised 2. American casualties maximised 3. AG achieves martyrdom
REALITY
7 August 1998 10:00 AG (driver) and KKM begin drive VBIED to USET
KKM encourages and boosts AG's morale, assists in case of unexpected challenges
Little more than halfway through journey, KKM departs VBIED, returns to operatives' house
Water tanker presence blocks AG's access to get closer to USET
AG panics, forgets about instructions to call
AG hesitates, unable to adapt or conceive alternative plan or route
10:39 AG detonates VBIED far from USET
Routine drills conducted at USET train employees in procedures for responding to bomb threats USET employees are better prepared and knowledgeable in crisis response
Intermediary Objectives: 1. Breach external USET security measures, barriers—unfulfilled 2. Position truck close to USET—unfulfilled
Outcome: 1. Damage to USEK less than planned 2. American casualties less than planned 3. AG achieves martyrdom
Key
AG: Ahmed the German, real name Hamden Khalif Allah Awad – Suicide Bomber; Driver
KKM: Khalfan Khamis Muhamed; Driver
VBIED: vehicular-based improvised explosive device
USET: U.S. embassy in Dar es Salaam, Tanzania

Source*: Author. The Attacks on the Tanzanian U.S. Embassy as Planned and Executed*

The effects of the attack on the U.S. embassy in Tanzania were additionally mitigated by crisis response policies and procedures of the embassy, which included weekly routine evacuation drills (Crowe, et al., 1999). While these drills were intended for responding to package bomb threats (Bernarding & Schuster, 2005), they nonetheless proved effective and supported employees' abilities to remain cognizant and resilient in their response to the attacks, saving lives.

The intended outcomes of the attacks were to maximise the damage to the United States, both in terms of infrastructural and human casualties, minimise the effects to Kenya, and reach fellow Muslims and spread the message of *jihad*—'holy war'—and martyrdom for the dream, as evidenced in the claims of responsibility issued by an al-Qaeda office in London (United States Committee on Foreign Relations, 2001; United States District Court Southern District of New York, 1998). In reality, the outcome for al-Qaeda was less than desired, because while the attacks did cause severe damage to the U.S. embassy and U.S. citizens, the overwhelming majority of victims were Kenyans (Kean & Hamilton, 2004; Wright, 2006). The claims—composed before the attacks occurred and not updated prior to distribution—also attributed responsibility to three martyrs for the cause; in reality, al-Owhali failed in his mission for martyrdom and Muslims around the world responded to the attack with confusion, horror, and dismay (Wright, 2006).

The extent to which al-Qaeda utilised feedback from this attack, particularly pertaining to the importance of their greatest vulnerability—accurately matching operatives' capabilities with appropriate operations—is unknown for certain. Nevertheless, it is possible to speculate the organisation, at a minimum, attempted to utilise feedback gathered about the conduct of activities for its future activities and operations. This conclusion is made acknowledging members have consistently demonstrated rigour in continuously innovating and adjusting their tactics based on past interactions with enemies, such as during and following the Soviet invasion of Afghanistan in 1979 (Kenney, 2008). Documents compiled or published by al-Qaeda leadership, including the periodical journals *In the Shadow of the Lances* and *The Vanguards of the Kharasan* (Kenney, 2008) and *Call of the Global Islamic Resistance—Guide to the Jihad Way* (Ilardi, 2009), incorporate lessons learnt from the Soviet-Afghanistan war, the Iraqi insurgency, and al-Qaeda operations against the United States; these publications also extract passages from the Qur'an (al-Qaeda, n.d.; Kenney, 2008). Additionally, manuals such as *Declaration of Jihad against the Country's Tyrants* prescribe that after each operation there should be a full evaluation "as far as advantages and disadvantages" as well as the operatives' fulfilment of their duties (al-Qaeda, n.d., p. 76). These manuals also include short stories describing operatives who employ lessons learnt for future operations to underscore the importance of feedback to maximise future success.

Regarding feedback on the necessity to accurately evaluate operatives' capability, al-Qaeda does not appear to have recognised the extent to which operatives are its greatest operational vulnerability. Indeed, prior to the 9/11 attacks, in contrast to the other operatives who distanced themselves from their old lives, families, and friends, United Airlines 93 pilot hijacker Ziad Jarrah reportedly maintained closer contact with his family and continued an existing romantic relationship, possibly causing him to have doubts about the plot as late as the summer of 2001 (Kean & Hamilton, 2004, p. 110). Of greater interest, Jarrah's plane was the only one to not reach a definitive target, the plan having been altered when passengers aboard learnt of the prior hijackings and thus reacted accordingly, attempting to seize control of the cockpit and overpower the hijackers (Kean & Hamilton, 2004). While the truth might never be fully known, it could be argued Jarrah's capabilities were mismatched for the operation, as he operated a dual-life, with only half his heart confident and committed to the operation, to the consequence that when the passengers deviated from the intended plan, his confidence lowered, resulting in his inability to recover and adjust to fulfil his mission successfully.

Strong in intelligence collection, analysis, and counterintelligence, al-Qaeda was able to compete with its rival, the U.S., by planning the 1998 embassy attacks; however, weak in its intelligence activities that assessed its operatives' abilities resulted in an operational failure. Al-Qaeda demonstrated a clear appreciation for and use of intelligence, performing a variety of activities to engage in competition to know, circumvent, and attack its enemy. Information collection and analysis permitted the establishment of a target baseline, from which a plan could be devised that both enabled al-Qaeda to feel in control over the ability to evoke surprise and sow terror and confident in their expectations for success. In these attacks, intelligence efforts to understand self, chiefly the operatives, was insufficient for the group to claim an appreciable victory, judging by the number of failed outcomes and the confused and appalled reactions of the intended audience.

Daesh

The extent and ways in which Daesh undertakes and utilises intelligence activities on a routine basis and in support of attack operations showcases similarities and contrasts with al-Qaeda. At the organisational level, Daesh's strengths are akin to al-Qaeda's, including its obsessive counterintelligence culture, rigorous collection of information, and voracious processes to learn from and about its adversaries. In contrast, Daesh's knowledge of self was caveated by the organisation's failure to operationalise intelligence to analyse and capitalise on its capabilities, including both *underestimating* and *overestimating* its members' competencies in pursuit of the *dream*. At the level of individual operations, Daesh incorporated feedback by increasing the involvement of planners in attack preparations and executions to address the *incompetencies* demonstrated by operatives. A risky move, these actions would make the group more vulnerable if the planners were apprehended by the adversary. In the 2015 Paris attacks, Daesh's misjudgement of operative competencies and weak analysis of its adversary's capabilities undermined its degree of success; while the attackers were able to successfully challenge French security services, the French responded quickly to the threat, thus limiting the attackers' maximisation of terror and damage.

Daesh's intelligence doctrine prioritised intelligence collection and learning from adversaries, while implementing a pervasive and ruthless counterintelligence ethos. These practices were further supplemented by feedback pulled from the security, military, and intelligence experiences and knowledge of top personnel and their former work under or encounters with Saddam Hussein's Ba'athist party and the Mukhabarat, or Iraqi intelligence services (Speckhard & Yayla, 2017). At the height of its power between 2014-2016, Daesh exercised territorial control over regions in Syria and Iraq and its central leadership included several former Iraqi intelligence officers and military generals, colonels, and insurgency fighters (Speckhard & Yayla, 2017, pp. 4-6; Suc, 2017a). In pursuit of the dream to establish a sovereign Islamic state, a dedicated intelligence department responsible for securing internal security and planning external operations emerged known as the *Amniyat* or *Emni* (Speckhard & Yayla, 2017). Internal security directly correlates with the effort to know thyself, and for Daesh, this manifested vis-à-vis information collection, counterintelligence, learning, and feedback.

Daesh's intelligence collection efforts, similar to al-Qaeda, were vast and rigorously meticulous. In contrast, while the organisation did collect information about enemies, potential targets, and future territorial pursuits, collection efforts mostly concentrated internally, amassing volumes of information on members, applicants, defectors, and prisoners. This collection of information served counterintelligence purposes and to continuously vet and assess the degree of risk members posed to the organisation. The intelligence on those living within the territories as well as recruits included basic information, such as names, occupations, studies and education, and military experience or training, but also details such as nationalities and citizenships, marital status, health conditions and injuries, hobbies, email addresses, social media profiles, and phone numbers (Suc, 2017a; Suc, 2017c; Speckhard & Yayla, 2017). In preparation for the 2015 Paris attacks, planners drew from their own familiarity with Paris and accumulated information on a range of plausible targets, both to suit this and potential future operations (Brisard & Jackson, 2016). Planners were given discretion in their choice of target, with guidance to select soft, easy targets to maximise damage on civilians, with the belief a greater number of casualties would urge change within French foreign policy (Brisard, 2015; Cruickshank, 2017). During these stages, the national stadium, Stade de France, and the Bataclan Theatre, in particular, would emerge as valuable targets, due to the relative ease of access, number of expected casualties, and ability to inflict physical and psychological harm on French and foreign populations.

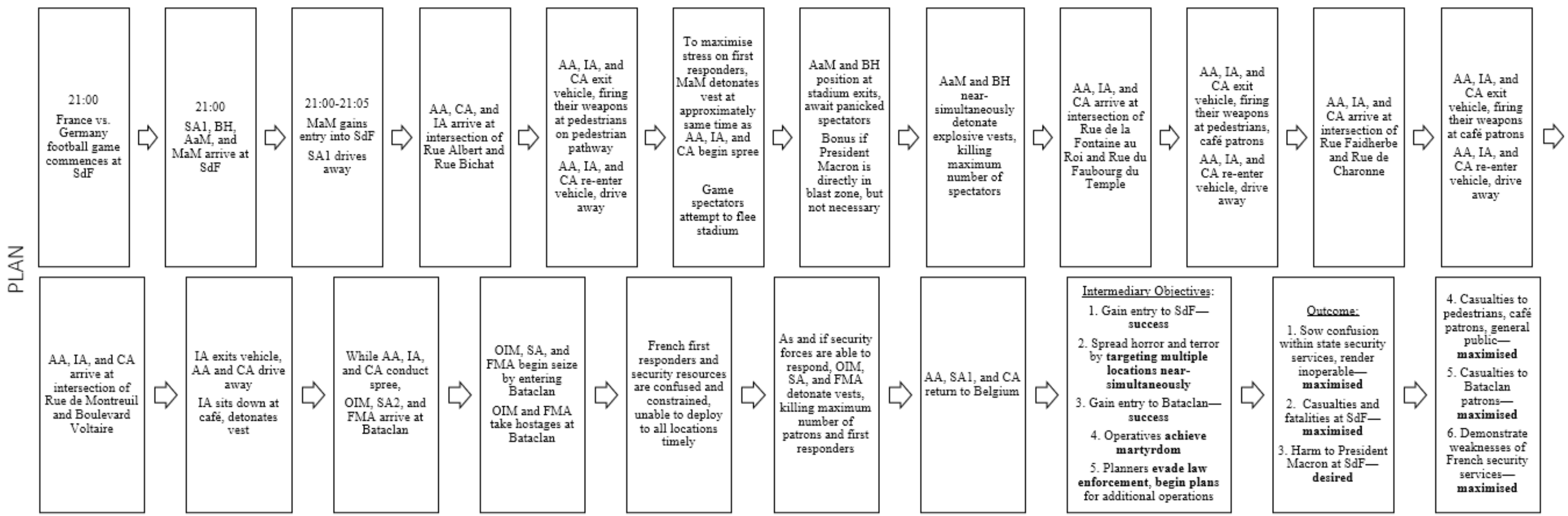
Counterintelligence practices further developed from direct interactions with and learning from adversaries, such as the intelligence services of the U.S., former U.S.S.R., Jordan, and Syria. Similar to al-Qaeda, Daesh sourced manuals on intelligence, espionage, and torture developed by the CIA and KGB (Suc, 2017a), directly translating the techniques into its own publications, such as its magazine *Inspire* and guide *How to Survive in the West* (Suc, 2017b), or combining them with the group's other inspirations and ideas for rewarding loyalty and punishing betrayal. Additionally, expounding upon feedback from their experiences under Saddam Hussein's dictatorial security state, the organisation sought to preserve internal security by devising an intricate network of informers (Suc, 2017b), encouraging members to spy and report on one another (Suc, 2017a). Counterintelligence practices aimed to thwart vulnerabilities posed by competing loyalties, detection by law enforcement, deception, and infiltration and to protect internal secrecy and the formidability of the Emni and its interworking; furthermore, tests of sincerity and the construction of 'intelligence barriers'—psychological boundaries that divided the type and extent of knowledge afforded to different groups of people within the organisation based on a need-to-know imperative—were implemented to assess the loyalty of untrusted recruits (Suc, 2017b; Callimachi, 2016) and to most importantly preserve the *dream*, strategy, and innerworkings of top leadership. These barriers took form as all members would adopt non-identifying *kunyas,—nom de guerres*— leaders would live and sleep in separate quarters from other group members, and operatives would be barred from seeking additional information or asking questions of their leaders and operational handlers (Suc, 2017a; Suc, 2017b; Suc, 2017d). Often, operatives were not informed of their mission or role in an attack nor permitted to meet their fellow operatives, until days prior to the attack's expected execution (Speckhard & Yayla, 2017; Suc, 2017b; Callimachi, 2016)—both practices in the 2015 Thalys train incident briefly detailed below.

Daesh's weak analytical ability resulted in a gap between expected and actual organisational capabilities evidenced in two ways: *underestimating* and *overestimating* operative competencies. First, the *underestimation* of competency resulted in recruits distancing themselves from or entirely disassociating with the organisation (Speckhard & Ellenberg, 2020), having become, in their own words, disillusioned (Anonymous, n.d; Speckhard & Ellenberg, 2020) with the dream and/or Daesh's strategies to achieve it. In these cases of *underestimation* and *underutilisation*, drawn by the dream to establish a territorial Islamic state and a desire to be a part of the state-building processes, hundreds of highly trained, experienced, or otherwise qualified technical experts flocked to Iraq and Syria, including doctors, scientists, technologists, engineers, and electricians (Vidino, et al., 2017, p. 66; Anonymous, n.d.). Eventual defectors would report that upon arriving in the territories, they and hundreds of foreign fighters would find themselves in one of two predicaments: either jobless and in limbo, waiting for an assignment within the territories or requested to return to their country of origin and await further instructions in carrying out an attack (Anonymous, n.d.; Speckhard & Yayla, 2017; Callimachi, 2016). In other instances, Daesh's leaders and planners *overestimated* operatives' competency. Some recruits, drawn by the illusion for adventure, were unschooled or ignorant of Islam, the Qur'an, and rules and regulations of waging *jihad* (Anonymous, n.d.) (Suc, 2017d). Others chosen to be martyrs were shocked to learn the nature of their future suicide missions, in part because of not studying the relevant Shari'ah law (Anonymous, n.d.). In terms of practical know-how, several operatives who would be sent back to their countries of origin to conduct attacks were unskilled in arms and explosives handling, procurement, or manufacture (Speckhard & Yayla, 2015), which leaders failed to cultivate for future attack success.

By overestimating operatives' competencies, leaders were negligent and failed to teach recruits about Islam, *jihad*, and martyrdom; train them in weapons and combat; and educate them on the attack preparation process—how to pick a target, collect and collate information surrounding the target, and devise a strategy that weighs pros, cons, possibilities, and probabilities—to maximise success (Anonymous, n.d.; Suc, 2017d; Speckhard & Yayla, 2017). Foreign fighters sent back to their countries of origin were afforded greater autonomy in their selection of targets, yet received ad hoc dictation and meagre support from leaders in Iraq and Syria. This, coupled with the lack of training in planning and conducting operations, insufficient confidence, and inadequate competence led to several botched operations, including the 2015 Villejuif church attack and the 2015 Thalys train attack. Both attacks were planned under the direction of Abdelhamid Abaaoud, a young foreign fighter whose connections, wealth, and skills would work favourably to gain him rank within the Emni as a planner for attacks overseas (Brisard, 2015; Homeland Security Advisory Council; Paris Public Safety Delegation, 2016), and who would come to also be one of the chief organisers of the 2015 Paris attacks. In both former attacks, Abaaoud underestimated the operatives' competencies—including their confidence, knowledge and technical ability—and thus failed to support the operatives towards the successful completion of their missions. In the first foiled attack, operative Sid Ahmed Ghlam was instructed to attack a church in Villejuif, France, but when the time came to execute the attack, he suffered from second thoughts (Vaux-Motnagny, 2020). Although Ghlam had previously travelled to Turkey, trained, and met directly with Abaaoud and other Emni members (Cruickshank, 2017), they failed to boost his morale to guarantee success and maintain his faith and commitment to the dream. Thus, fumbling with a seeping doubt, while attempting to put his gun in his belt, Ghlam instead shot himself in the leg and was later arrested (Callimachi, 2016; Suc, 2017d). In another operational debacle, the botched 2015 Thalys train attack, the technical *competence* of operative Ayoub El Khazzani was underestimated. Handled by Abaaoud, who equipped him with nine rounds of ammunition, a pistol, gasoline, a box cutter, and an AK-47 (Homeland Security Advisory Council; Paris Public Safety Delegation, 2016), El Khazzani did not possess the skill to employ the weapons, first jamming the AK-47 and then clumsily scrabbling with his weapons, unsure how to fix the AK-47 and proceed with the attack, during which time he was subdued by train passengers (Homeland Security Advisory Council; Paris Public Safety Delegation, 2016; Brisard, 2015).

The 2015 Paris attacks were thus an undertaking by Abaaoud and Daesh leadership to incorporate feedback—alongside existing collection and counterintelligence practices—to remedy such failures, and, taken as a whole result, the Paris attacks for Daesh were an operational success. In these attacks, Abaaoud assumed an operative role. His and a periphery cell's in-real-time support were key boosters where the operatives lacked the necessary competence or knowledge of the operation for the attack to be successful. Two timelines of the attacks, as planned (Fig. 7) and as executed (Fig. 8) are illustrated below.

Fig. 7



21:00 France vs. Germany football game commences at SdF

21:00 SA1, BH, AaM, and MaM arrive at SdF

21:00-21:05 MaM gains entry into SdF SA1 drives away

AA, CA, and IA arrive at intersection of Rue Albert and Rue Bichat

AA, IA, and CA exit vehicle, firing their weapons at pedestrians on pedestrian pathway AA, IA, and CA re-enter vehicle, drive away

To maximise stress on first responders, MaM detonates vest at approximately same time as AA, IA, and CA begin spree

Game spectators attempt to flee stadium

AaM and BH position at stadium exits, await panicked spectators Bonus if President Macron is directly in blast zone, but not necessary

AaM and BH near-simultaneously detonate explosive vests, killing maximum number of spectators

AA, IA, and CA arrive at intersection of Rue de la Fontaine au Roi and Rue du Faubourg du Temple

AA, IA, and CA exit vehicle, firing their weapons at pedestrians, café patrons AA, IA, and CA re-enter vehicle, drive away

AA, IA, and CA arrive at intersection of Rue Faidherbe and Rue de Charonne

AA, IA, and CA exit vehicle, firing their weapons at café patrons AA, IA, and CA re-enter vehicle, drive away

AA, IA, and CA arrive at intersection of Rue de Montreuil and Boulevard Voltaire

IA exits vehicle, AA and CA drive away IA sits down at café, detonates vest

While AA, IA, and CA conduct spree, OIM, SA2, and FMA arrive at Bataclan

OIM, SA, and FMA begin seize by entering Bataclan OIM and FMA take hostages at Bataclan

French first responders and security resources are confused and constrained, unable to deploy to all locations timely

As and if security forces are able to respond, OIM, SA, and FMA detonate vests, killing maximum number of patrons and first responders

AA, SA1, and CA return to Belgium

Intermediary Objectives:
1. Gain entry to SdF—**success**
2. Spread horror and terror by **targeting multiple locations near-simultaneously**
3. Gain entry to Bataclan—**success**
4. Operatives **achieve martyrdom**
5. Planners **evade law enforcement, begin plans** for additional operations

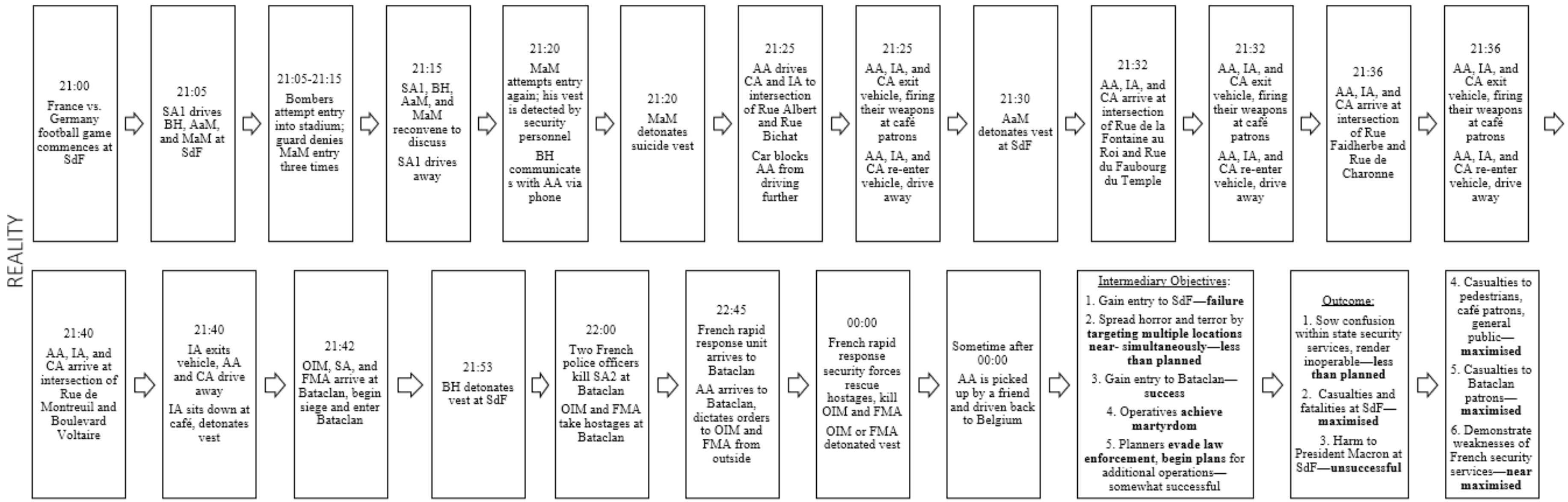
Outcome:
1. Sow confusion within state security services, render inoperable—**maximised**
2. Casualties and fatalities at SdF—**maximised**
3. Harm to President Macron at SdF—**desired**

4. Casualties to pedestrians, café patrons, general public—**maximised**
5. Casualties to Bataclan patrons—**maximised**
6. Demonstrate weaknesses of French security services—**maximised**

Key
SdF: Stade de France
SA1: Salah Abdeslam; Driver
BH: Bilal Hadfi; Suicide Bomber
AaM: Ahmad al-Mohammed; Suicide Bomber
MaM: M al-Mohammed; Suicide Bomber
AA: Abdelhamid Abaaoud; Planner; Driver; Shooter
CA: Chakib Akrouh Shooter
IA: Ibrahim Abdeslam; Shooter; Suicide Bomber
OIM: Omar Ismail Mostefai; Shooter; Suicide Bomber
SA2: Samy Amimour; Shooter; Suicide Bomber
FMA: Foued Mohamed-Aggad; Shooter; Suicide Bomber

Source*: Author. The Paris Attacks as Planned*

Fig. 8



REALITY
21:00 France vs. Germany football game commences at SdF
21:05 SA1 drives BH, AaM, and MaM at SdF
21:05-21:15 Bombers attempt entry into stadium; guard denies MaM entry three times
21:15 SA1, BH, AaM, and MaM reconvene to discuss
SA1 drives away
21:20 MaM attempts entry again; his vest is detected by security personnel
BH communicates with AA via phone
21:20 MaM detonates suicide vest
21:25 AA drives CA and IA to intersection of Rue Albert and Rue Bichat
Car blocks AA from driving further
21:25 AA, IA, and CA exit vehicle, firing their weapons at café patrons
AA, IA, and CA re-enter vehicle, drive away
21:30 AaM detonates vest at SdF
21:32 AA, IA, and CA arrive at intersection of Rue de la Fontaine au Roi and Rue du Faubourg du Temple
21:32 AA, IA, and CA exit vehicle, firing their weapons at café patrons
AA, IA, and CA re-enter vehicle, drive away
21:36 AA, IA, and CA arrive at intersection of Rue Faidherbe and Rue de Charonne
21:36 AA, IA, and CA exit vehicle, firing their weapons at café patrons
AA, IA, and CA re-enter vehicle, drive away
21:40 AA, IA, and CA arrive at intersection of Rue de Montreuil and Boulevard Voltaire
21:40 IA exits vehicle, AA and CA drive away
IA sits down at café, detonates vest
21:42 OIM, SA, and FMA arrive at Bataclan, begin siege and enter Bataclan
21:53 BH detonates vest at SdF
22:00 Two French police officers kill SA2 at Bataclan
OIM and FMA take hostages at Bataclan
22:45 French rapid response unit arrives to Bataclan
AA arrives to Bataclan, dictates orders to OIM and FMA from outside
00:00 French rapid response security forces rescue hostages, kill OIM and FMA
OIM or FMA detonated vest
Sometime after 00:00 AA is picked up by a friend and driven back to Belgium
Intermediary Objectives:
1. Gain entry to SdF—failure
2. Spread horror and terror by targeting multiple locations near- simultaneously—less than planned
3. Gain entry to Bataclan—success
4. Operatives achieve martyrdom
5. Planners evade law enforcement, begin plans for additional operations—somewhat successful
Outcome:
1. Sow confusion within state security services, render inoperable—less than planned
2. Casualties and fatalities at SdF—maximised
3. Harm to President Macron at SdF—unsuccessful
4. Casualties to pedestrians, café patrons, general public—maximised
5. Casualties to Bataclan patrons—maximised
6. Demonstrate weaknesses of French security services—near maximised

Key

SdF: Stade de France
SA1: Salah Abdeslam; Driver
BH: Bilal Hadfi; Suicide Bomber
AaM: Ahmad al-Mohammed; Suicide Bomber

MaM: M al-Mohammed; Suicide Bomber
AA: Abdelhamid Abaaoud; Planner; Driver; Shooter
CA: Chakib Akrouh Shooter
IA: Ibrahim Abdeslam; Shooter; Suicide Bomber

OIM: Omar Ismail Mostefai; Shooter; Suicide Bomber
SA2: Samy Amimour; Shooter; Suicide Bomber
FMA: Foued Mohamed-Aggad; Shooter; Suicide Bomber

Source*: Author. The Paris Attacks as Executed*

In preparation for the Paris attacks, planners collected information on multiple venues as targets; they sourced and downloaded blueprints of their seating layouts, entry and exit points, passageways, emergency routes, and stairways; scoured maps of Paris, including its pedestrian streets; and researched the symbolic significance of particular targets (Cruickshank, 2017). Stade de France would prove to be a valuable target due to its large capacity for patrons, and if the attacks were to take place during a game when French president François Hollande was expected to be in attendance, this could be interpreted by sympathisers as a symbolic strike at the heart of the chief enemy—France. During these stages of information collection and analysis, the Bataclan Theatre would also emerge as an advantageous option because an attack on it could be interpreted as an allegorical assault against additional adversaries; the Bataclan, under Jewish ownership, had previously hosted many pro-Israel events (Rotella, 2016) and the band expected to play the night of the attacks originated from the United States, with expectations for a large audience of foreigners, estimated at approximately 1500 (Moloney, 2019; Noël, et al., 2018).

Intent on maximising carnage at the Stade de France and the possibility of inflicting direct harm on president Hollande, the attackers' plans prescribed for one operative to slip past ticket checkers and into the stadium shortly after the game's start and detonate his vest. Reacting, panicked and fearful spectators were then expected to surge the stadium's exits, where two additional bombers would be positioned and ready to detonate their vests (Europol, 2016). It can be speculated the attackers might have anticipated a stronger presence of state security services at the stadium, given Hollande's attendance, and understood this as an opportune moment to undermine a notable portion of the French security divisions. Following the first detonation, these guards and law enforcement agents might have been expected to surge the entrances of the stadium, therefore also becoming victims of the second and third detonations, thus stunting and overwhelming the French security paradigm.

In reality, despite their collection of OSINT and HUMINT- based information, personal familiarities with Paris, and surveillance of the stadium, the planners failed to realise the easiest way into the stadium was not through brute force, but by purchasing tickets; it was the first operative's lack of a ticket which led him to be denied entrance to the stadium four times by security personnel (Cruickshank, 2017), at which point guards became aware of the IED-laced suicide vest beneath his clothes (Homeland Security Advisory Council; Paris Public Safety Delegation, 2016). During this time, the other two suicide bombers, anxious because the plan had gone awry and lacking the self-confidence and empowerment to adapt and take necessary action based on their own judgement, frantically called their distant planners to seek in-real-time guidance and instruction (Cruickshank, 2017; Brisard, 2015). The French security response to continue the game following the first detonation, to not inform the spectators, and to secure the premises by not allowing spectators to leave following the game's conclusion (Homeland Security Advisory Council; Paris Public Safety Delegation, 2016; Mehta, 2015) went against the expectations of the planners and bombers. Facing disrupted plans, faltered confidence, and unsupported empowerment, the two remaining bombers could not conceive a way to achieve their objective to maximise casualties. So, in a half-hearted effort, they detonated their vests approximately 25 minutes and 50 minutes after the attack began, resulting in a minimal effect on the public and French security services (Cruickshank, 2017; Reuters, 2015). At the Bataclan as well, suicide-vest-clad operatives stumbled with uncertainty and doubt in their ability infiltrating their consciences, as they plan to take hostages and make demands—arguably a technique demanding exchange or *negotiation*—seemed at odds with achieving martyrdom through a suicide mission. Unsure and uninformed, the operatives debated calling their planners for clarification and assistance (Speckhard & Yayla, 2017), but struggled to find a mobile signal, resulting in a cycle of frustrations and hesitations (Cruickshank, 2017). Irritated by his operatives' *incompetence*, Abaaoud was later observed by witnesses and on metro CCTV cameras shouting orders over the phone to the operatives inside, himself having had departed and later re-entered the city centre in desperation for the attack to be a success (Brisard, 2015; Cruickshank, 2017).

The role of intelligence within Daesh and during the Paris attacks illustrate key similarities and differences to al-Qaeda. In comparison, both groups demonstrate a clear awareness of the value of intelligence for non-operational and operational activities at the level of top leadership and planners. This is vital: intelligence acts as a bolstering mechanism to boost the confidence of leadership and to afford them a sense of certainty or control over the (envisioned successful) outcome of their struggles against state adversaries. To support their position in the rivalry, these groups prioritise the collection of information, counterintelligence, and learning from others, including the U.S., the former U.S.S.R., and France. With the exception of collection and counterintelligence, these activities were largely outward-focused to *know thy enemy*, including its weaknesses, vulnerabilities, strengths, and capabilities. Counterintelligence, supported by Daesh's narrowed collection efforts, on the other hand, was a pervasive and even lethal practice that primarily manifested in the continuous vetting of members vis-à-vis tests of loyalty, internal spies, and quasi-community policing. Throughout the critical planning stages of an attack, both groups devise meticulous plans to ensure their operational success, but fail to analyse information collected, brainstorm "what-if" scenarios or develop contingency plans, as well as empower operatives with adequate training, authority, confidence, and knowledge of an operation to re-adjust their tactics as necessary as an attack unfolds. Indeed, for Daesh, a lack of analysis led to misjudgement of French capabilities, who were flexibly and promptly able to adapt to the unfolding crisis saved an untold number of lives. These final points also underscore shortcomings in the *knowledge of self* and the challenge to align operatives' competencies with planners' strategies and the overall group's needs and dreams.

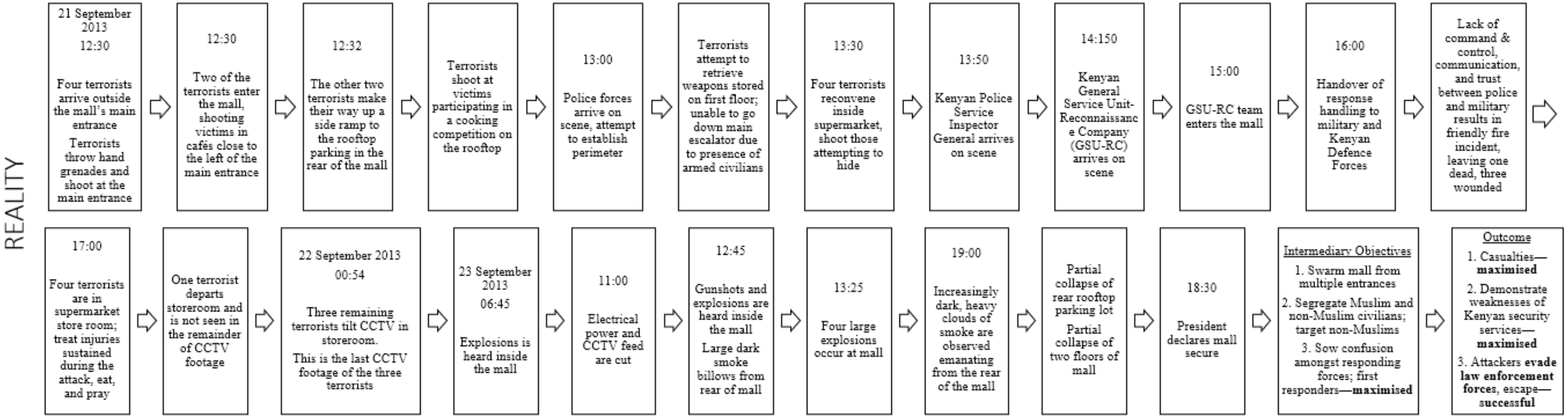
Speaking further on developing an understanding of self, similar to al-Qaeda's planners who vigorously incorporated lessons learnt into their future operations by developing post-action reports, the Paris attacks implemented feedback from prior operational busts in Europe. Parallel to al-Qaeda, who most saliently underestimated their operatives' competencies and the importance of confidence, Daesh also failed to sufficiently calculate, calibrate, and boost their operatives' confidence. By slight contrast, Daesh's attempt to address confidence and grasp better control over the outcome of its attacks by injecting planners dually as operatives worked to an extent in the opposite effect the organisation intended. Indeed, Abaaoud's involvement in the attack's execution and the in-real-time phone assistance and coordination from a cell based in Belgium (Cruickshank, 2015; Cruickshank, 2017) became operational crutches. This crutch is evidenced as the other operatives' competencies were lower than anticipated and they lacked support in the form of *knowledge* of the whole operation's plans and correspondingly a lack of *empowerment* to act independently. Requiring operatives to continuously request the green light from leadership before proceeding thus indicates planners' lack of *confidence* in operatives, which was in turn underscored by a weak sense of understanding of their operatives and competencies.

Al-Shabaab

The final case study, al-Shabaab's 2013 attacks on Nairobi's Westgate Mall, serves as a complement to the two former cases. While this case is plagued by a lack of clarity and key details remain unconfirmed or available to the public, it is still possible to develop a speculative understanding of al-Shabaab's use of intelligence in the attack by synthesising known information about al-Shabaab and its intelligence wing, the *Amniyat*, with observations of the organisation's change in its *modus operandi*, and evidence from the attack itself. These attacks exemplify that the competition between terrorists and their state rivals is not one of quantifiable man-or-machine power, but one of harnessing intelligence to strategically orient one's capabilities—amplifying the adversary's vulnerabilities and overrunning their capabilities—and to be cognizant of one's own vulnerabilities. This compares with the two former operations, which required more physical resources, precision to detail, and coordination across a temporal region for the most damaging effects. These former attacks further failed to achieve their intended levels of success owing to *overestimating* self and *underestimating* the enemy. Al-Shabaab's attacks, discernible for their lower-cost, lower-tech, and lower-sophistication, on the other hand, gravely debilitated and humiliated Kenya's security services, largely in part because the enemy's strength was *overestimated*—in reality, the Kenyan forces were inefficient, disorganised, and a much larger organisational *vulnerability* than a *capability*.

As little is confirmed about al-Shabaab's attack planning, a depiction of the Westgate attack as it unfolded is depicted in Fig. 9 below.

Fig. 9


REALITY
21 September 2013 12:30 Four terrorists arrive outside the mall's main entrance Terrorists throw hand grenades and shoot at the main entrance
12:30 Two of the terrorists enter the mall, shooting victims in cafés close to the left of the main entrance
12:32 The other two terrorists make their way up a side ramp to the rooftop parking in the rear of the mall
Terrorists shoot at victims participating in a cooking competition on the rooftop
13:00 Police forces arrive on scene, attempt to establish perimeter
Terrorists attempt to retrieve weapons stored on first floor; unable to go down main escalator due to presence of armed civilians
13:30 Four terrorists reconvene inside supermarket, shoot those attempting to hide
13:50 Kenyan Police Service Inspector General arrives on scene
14:150 Kenyan General Service Unit-Reconnaissance Company (GSU-RC) arrives on scene
15:00 GSU-RC team enters the mall
16:00 Handover of response handling to military and Kenyan Defence Forces
Lack of command & control, communication, and trust between police and military results in friendly fire incident, leaving one dead, three wounded
17:00 Four terrorists are in supermarket store room; treat injuries sustained during the attack, eat, and pray
One terrorist departs storeroom and is not seen in the remainder of CCTV footage
22 September 2013 00:54 Three remaining terrorists tilt CCTV in storeroom. This is the last CCTV footage of the three terrorists
23 September 2013 06:45 Explosions is heard inside the mall
11:00 Electrical power and CCTV feed are cut
12:45 Gunshots and explosions are heard inside the mall Large dark smoke billows from rear of mall
13:25 Four large explosions occur at mall
19:00 Increasingly dark, heavy clouds of smoke are observed emanating from the rear of the mall
Partial collapse of rear rooftop parking lot Partial collapse of two floors of mall
18:30 President declares mall secure
Intermediary Objectives 1. Swarm mall from multiple entrances 2. Segregate Muslim and non-Muslim civilians; target non-Muslims 3. Sow confusion amongst responding forces; first responders—maximised
Outcome 1. Casualties—maximised 2. Demonstrate weaknesses of Kenyan security services—maximised 3. Attackers evade law enforcement forces, escape—successful

Source*: Author. The Westgate Mall Attack as Executed*

In the organisation's first successful operation in Nairobi (Blanchard, 2013), on 21 September 2013, four al-Shabaab operatives armed with grenades and rifles approached the Westgate Mall and divided into teams of two, with one set approaching the main entrance and the second moving up a side ramp to access the rooftop parking lot (BBC, 2013). Attacking a mall was a change to al-Shabaab's attack *modus operandi*, which—except for its 2010 attacks in Kampala, Uganda—were characterised by VBIED and suicide-bombing attacks targeting Somali, Ethiopian, and Kenyan military bases and governmental establishments; international peacekeeping coalitions, such as the African Union Mission in Somalia (AMISOM); and NGOs and humanitarian aid convoys (Menkhaus, 2014; Center for International Security and Cooperation, 2019; Anzalone, 2016). While uncharacteristic, this move was strategic; attacking a high-end mall frequented by foreigners on a Sunday around noon, al-Shabaab militants could inflict more damage to Kenyan and foreign populations while also minimising a degree of Muslim casualties, who might have been expected to be away for routine mid-morning prayers. The planners' intent for its operatives to escape is evident by their lack of suicide belts/vests—also atypical of its *modus operandi*—and witness claims that some of the attackers would change their attire during the attack (New York Police Department, 2013; Howden, 2013). Compared with offices of the United Nations and other buildings of strategic or military importance in Nairobi, which are distant from main streets, the mall itself had several entry and exit points (New York Police Department, 2013; Kansas Fusion Center, 2013) and proximity to major streets, affording its operatives an easy escape. Furthermore, al-Shabaab planners could reasonably expect resistance in the presence of security services to be low at the mall, compared with the infrastructures of the United Nations, Kenyan government, and Kenyan military.

Throughout the attacks, operatives exhibited familiarity with the location, expertly navigating its many halls to corner civilians in narrow passages and at congestion points (Mirgani, 2017; Butime, 2014). Yet despite their intimate understanding of the facility and confidence in their ability to undermine Kenyan state security services—in which they succeeded—al Shabaab's planners did not account for the presence of plainclothes law enforcement and armed civilians (New York Police Department, 2013), who would complicate the operatives' ability to secure access to additional areas on the mall's lower floors, including a store where they had allegedly stashed weapons in the days prior (BBC, 2013; McConnell, 2014; Butime, 2014). Confused and challenged by these unexpected difficulties, the four operatives were forced to retreat and seek refuge in the mall's supermarket storeroom. With confidence shaken and conflicted over how to navigate past these unmarked sentries, the operatives sought assistance by calling the operation's planners before turning off the CCTV cameras observing them (Kansas Fusion Center, 2013; New York Police Department, 2013), and disappearing from view. To date, conflicting reports debate whether the operatives were killed in the aftermath, particularly following explosions that collapsed the upper two floors of the mall. With their last confirmed appearance a few minutes before 0100 HRS (New York Police Department, 2013) and Kenyan police and military forces in a spat and their withdrawal from the mall during the night—citing a lack of night vision equipment (Kansas Fusion Center, 2013)—,coupled with electrical lines and CCTV feed cut at 1100HRS (New York Police Department, 2013), this author maintains it can be claimed the attackers had more than enough time and opportunity to evade capture and escape in the ensuing confusion and chaos. Even if this can be disputed, al-Shabaab nevertheless succeeded overwhelmingly in debilitating the Kenyan security services, which lacked control and command in its own ranks and led to a friendly-fire standoff between military and police personnel, resulting in one death and three injuries (New York Police Department, 2013; Okari, 2014). This was followed by a consequential, prolonged recuperation period (Okari, 2014), during which the terrorists could have, at a minimum, relished in the reigning public's terror and their adversary's blunders, if not have used the opportunity to escape.

To grasp an understanding of these Kenyan security service capabilities—and their volatile position as a dual vulnerability—al-Shabaab developed an innovative intelligence collection technique, which further exploited its enemies vulnerabilities to boost its own capabilities. Recognising its enemy's forces were prone to frequent brothels and employ sex workers, al-Shabaab approached these women and offered them financial rewards and physical protection in return for information shared by military leaders during their stays with the prostitutes (Petrich, 2018; Petrich & Donnelly, 2019). The extent of the Kenyan forces' *incompetence* is further highlighted in their failure to secure the mall's perimeter and cordon off the area from curious onlookers (New York Police Department, 2013) and their failure to access or use CCTV footage in real-time before the power was cut, both of which would have assisted in the service's ability to locate and thwart the terrorists' escape.

Reaping more current successes, al-Shabaab did not always possess the strength it boasts today; in its early years, the group was inefficient and faced multiple failures, including a botched direct offensive against AMISOM forces in September 2010 known as the Ramadan Offensive, where al-Shabaab forces were defeated (Counter-Extremism Project, 2021). By learning from its failures when facing forces directly against its adversaries, al-Shabaab adopted terrorism as a tactic and shifted its strategies to target civilians (Anzalone, 2016). During 2010-2012, disagreement over strategy, tactical changes, and a weak counterintelligence culture threatened group cohesion and led to the splintering of the group and the adoption of new strategies which stand to date. These include a formidable intelligence unit comprised of multiple siloed sub-units—including intelligence collectors, external operations planners, suicide brigades, assassination squadrons, and finance and logistics teams (United Nations Security Council, 2013). Interestingly, during this time, the most significant structural problem to arise was the struggle to define and subsequently uphold the dream, leading to a power struggle between Ahmad Abdi Godane and Ibrahim Haji Jama, two co-founders of the organisation (Roble, 2013; Menkhaus, 2014). Being an organisation composed of several clans with differing perspectives and at times divergent interests, al-Shabaab would experience voluminous defections, as clan interests trumped priority over the leaders' dream of a united, fundamentalist Islamic state in Somalia; leaders also disagreed over launching campaigns and operations internationally and forging alliances—as Godane preferred—or concentrating efforts within Somalia (Menkhaus, 2014; Anzalone, 2014). Disagreements culminated to a peak just months before the Westgate attack, manifested in an internecine purge, during which Godane directed the murder of hundreds of the organisation's members. As a result of the purge, he would be able to restructure the organisation's core intelligence network— the Amniyat—to his liking and employ counterintelligence practices, including the threat and use of torture against suspected defectors (BBC, 2012; Speckhard & Shajkovci, 2019).

Exuberant and emboldened since its restructuring and clear successes in the Westgate Mall attack, al-Shabaab's maturity as a capable, increasingly active and competitive organisation cannot be denied. From the group's designation as a terrorist organisation by the U.S. State Department in 2008 through September 2013, the organisation executed fewer than fifteen high-profile (e.g. military, security, government, or law enforcement targets) or complex, coordinated attacks; by the time of this writing in mid-2021, the lethality and the number of high-profile or complex, coordinated attacks increased no less than five-fold, including al-Shabaab's attack at Garissa University in Kenya, which killed 148 (2015); on a military base in Af Urur, Somalia, which killed 59 and injured 38 (2017); in the centre of Somalia's capital Mogadishu, which killed at least 580 (2017); and near Somalia's Criminal Investigations Department and a hotel frequented by government and security officials, which killed 52 and injured at least 100 (2018) (Counter-Extremism Project, 2021). In these and other attacks, al-Shabaab demonstrated utilising feedback regarding its ability to compete with (and at times overwhelm) domestic and foreign security services, but also attempted to learn from the tactics and techniques of others, including al-Qaeda, with whom the organisation pledged allegiance in 2012 (BBC, 2013; Counter-Extremism Project, 2021). Additionally, documents found on an al-Shabaab terrorist in 2014 detailed the Westgate planners' intent to replicate the strategies of perpetrators in Mumbai's 2008 terrorist attacks, including utilising low-sophistication weapons and technologies, targeting sites of Jewish and/or foreign influence or activity, and employing techniques of swarming, all aimed to devastate responding security forces (Cruickshank, et al., 2013).

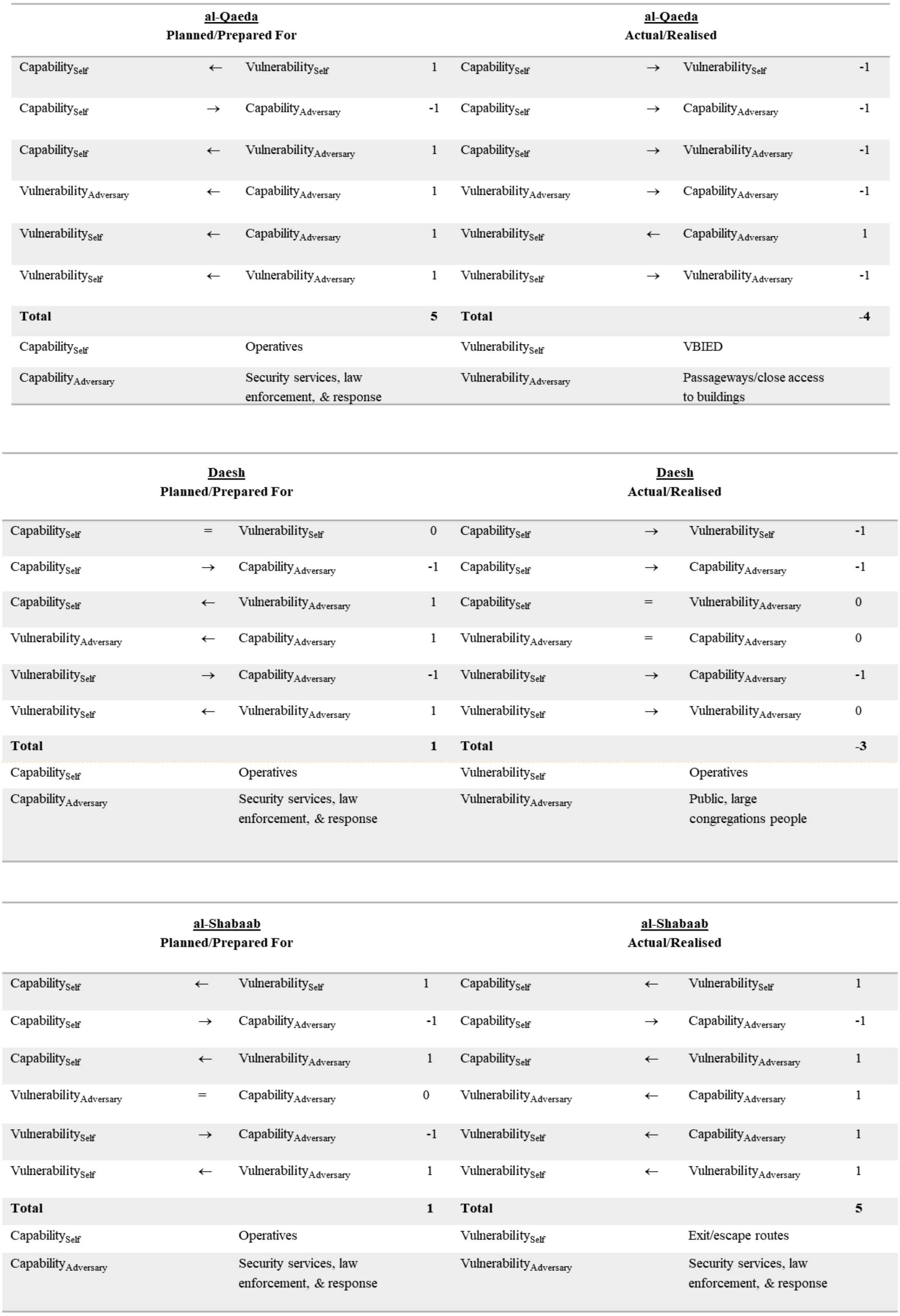
Tying it Together: Preparation for Production

These three case studies attempted to evince an understanding of how terrorist organisations exercise and operationalise intelligence for their routine activities and attack operations. Taken in sum, these cases underline the proposition first, that terrorists utilise intelligence and secondly, of superior importance, that the purpose of intelligence is to embolden terrorist organisations with confidence in the judgement of their vulnerabilities and capabilities against those of their adversaries. Consistent with the findings of Bell and Gentry, these groups demonstrate proclivity towards rigorous information collection and ruthless counterintelligence, while evidencing a struggle with analysis. In contrast with Bell's and Gentry's arguments, these findings argue intelligence analysis is not necessarily due to a lack of *strategic intelligence*. In fact, it is in the execution of attacks themselves—operational steppingstones towards the fulfilment of the dream—where terrorist organisations are challenged in their ability to judge their capabilities and vulnerabilities against those of their adversaries. This operational intelligence also reveals the difficulties of managing *volatility*—a measure of risk between organisational *capabilities* and organisational *vulnerabilities*. Indeed for terrorist organisations, operatives are extremely *volatile* due to the tenuous balance of vulnerability or capability. In the latter two cases, the terrorist organisations were unable to sway their operatives' volatility in the favour of being organisational capabilities. In the latter case, al-Shabaab militants triumphed from its adversary's inability to manage their own volatilities, the Kenyan security services.

In al-Qaeda's attacks, planners miscalculated the extent of their capabilities and vulnerabilities, believing their operatives were competent and able to manoeuvre the VBIED close enough to the embassy's undefended passageway to maximise U.S. damage. In reality, the operatives proved unable to adapt their tactics to exploit their opponent's weaknesses. For Daesh, the recognition of operative incompetence led the planners to involve themselves directly in executing the attack. To a fate similar to al-Qaeda, these acts suffered to realise their intended effects as operatives needed supervisory approval at each stage and thus could not proceed expediently. Lastly, al-Shabaab's planners, while possibly not underestimating their own capabilities, could at least celebrate from underestimating the severity of the Kenyan forces' vulnerabilities, which allowed al-Shabaab's militants to inflict more chaos, confusion, and carnage—more success than anticipated.

The tables below break down each terrorist organisation's possible interpretations of how each perceived their respective and relative capabilities or vulnerabilities, which in turn heartened them with confidence to strike.

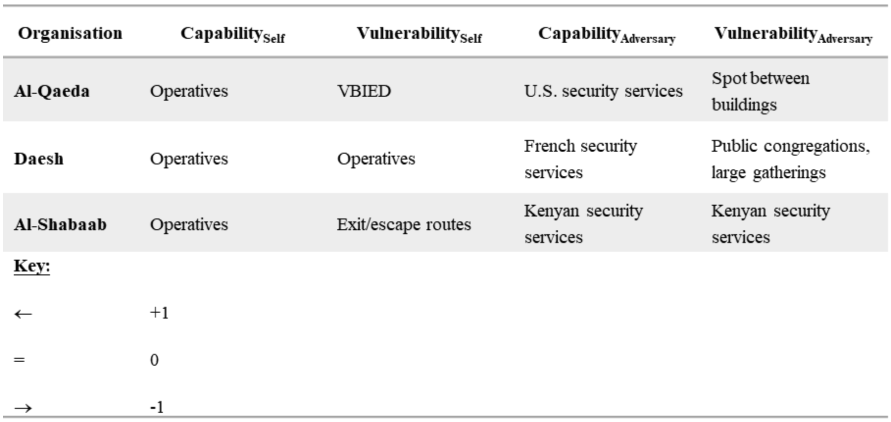
Fig. 10



al-Qaeda Planned/Prepared For				al-Qaeda Actual/Realised			
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Self}}$	1	Capability$_{\text{Self}}$	→	Vulnerability$_{\text{Self}}$	-1
Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Capability$_{\text{Self}}$	→	Vulnerability$_{\text{Adversary}}$	-1
Vulnerability$_{\text{Adversary}}$	←	Capability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Adversary}}$	→	Capability$_{\text{Adversary}}$	-1
Vulnerability$_{\text{Self}}$	←	Capability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	←	Capability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	→	Vulnerability$_{\text{Adversary}}$	-1
Total			**5**	**Total**			**-4**
Capability$_{\text{Self}}$		Operatives		Vulnerability$_{\text{Self}}$		VBIED	
Capability$_{\text{Adversary}}$		Security services, law enforcement, & response		Vulnerability$_{\text{Adversary}}$		Passageways/close access to buildings	

Daesh Planned/Prepared For				Daesh Actual/Realised			
Capability$_{\text{Self}}$	=	Vulnerability$_{\text{Self}}$	0	Capability$_{\text{Self}}$	→	Vulnerability$_{\text{Self}}$	-1
Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Capability$_{\text{Self}}$	=	Vulnerability$_{\text{Adversary}}$	0
Vulnerability$_{\text{Adversary}}$	←	Capability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Adversary}}$	=	Capability$_{\text{Adversary}}$	0
Vulnerability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Vulnerability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	→	Vulnerability$_{\text{Adversary}}$	0
Total			**1**	**Total**			**-3**
Capability$_{\text{Self}}$		Operatives		Vulnerability$_{\text{Self}}$		Operatives	
Capability$_{\text{Adversary}}$		Security services, law enforcement, & response		Vulnerability$_{\text{Adversary}}$		Public, large congregations people	

al-Shabaab Planned/Prepared For				al-Shabaab Actual/Realised			
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Self}}$	1	Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Self}}$	1
Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Adversary}}$	=	Capability$_{\text{Adversary}}$	0	Vulnerability$_{\text{Adversary}}$	←	Capability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Vulnerability$_{\text{Self}}$	←	Capability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1
Total			**1**	**Total**			**5**
Capability$_{\text{Self}}$		Operatives		Vulnerability$_{\text{Self}}$		Exit/escape routes	
Capability$_{\text{Adversary}}$		Security services, law enforcement, & response		Vulnerability$_{\text{Adversary}}$		Security services, law enforcement, & response	



Organisation	Capability$_{\text{Self}}$	Vulnerability$_{\text{Self}}$	Capability$_{\text{Adversary}}$	Vulnerability$_{\text{Adversary}}$
Al-Qaeda	Operatives	VBIED	U.S. security services	Spot between buildings
Daesh	Operatives	Operatives	French security services	Public congregations, large gatherings
Al-Shabaab	Operatives	Exit/escape routes	Kenyan security services	Kenyan security services

Key:

←	+1
=	0
→	-1

Source*: Author. Perceived Capabilities and Vulnerabilities in Terrorist Attacks*

The direction of the arrow indicates the direction of favour while '=' indicates no obvious favour in a particular direction or the ability for these attributes to challenge one another. For instance, "Vulnerability$_{\text{Self}}$ ¬ Capability$_{\text{Adversary}}$" indicates when posited against one another, one perceives their vulnerabilities are 'stronger than' or unable to be exploited by their adversary's capabilities, thus working *towards* their favour (+1). "Vulnerability$_{\text{Self}}$ ® Vulnerability$_{\text{Adversary}}$" illustrates the perception that an adversary's vulnerabilities are favoured over one's own vulnerabilities, that is, one's own vulnerabilities are challenged or at a disadvantage to their adversary's, working *against* their favour (-1). Where the total score is *positive*, an actor feels confident in the ability to succeed with an attack and is thus more likely to engage in open action and confrontation with their opponent; where the score is *negative*, an actor is less confident in the probability for success, which might dissuade against executing an operation until the circumstances or relevant factors change to be more strongly in their favour. This is well illustrated with Daesh, where in absolute terms, perceptions generated a marginal opportunity for success at +1, yet the opportunity for success was still positive in their favour, triggering the confidence to attack, which they did. Al-Shabaab, equipped with limited resources and manpower, predicted fringe success. Yet in contrast with the other groups, its adversary's vulnerabilities were in reality much greater than its capabilities to overcome them, to which Al-Shabaab could then celebrate in the tremendous weaknesses of its adversary if not its own meagre strengths.

Additional conclusions can be drawn from these studies. Most profoundly, terrorist organisations operationalise intelligence to minimise their lack of confidence in their ability to succeed. In a competition against an asymmetrically advantageous adversary, confidence is essential for the organisation to take action in pursuit of its dreams, and for terrorist organisations, the challenges of securing and sustaining confidence manifest in three forms. First, planners lack confidence in operatives. Threatened by their lack of control over their operating environment and the prospects their operatives will be *incompetent*, planners compulsively collect troves of detailed information to guide their operatives' every action in an attack and hedge against failure. Details and volume, even if they do not inherently add intrinsic value, are a proxy through which organisers can plan for operational certainty and success. As operatives are *volatile*, organisational leaders additionally take care to implement counterintelligence practices aimed at segregating their operatives physically, psychologically, and intellectually from other aspects of the organisation. Second, operatives lack confidence in *self*, which leads them to stumble or often retreat when unexpected anomalies present a challenge or need to deviate from the operation's plans. For terrorist organisations, operatives embody the epitome of *volatility*. While operatives might be equipped with tactical and combat knowledge, for counterintelligence purposes, planners often do not divulge all details of an attack to them, nor equip them with additional circumstantial or 'periphery knowledge,' which could prove useful in the event the execution goes awry. Because operatives' knowledge is short-sighted and they are not trained to be empowered nor resilient when faced with disruptions to attack plans, operatives often lose faith in themselves or even their mission. Lastly, the organisation suffers when any of its members lack confidence in the dream. When members are not united by a common dream, devoid of commitment to bringing the dream into reality, or lack assurance that its reality is possible, the organisation will be unable to progress forward. Indeed, the dream can only exist and come to be if there is a belief that it can, does, or will exist.

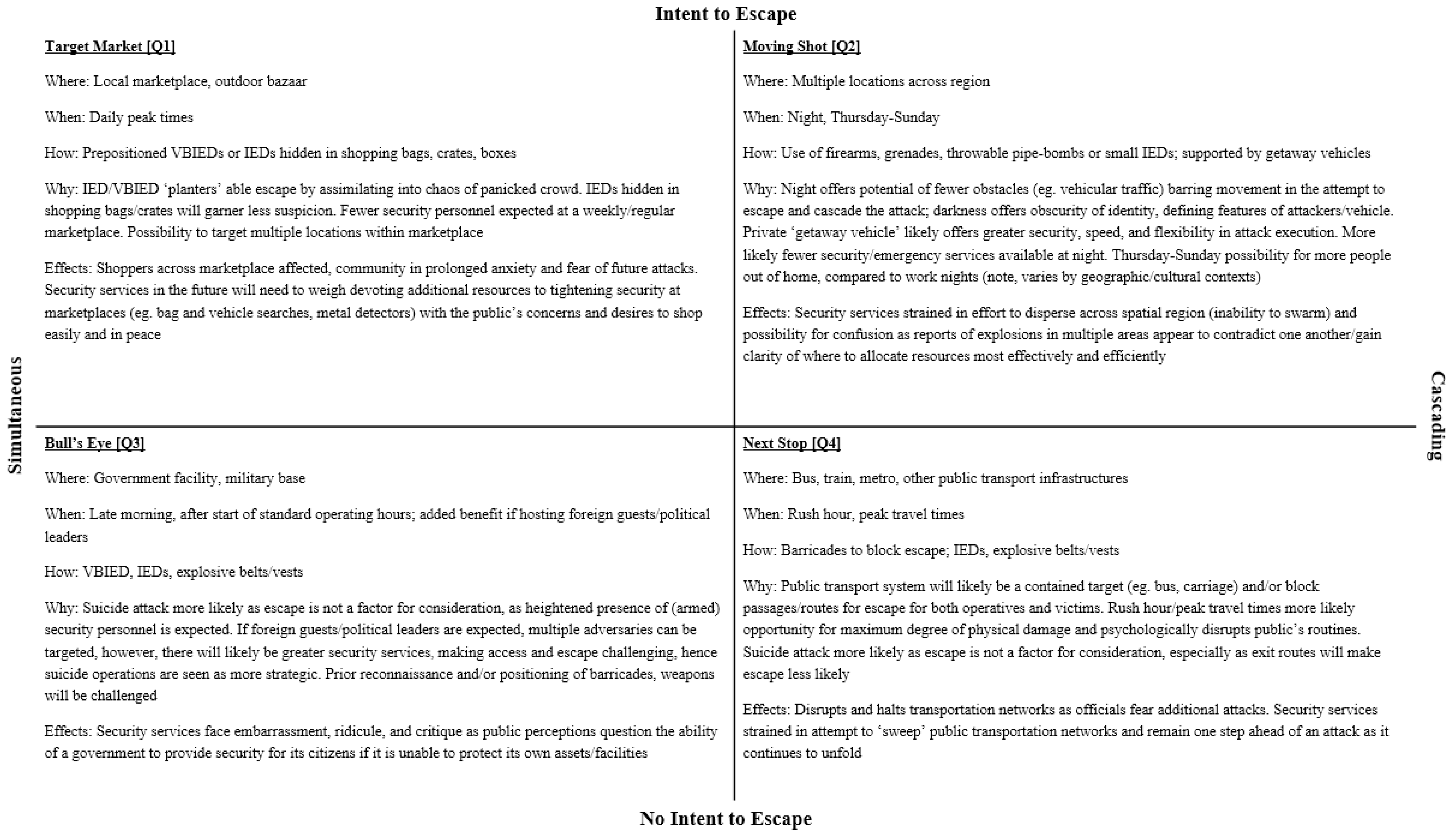
Anticipating the Attack & SATs

Lastly, as a look towards the future, this study applies Quadrant Crunching and Red Hat Analysis as techniques through which frontline security personnel, first responders, and crisis management planners might be able to devise strategies to avert, detect, or moderate terrorist attacks. Structured Analytic Techniques (SATs) are tools to help analysts "break down a specific analytic problem into its component parts and [by] specifying a step-by-step process for handling these parts, structured analytic techniques help to organize the amorphous mass of data with which analysts must contend" (Heuer & Pherson, 2011, p. 25). Two techniques utilised in this study are Quadrant Crunching—to first develop scenarios—and Red Hat Analysis—to then postulate how scenarios could unfold. These techniques are chosen specifically as they strive to “reframe” (Heuer & Pherson, 2011) the analyst’s way of thinking to challenge biases and break mental mindsets. These techniques also help the analyst generate multiple perspectives on an issue or alternatively a host of options, thus reducing the potential for surprise.

Quadrant Crunching is a systematic procedure conceived “to help counterterrorism analysts and decision-makers identify the different ways radical extremists might mount a terrorist attack” (Heuer & Pherson, 2011, p. 144). Using this framework, analysts identify and challenge their assumptions to identify key variables and develop feasible future scenarios; by way of developing alternative futures, this technique helps reduce the potential for surprise. This study uses the following variables to develop a variety of possible CCA scenarios as perpetrated by a cell of terrorist operatives: sequence of events (simultaneous and cascading) and intent for operatives to escape (present and absent). The four plausible scenarios are then taken a step further, using Red Hat Analysis to postulate how such an attack might unfold. Red Hat Analysis is a technique where an analyst puts themselves in another individual’s shoes to replicate the individual’s decision-making processes and predict their future behaviour or actions (Pherson Associates, LLC, 2016). An analyst must make a conscious effort to change their “perspective from that of an analyst observing and forecasting an adversary’s behavior to that of a leader [for example, a foreign leader, criminal, or competitor] who must make a difficult decision within that operational culture” (Heuer & Pherson, 2011, p. 198) and to perceive an emotion, event, or situation as the subject actor perceives it. This tool offers benefits for counterterrorism efforts for avoiding mirror imaging bias, or ‘terrorists act in the ways we act,’ and projection bias, or ‘terrorists act in the ways we think they act,’ or for “identifying when to intervene [or] where attacks are likely to occur” (Romyn & Mark, 2014, p. 495). This technique also builds from the recognition that the reluctance or failure to understand how others think might be a “fundamental reason why it [intelligence] is so frequently wrong” (Jervis, 2012).

Using these two variables, possible characteristics of each type of attack are detailed in the matrix below (Fig. 11).

Fig. 11



Intent to Escape

Target Market [Q1]

Where: Local marketplace, outdoor bazaar

When: Daily peak times

How: Prepositioned VBIEDs or IEDs hidden in shopping bags, crates, boxes

Why: IED/VBIED 'planters' able escape by assimilating into chaos of panicked crowd. IEDs hidden in shopping bags/crates will garner less suspicion. Fewer security personnel expected at a weekly/regular marketplace. Possibility to target multiple locations within marketplace

Effects: Shoppers across marketplace affected, community in prolonged anxiety and fear of future attacks. Security services in the future will need to weigh devoting additional resources to tightening security at marketplaces (eg. bag and vehicle searches, metal detectors) with the public's concerns and desires to shop easily and in peace

Moving Shot [Q2]

Where: Multiple locations across region

When: Night, Thursday-Sunday

How: Use of firearms, grenades, throwable pipe-bombs or small IEDs; supported by getaway vehicles

Why: Night offers potential of fewer obstacles (eg. vehicular traffic) barring movement in the attempt to escape and cascade the attack; darkness offers obscurity of identity, defining features of attackers/vehicle. Private 'getaway vehicle' likely offers greater security, speed, and flexibility in attack execution. More likely fewer security/emergency services available at night. Thursday-Sunday possibility for more people out of home, compared to work nights (note, varies by geographic/cultural contexts)

Effects: Security services strained in effort to disperse across spatial region (inability to swarm) and possibility for confusion as reports of explosions in multiple areas appear to contradict one another/gain clarity of where to allocate resources most effectively and efficiently

Simultaneous

Cascading

Bull's Eye [Q3]

Where: Government facility, military base

When: Late morning, after start of standard operating hours; added benefit if hosting foreign guests/political leaders

How: VBIED, IEDs, explosive belts/vests

Why: Suicide attack more likely as escape is not a factor for consideration, as heightened presence of (armed) security personnel is expected. If foreign guests/political leaders are expected, multiple adversaries can be targeted, however, there will likely be greater security services, making access and escape challenging, hence suicide operations are seen as more strategic. Prior reconnaissance and/or positioning of barricades, weapons will be challenged

Effects: Security services face embarrassment, ridicule, and critique as public perceptions question the ability of a government to provide security for its citizens if it is unable to protect its own assets/facilities

Next Stop [Q4]

Where: Bus, train, metro, other public transport infrastructures

When: Rush hour, peak travel times

How: Barricades to block escape; IEDs, explosive belts/vests

Why: Public transport system will likely be a contained target (eg. bus, carriage) and/or block passages/routes for escape for both operatives and victims. Rush hour/peak travel times more likely opportunity for maximum degree of physical damage and psychologically disrupts public's routines. Suicide attack more likely as escape is not a factor for consideration, especially as exit routes will make escape less likely

Effects: Disrupts and halts transportation networks as officials fear additional attacks. Security services strained in attempt to 'sweep' public transportation networks and remain one step ahead of an attack as it continues to unfold

No Intent to Escape

Source*: Author. Terrorist Attack Options on Considerations of 'Sequence of Events' and 'Intent to Escape'*

Target Market (Q1)

With the intent to escape and attacks that occur simultaneously, terrorists might opt to attack a populous, outdoor *Target Market* or bazaar. IEDs hidden in produce crates could avoid suspicion, and placed at multiple locations throughout the marketplace, maximise casualties throughout. In this type of incident—similar to the 2013 Westgate Mall attack—terrorists could escape by assimilating themselves in with panicked, fleeing shoppers. Particularly in tightly-knit communities or at markets of historical or social significance, prolonged psychological effects—including fear, apprehension, and anxiety—might alter the attitudes of future shoppers and taint the viability of the marketplace in the future. Decision-makers will need to carefully weigh their options for future security measures, as shoppers will demand greater security or efforts to ensure their safety, yet they might be opposed to the hassle of arduous bag and body searches.

Moving Shot (Q2)

Moving Shot has a unique potential to paralyse state security services. In this type of attack, terrorists perpetrate an attack with several 'phases' and an aim to escape, waging a game of 'cat and mouse,' believing they have an upper hand, whereas state services are left bewildered and uncertain *if*, *where*, and *when* a next stage might occur. When occurring across a spatial region, such as multiple streets of a city—as in the 2015 Paris attacks—first responders might also be initially confused over seemingly conflicting reports of violence in multiple areas. To maximise casualties—while subject to cultural concepts and attitudes towards time—the attack might take place when more people are expected to be outside, such as the end of the workweek; striking at night could also work to the terrorists' favour in this scenario as less rush-hour traffic and darkness would indirectly assist their efforts to evade or escape law enforcement.

Bull's Eye (Q3)

Striking the *Bull's Eye*—a facility or location of chief political, military, or security significance—is a riskier endeavour for a terrorist organisation, owing to a greater likelihood for the presence of searches and checks, armed guards, and other security measures. For these reasons, the organisation might not expect its operatives to have a greater chance to escape and, consequently, opt for suicide-bombing as a tactic, such as apparent in the 1998 U.S. embassy bombings. While these additional security measures and forces might be expected, thus challenging the ability for terrorists to succeed, terrorists might perceive such an attack as advantageous for two reasons: first, an attack on such a 'high-profile,' 'inaccessible,' or ‘mighty’ adversary would demonstrate to sympathisers that despite being at comparable resource and legitimacy disadvantages, the terrorist organisation does possess its own strength and that the enemy is not infallible. Moreover, security services will be directly embarrassed—if not degraded and damaged—following an attack, provoking onlookers to wonder, ‘If the state is unable to protect itself, how can we trust the state to protect us?’

Next Stop (Q4)

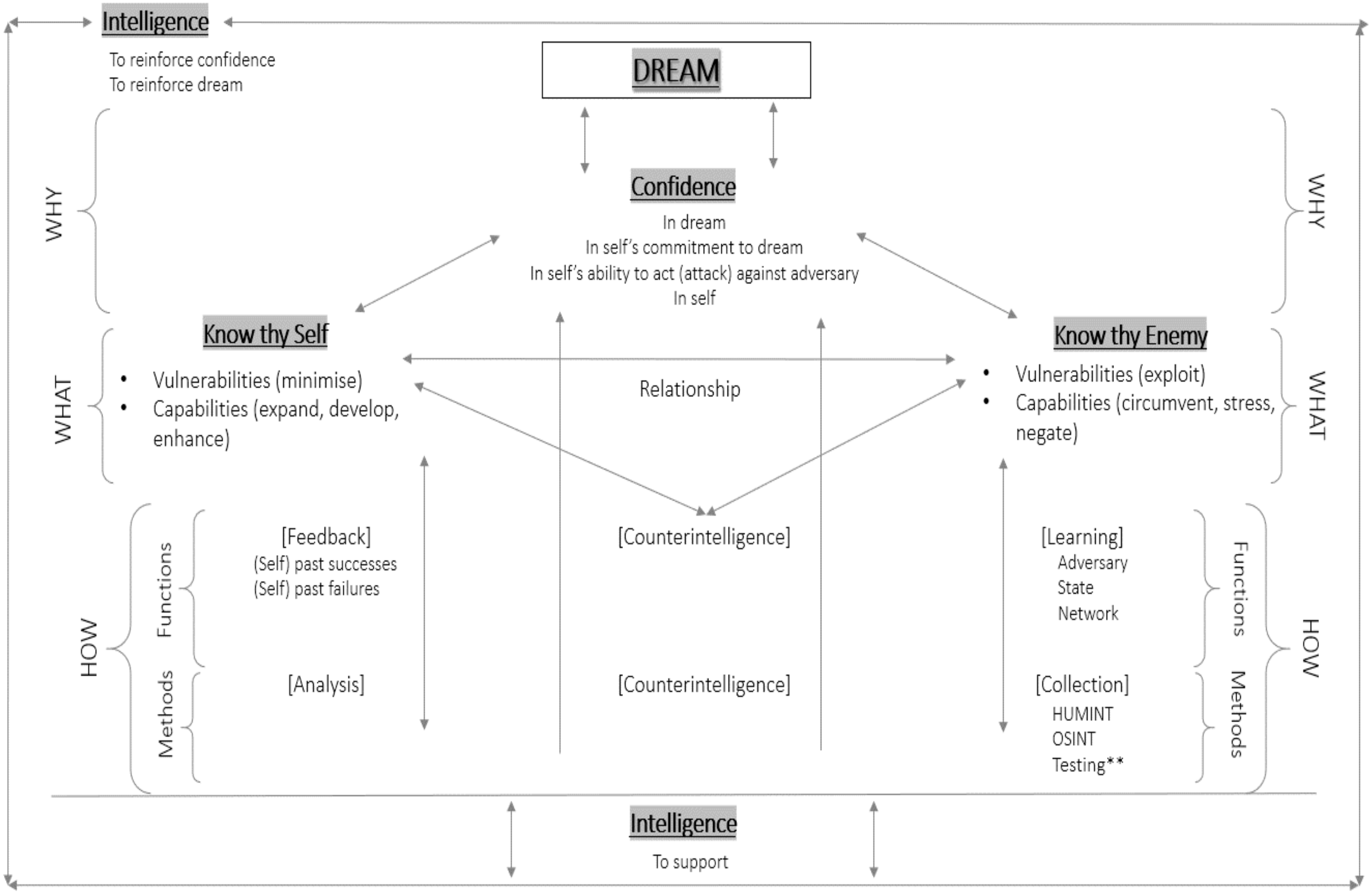
Lastly, in the *Next Stop*, terrorists might strive to maximise casualties with a cascading attack but perceive no need for its operatives to escape. With these considerations, a terrorist organisation might select a public transport system, where confined spaces—such as train carriages, buses, or underground metro passageways and halls—might make it more challenging for passengers and perpetrators alike to escape. Terrorist attacks executed during peak travel times or rush-hour might reap greater casualties and cause further ramifications on transportation networks, as the affected infrastructures and routes might need to be temporarily shut down or taken out of service as they are searched. Similarly to *Moving Shot*, security services and resources might be over-extended or even unable to keep up with multiple phases of an attack, coupled with the need to conduct thorough sweeps of transportation networks. While not necessarily examples of *cascading, no intent to escape attacks*, the 1980 Bologna massacre—the bombing of the central train station in Bologna, Italy—and the 1995 Tokyo subway Sarin attack were both terrorist incidents targeting public transportation networks, and these can shed light on possible effects of future attacks on public transportation infrastructure. For instance, in both incidents, ambulance and police services struggled to access and transport trapped victims, and in the years following each incident, direct and indirect audiences suffered from psychological and physical trauma, including severe injuries, PTSD, and heightened anxiety when needing to travel (Comune di Bologna, 2021) (Tota, 2013) (Olson, 1999).

Final Remarks

Before contributing this study’s own theory on terrorists’ intelligence, it is essential to acknowledge disconfirming evidence or suggest alternative explanations for this study’s findings. In the first instance, terrorists might not equate the actions they perform with traditional notions of *intelligence*. While a viable claim, this explanation ignores, at least for the organisations explored in this analysis, proof that several top leaders formerly ranked as military and intelligence officers within state intelligence services and structured their terrorist organisations using lessons learnt from their experiences. Turning to confidence, it might be argued because terrorist organisations believe they have little to lose but much to gain, terrorists might not require intelligence, nor much confidence to strike their rivals through attacks. This argument is reasonable when considering that some terrorist organisations have an unbroken faith that their dreams have already been achieved in the future. These arguments, though, indirectly underpin terrorists' beliefs and confidence in their dream and its success. In fact, this study does not claim that intelligence enables the realisation of the dream, that intelligence equates confidence, nor that terrorists amass databases of collected information, which they scrutinise to discover loopholes. Instead, this study discovers intelligence can support and reinforce the terrorists' dream. Intelligence also paves the way for terrorists to exert and perceive a degree of control in their operating environment and the overall success of their actions. This last statement is important for first responders and even high-level politicians and policymakers—*terrorists plan to succeed and fail to plan for failure*. They equate intelligence with assurance to the extent that should their attack plans go awry, they are largely unadaptable or they still believe even through blunders, mistakes, and operational disasters, they are ultimately successful. The value of the threat is in the response to it. Two vital keys to expressly denying terrorists' success then would be first to disrupt these meticulous plans and second to respond by *not* supplanting terrorists with the attention and frenzy of panic and recognition on which they thrive. Lastly, measures of intelligence and confidence cannot be reduced to characteristics of just quantity or quality; it is also perception, and as rational actors, terrorists do not inherently need SIGINT of their adversary's communications nor MASINT, which details their adversary's radar assets. Rather, they need a perception that when planning an attack, the net of their capabilities and vulnerabilities juxtaposed against their adversary's net capabilities and vulnerabilities will be more favourable on their behalf.

This research proposes an additional theory for intelligence and counterterrorism studies based on its findings pertaining to the role of intelligence for terrorist organisations plotting attacks. This theory purports that terrorists operationalise intelligence in attempts to support and reinforce their confidence and dream. The intelligence competition thus ensues as terrorist organisations use a variety of intelligence *means* to inform themselves of capabilities and vulnerabilities of themselves and their rivals, from which they garner an assurance of command over the uncertainty of an attack and in its successful outcome. The graphic below outlines this theory of *Terrorist Intelligence and Confidence (TIC)* (Fig. 12).

Fig. 12



**"Testing" is understood as a method by which VNSA-Ts operate below the threshold of violence, yet, directly engage with a target or enemy prior to an attack, in a 'trial' to collect information. This includes any active, direct action that probes to acquire more information in particular about a particular target or audience. Examples include carrying weapons in the vicinity of a target site to gauge security guards' reactions, dropping/abandoning items to judge the public's reaction.

Source*: Author. Terrorist Intelligence and Confidence (TIC)*

As illustrated, the processes in this theory can be concurrent, continuous, multidirectional, and informative. When terrorists devise attack operations, intelligence serves as foundational *support* and surrounding *reinforcement* mechanism for the terrorists' dream. At the base are the methods and functions of intelligence: *how* intelligence is both performed [*methods*] and operationalised [*functions*]. Terrorists *collect* and *analyse* information, while also denying and espousing practices or performing activities intended to deny 'outsiders' and even 'insiders' access to information, processes, and organisation. It is imperative to note these latter *counterintelligence* practices and activities can offer *positive* support/reinforcement for the dream—actively seeking out or acquiring personnel, information, or opportunities that confirm or validate the dream—or they can offer *negative* support/reinforcement for the dream—disavowing or rejecting personnel, information, or opportunities which disconfirm or invalidate the dream. With these *methods*, intelligence serves, or *functions,* to educate terrorists from/about their adversaries and from/about themselves. Of their adversaries, terrorists seek *knowledge* of the capabilities and vulnerabilities—the former, which the terrorist intends to circumvent, thwart, or negate, and the latter which should be exploited. Terrorists utilise this *knowledge* of both their adversaries and themselves to match capabilities and vulnerabilities with attack opportunities where the terrorist can achieve some type of favourable impact or success. Moreover, this *knowledge* corresponds with impressions of certainty and control over the effects resulting from particular actions, thus triggering confidence in self, actions, and the ultimate dream. Because these elements are not unidirectional, the dream also serves as the motivation ultimatum for why terrorists feel compelled to attack.

Within intelligence studies, *Terrorists' Intelligence and Confidence (TIC*) supports Gill's argument that intelligence serves as "Both a *form of* and *resource for* the exercise of power," (2018, p. 581) as it is evident intelligence emboldens a terrorist organisation to attack. In these circumstances, power manifests in the ability to act and exert control over a situation or set of circumstances; confidence is power. The implications for this theory are not limited to intelligence and (counter)-terrorism disciplines. Expanding on notions of power, future research might find relevance for this work and social and power control theories (Fiske, 1996) (Dowding, 2011), balance of power theory, and power dependence relations (Emerson, 1993). This research thus concludes with an encouragement for further inquiry to expand on themes of VNSAs' intelligence and the role of intelligence and confidence in power and control relations.

Bibliography

al-Qaeda, n.d. *Declaration of Jihad Against the Country's Tyrants,* s.l.: s.n.

Anonymous, n.d. *Analysis of the State of ISI,* s.l.: Combating Terrorism Center at West Point.

Anzalone, C., 2014. The Life and Death of Al-Shabab Leader Ahmed Godane. *CTC Sentinel,* 7(9), pp. 19-22.

Anzalone, C., 2016. The Resilience of al-Shabaab. *CTC Sentinel,* 9(4), pp. 13-20.

BBC, 2012. *Defections put militant al-Shabab on the run in Somalia.* s.l.:BBC.

BBC, 2013. *Nairobi siege: How the attack happened.* s.l.:BBC.

BBC, 2016. *Paris attacks: Who were the attackers?.* s.l.:s.n.

Bell, J. B., 1994. The Armed Struggle and Underground Intelligence: An Overview. *Studies in Conflict & Terrorism,* 17(2), pp. 115-150.

Bennett, B. T., 2018. *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel.* Hoboken: John Wiley & Sons, Inc..

Bernarding, K. & Schuster, M., 2005. *Anatomy of a Terrorist Attack: An in-Depth Investigation Into the 1998 Bombings of the U.S. Embassies in Kenya and Tanzania,* Pittsburgh: Matthew B. Ridgway Center for International Security Studies.

Bitton, R., 2019. Getting the right picture for the wrong reasons: intelligence analysis by Hezbollah and Hamas. *Intelligence and National Security,* 34(7), pp. 1027-1044.

Blanchard, L. P., 2013. *The September 2013 Terrorist Attack in Kenya: In Brief,* Washington, D.C.: Congressional Research Service.

Brackett, D. W., 1996. *Holy terror : Armageddon in Tokyo.* New York: Weatherhill.

Bramford, B. W. C., 2005. The role and effectiveness of intelligence in Northern Ireland. *Intelligence and National Security,* 20(4), pp. 581-607.

Breakspear, A., 2013. A New Definition of Intelligence. *Intelligence and National Security,* 28(5), pp. 678-693.

Brisard, J.-C., 2015. The Paris Attacks and the Evolving Islamic State Threat to France. *CTC Sentinel,* 8(11), pp. 5-9.

Brisard, J.-C. & Jackson, K., 2016. The Islamic State's External Operations and the French-Belgian Nexus. *CTC Sentinel,* 9(11), pp. 8-15.

Butime, H. R., 2014. *The Lay-Out of Westgate Mall and its Significance in the Westgate Mall Attack in Kenya.* s.l.:Small Wars Journal.

Callimachi, R., 2016. *How ISIS Built the Machinery of Terror Under Europe's Gaze.* s.l.:New York Times.

Center for International Security and Cooperation, 2019. *Al Shabaab.* [Online] Available at: https://cisac.fsi.stanford.edu/mappingmilitants/profiles/al-shabaab

Clark, R. M., 2013. Perspectives on Intelligence Collection. *Journal of U.S. Intelligence Studies,* 20(2), pp. 47-53.

Clark, R. M., 2017. *Intelligence Analysis: A Target-Centric Approach.* Los Angeles: CQ Press.

Comune di Bologna, 2021. *Associazione tra i Familiari delle Vittime della Strage della Stazione di Bologna del 2 Agosto 1980.* Bologna: s.n.

Counter-Extremism Project, 2021. *Al-Shabaab,* s.l.: Counter-Extremism Project.

Crowe, W. J. et al., 1999. *Report of the Accountability Review Boards on the Embassy Bombings in Nairobi and Dar es Salaam on August 7, 1998,* s.l.: Accountability Review Boards.

Cruickshank, P., 2015. *Inside the ISIS plot to attack the heart of Europe.* s.l.:CNN.

Cruickshank, P., 2017. *The inside story of the Paris and Brussels attacks.* s.l.: CNN.

Cruickshank, P., Lister, T. & Robertson, N., 2013. *Evidence suggests that Al-Shabaab is shifting focus to 'soft' targets.* s.l.:CNN.

Dowding, K., 2011. Power as control theory. In: *Encyclopedia of power.* s.l.:SAGE Publications, pp. 505-508.

Emerson, R., 1993. Power-Dependence Relations. In: *Power in Modern Societies.* Milton Park: Routledge, pp. 31-41.

Europol, 2016. *Changes in modus operandi of Islamic State Terrorist Attacks,* The Hague: Europol.

Federal Bureau of Investigation (FBI), 1998. *Bombings of the Embassies of the United States of America at Nairobi, Kenya and Dar Es Salaam, Tanzania: Declassified Summary,* Washington, D.C.: U.S. Department of Justice.

Federation of American Scientists, n.d. *Section 4 Terrorist Intelligence Operations.* [Online] Available at: https://fas.org/irp/nsa/ioss/threat96/part04.htm

Fiske, S. T. a. D. E., 1996. Control, Interdependence, and Power: Understanding Social Cognition and Its Social Context. *European Review of Social Psychology,* Issue 1, pp. 31-61.

Gentry, J. A., 2016. Toward a Theory of Non-State Actors' Intelligence. *Intelligence and National Security,* Volume 4, pp. 465-489.

Gentry, J. A., 2018. Favorite INTs: how they develop, why they matter. *Intelligence and National Security,* 33(6), pp. 822-838.

Gentry, J. A. & Spencer, D. E., 2010. Colombia's FARC: A Portrait of Insurgent Intelligence. *Intelligence and National Security,* 25(4), pp. 453-478.

Gill, P., 2010. Theories of Intelligence. In: *The Oxford Handbook of National Security Intelligence.* Oxford: Oxford University Press, pp. 1-18.

Gill, P., 2018. The Way Ahead in Explaining Intelligence organization and process. *Intelligence and National Security,* 33(4), pp. 574-586.

Goshcha, C. E., 2007. Intelligence in a time of decolonization: The case of the Democratic Republic of Vietnam at war (1945-50). *Intelligence and National Security,* 22(1), pp. 100-138.

Harber, J. R., 2009. Unconventional Spies: The Counterintelligence Threat from Non-State Actors. *International Journal of Intelligence and Counterintelligence,* 22(2), pp. 221-236.

Harmon, C. C., 2000. Counter-Intelligence by Terror Groups. *Journal of Counterterrorism & Security Internatinal ,* pp. 1-5.

Heuer, R. J. & Pherson, R. H., 2011. *Structured Analytic Techniques for Intelligence Analysis.* Washington, D.C.: CQ Press.

Hoffman, B., 2006. *Inside Terrorism.* 2 ed. New York: Columbia University Press.

Holbrook, D., 2015. A critical analysis of the role of the internet in the preparation and planning of acts of terrorism. *Dynamics of Asymmetric Conflict,* 8(2), pp. 121-133.

Homeland Security Advisory Council; Paris Public Safety Delegation, 2016. *The Attacks on Paris: Lessons Learned,* Los Angeles: Homeland Security Advisory Council.

Howden, D., 2013. *Terror in Nairobi: the full story behind al-Shabaab's mall attack.* Nairobi: The Guardian.

Hulnick, A. S., 2006. What's wrong with the Intelligence Cycle. *Intelligence and National Security,* Volume 6, pp. 959-979.

Illardi, G. J., 2008. Al Qaeda's Operational Intelligence--A Prerequisite to Action. *Studies in Conflict & Terrorism,* 31(12), pp. 1072-1102.

Ilardi, G. J., 2009. Al-Qaeda's Counterintelligence Doctrine: The Pursuit of Operational Certainty and Control. *International Journal of Intelligence and CounterIntelligence,* 22(2), pp. 246-274.

Illardi, G. J., 2009. The 9/11 Attacks--A Study of Al Qaeda's Use of Intelligence and Counterintelligence. *Studies in Conflict & Terrorism,* 32(3).

Illardi, G. J., 2010. IRA Operational Intelligence: The Heardbeat of the War. *Small Wars & Insurgencies,* 21(2), pp. 331-358.

Illardi, J. G., 2010. Irish Republican Army Counterintelligence. *International Journal of Intelligence and Counterintelligence,* 23(1), pp. 1-26.

Irish Republican Army (IRA), 1965. *Handbook for Volunteers of the Irish Republican Army: Notes on Guerilla Warfare.* Dublin: s.n.

Jackson, P., 2010. On Uncertainty and the Limits of Intelligence. In: *The Oxford Handbook of National Security Intelligence.* Oxford: s.n., pp. 451-471.

Jackson, P., 2019. Intelligence in a modern insurgency: the case study of the Maoist insurgency in Nepal. *Intelligence and National Security,* 34(7), pp. 999-1013.

Jervis, R., 2012. The Politics and Psychology of Intelligence and Intelligence Reform. In: *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War.* s.l.:Cornell Paperbacks, pp. 156-196.

Johnson, L. K., 1986. Making the intelligence "Cycle" work. *International Journal of Intelligence and Counter Intelligence,* 1(4), pp. 1-23.

Joint Counterterrorism Assessment Team, n.d. *Counterterrorism Guide for Public Safety Personnel,* Washington, D.C: U.S. National Counterterrorism Center, U.S. Department of Homeland Security, and U.S. Department of Justice.

Joshi, M., 1996. On the razor's edge: The liberation tigers of Tamil Eelam. *Studies in Conflict & Terrorism,* 19(1), pp. 19-42¸.

Kansas Fusion Center, 2013. *Lessons Learned: Westgate Mall Attack,* s.l.: Kansas Fusion Center.

Kean, T. H. & Hamilton, L., 2004. *The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States.,* Washington, D.C.: National Commission on Terrorist Attacks upon the United States.

Kenney, M., 2008. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation.* State College: Pennsylvania University Press.

Kenney, M., 2010. Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists. *Terrorism and Political Violence,* 22(2).

Kent, S., 1949. *Strategic Intelligence for American World Policy.* Princeton: Princeton University Press.

Kerstetter, W. A., 1979. Terrorism and Intelligence. *Studies in Conflict and Terrorism,* 3(1-2), pp. 109-115.

Laqueur, W., 1987. *The Age of Terrorism.* Boston: Little, Brown and Company.

Lowenthal, M. M., 2020. *Intelligence: From Secrets to Policy.* Thousand Oaks: CQ Press.

Magee, A. C., 2010. Countering Nontraditional HUMINT Collection Threats. *International Journal of Intelligence and Counterintelligence,* 23(3), pp. 509-520.

Marrin, S., 2017. Understanding and improving intelligence analysis by learning from other disciplines. *Intelligence and National Security,* 32(5), pp. 539-547.

Marrin, S., 2018. Evaluating intelligence theories: current state of play. *Intelligence and National Security,* 33(4), p. 479.

Marrin, S. & Torres, E., 2017. Improving how to think in intelligence analysis and medicine. *Intelligence and National Security,* 32(5), pp. 649-662.

McConnell, T., 2014. *'Close Your Eyes and Pretend to be Dead'.* s.l.:Foreign Policy.

Mehta, N., 2015. *What we can learn from Paris.* s.l.: India Times.

Menkhaus, K., 2014. Al-Shabab’s Capabilities Post-Westgate. *CTC Sentinel,* 7(2), pp. 4-9.

Mirgani, S., 2017. *Target Markets--International Terrorism Meets Global Capitalism in the Mall.* Verlag: Center for International and Regional Studies.

Moloney, J. a. M. D., 2019. The Paris Terrorist Attacks: Implications for First Responders. *Journal of High Threat and Austere Medicine,* pp. 1-8.

Monaghan, R., 2019. Loyalist supergrass trials: an opportunity for open source intelligence?. *Intelligence and National Security,* 34(7), pp. 1014-1026.

New York Police Department, 2013. *Analysis of Al-Shabaab's Attack at the Westgate Mall in Nairobi, Kenya,* New York: New York Police Department.

Noël, S. et al., 2018. Lessons learned from Paris and Nice. *ISBT Science Series,* Volume 13, p. 35–46.

O'Brien, K. A., 2008. Assessing Hostile Reconnaissance and Terrorist Intelligence Activities. *The RUSI Journal,* 153(5), pp. 34-39.

Okari, D., 2014. *Kenya's Westgate attack: Unanswered questions one year on.* Nairobi: BBC.

Olson, K. B., 1999. Aum Shinrikyo: Once and Future Threat?. *Emerging Infectious Diseases,* Volume 4, pp. 513-516.

Petrich , K. & Donnelly, P., 2019. Worth Many Sins: Al-Shabaab's Shifting Relationship with Kenyan Women. *Small Wars & Insurgencies,* Volume 30.

Petrich, K., 2018. *Al-Shabaab's Mata Hari Network.* s.l.:War on the Rocks.

Pherson Associates, LLC, 2016. *Handbook of Analytic Tools and Techniques.* Reston: Pherson Associates, LLC.

Rabasa, A., 2006. Al-Qaeda's Operational Planning Cycle. In: *Beyond Al-Qaeda: The Global Jihadist Movement.* Santa Monica: RAND Corporation, pp. 63-68.

Random, M., 1958. Intelligence as a Science. *Studies in Intelligence,* 2(2).

Ressa, M., 2003. *Seeds of Terror.* New York: Free Press.

Reuters, 2015. *Timeline of Paris attacks according to public prosecutor.* Paris: Reuters.

Richards, J., 2014. *An Institutional History of the Liberation Tigers of Tamil Eelam (LTTE),* Geneva: The Graduate Institute of Geneva: The Centre on Conflict, Development and Peacebuilding.

Roble, M. A., 2013. Somalia's al-Shabaab Movement Turns on Itself. *Terrorism Monitor,* 11(16).

Romyn, D. & Mark, K., 2014. Terrorists' planning of attacks: a simulated 'red-team' investigation into decision-making. *Psychology, Crime & Law,* 20(5), pp. 480-496.

Rotella, S., 2016. *U.S. Identifies Key Player in ISIS Attacks on Europe.* s.l.:ProPublica.

Ryan, C. P., 2018. What is a complex coordinated attack (CCA)?. *Homeland Security Today,* January.pp. 1-13.

Shulsky, A. N. & Schmitt, G. A., 2002. *Silent Warfare: Understanding the World of Intelligence.* 3 ed. Dulles: Potomac Books, Inc..

Smith, B. L., Roberts, P. & Damphouse, K. R., 2017. The Terrorists' Planning Cycle: Patterns of Pre-incident Behavior. In: *The Handbook of the Criminology of Terrorism.* West Sussex: Wiley Blackwell, pp. 62-76.

Speckhard, A. & Ellenberg, M. D., 2020. ISIS in Their Own Words: Recruitment History, Motivations for Joining, Travel, Experience in ISIS, and Disillusionment over Time--Analysis of In-depth Interviews of ISIS Returnees, Defectors and Prisoners. *Journal of Strategic Security,* 13(1), pp. 82-127.

Speckhard, A. & Shajkovci, A., 2019. The Jihad in Kenya: Understanding Al-Shabaab Recruitment and Terrorist Activity inside Kenya—in Their Own Words. *African Security,* 12(1), pp. 3-61.

Speckhard, A. & Yayla, A. S., 2015. Eyewitness Accounts from Recent Defectors from Islamic State: Why They Joined, What They Saw, Why They Quit. *Perspectives on Terrorism,* 9(6), pp. 95-118.

Speckhard, A. & Yayla, A. S., 2017. The ISIS Emni: Origins and Inner Workings of ISIS's Intelligence Apparatus. *Perspectives on Terrorism,* 11(1), pp. 2-16.

Strachan-Morris, D., 2019a. Developing Theory on the Use of Intelligence by Non-State Actors: Five Case Studies on Insurgent Intelligence. *Intelligence and National Security,* 34(7), pp. 980-984.

Strachan-Morris, D., 2019b. The use of intelligence by insurgent groups: the North Vietnamese in the Second Indochina War as a case study. *Intelligence and National Security,* 34(7), pp. 985-998.

Stratfor, 2009. *The Terrorist Attack Cycle,* s.l.: Stratfor Global Intelligence.

Stratfor, n.d. *Understanding the Attack Cycle and Its Vulnerabilities,* s.l.: Stratfor Global Intelligence.

Suc, M., 2017a. How the Islamic State's Secret Services Hunt Down Informers. *Mediapart,* September.

Suc, M., 2017b. The Covert Operations Behind Islamic State's Terror Campaign in Europe. *Mediapart,* September.

Suc, M., 2017c. The Dark World of the Islamic State Group's Secret Services. *Mediapart,* August.

Suc, M., 2017d. The Threat From Islamic State's 'Fifth Column' in Europe. *Mediapart,* November.

Tantalakis, E., 2019. Insurgents' intelligence network and practices during the Greek Civil War. *Intelligence and National Security,* 34(7), pp. 1045-1063.

Thiranagama, S., 2010. In Praise of Traitors: Intimacy, Betrayal, and the Sri Lankan Tamil Community. In: T. Kelly & S. Tiranagama, eds. *Traitors, Suspicion, Intimacy and the Ethics of State-building.* Philadelphia: University of Pennsylvania Press, p. 126–149.

Torres-Soriano, M. R., 2019. How Do Terrorists Choose Their Targets for an Attack? The View from Inside an Independent Cell. *Terrorism and Political Violence,* pp. 1-15.

Tota, A. L., 2013. How to Transform a ‘Place of Violence’ into a ‘Space of Collective Remembering’: Italy and its Traumatic Past.. *Journal of Terrorism Research,* 4(1).

United Nations Office on Drugs and Crime, 2012. *The Use of the Internet for Terrorist Purposes,* Vienna: United Nations.

United Nations Security Council, 2013. *Report of the Monitoring Group on Somalia and Eritrea pursuant to Security Council resolution 2060 (2012): Somalia,* Geneva: United Nations Security Council.

United States Committee on Foreign Relations, 2001. *The Global Reach of Al-Qaeda: Hearing before the Subcommittee on International Operations and Terrorism of the Committee on Foreign Relations.* Washington, D.C.: s.n.

United States District Court Southern District of New York, 1998. *United States of America v. Usama bin Laden S(7) 98 Cr. 1023 (LBS) Indictment.* New York: s.n.

Vaux-Motnagny, N., 2020. *Trial opens for failed Daesh attack on French church.* s.l.:Arab News.

Vidino, L., Marone, F. & Entenmann, E., 2017. *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West.* Milan: Ledizioni LediPublishing.

Wagner, A., 2007. Intelligence for Counter-Terrorism: Technology and Methods. *Journal of Policing, Intelligence and Counter Terrorism,* 2(2), pp. 48-61.

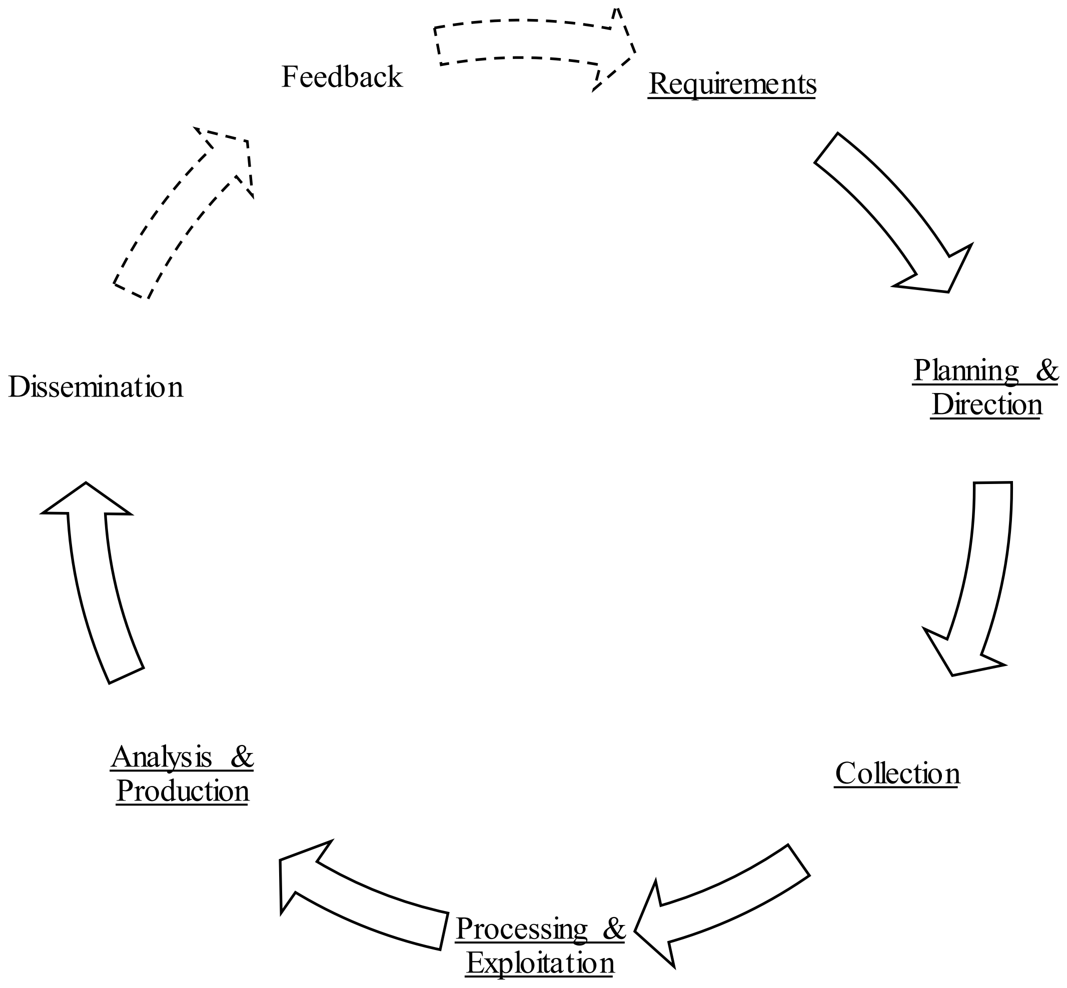
Warner, M., 2002. Wanted: A Defintion of 'Intelligence'. *Studies in Intelligence,* 46(3), pp. 15-22.

Weber, M., 2015. *Rationalism and Modern Society.* New York: Palgrave Books.

Wright, L., 2006. *The Looming Tower: Al-Qaeda and the Road to 9/11.* New York: Alfred A. Knopf.

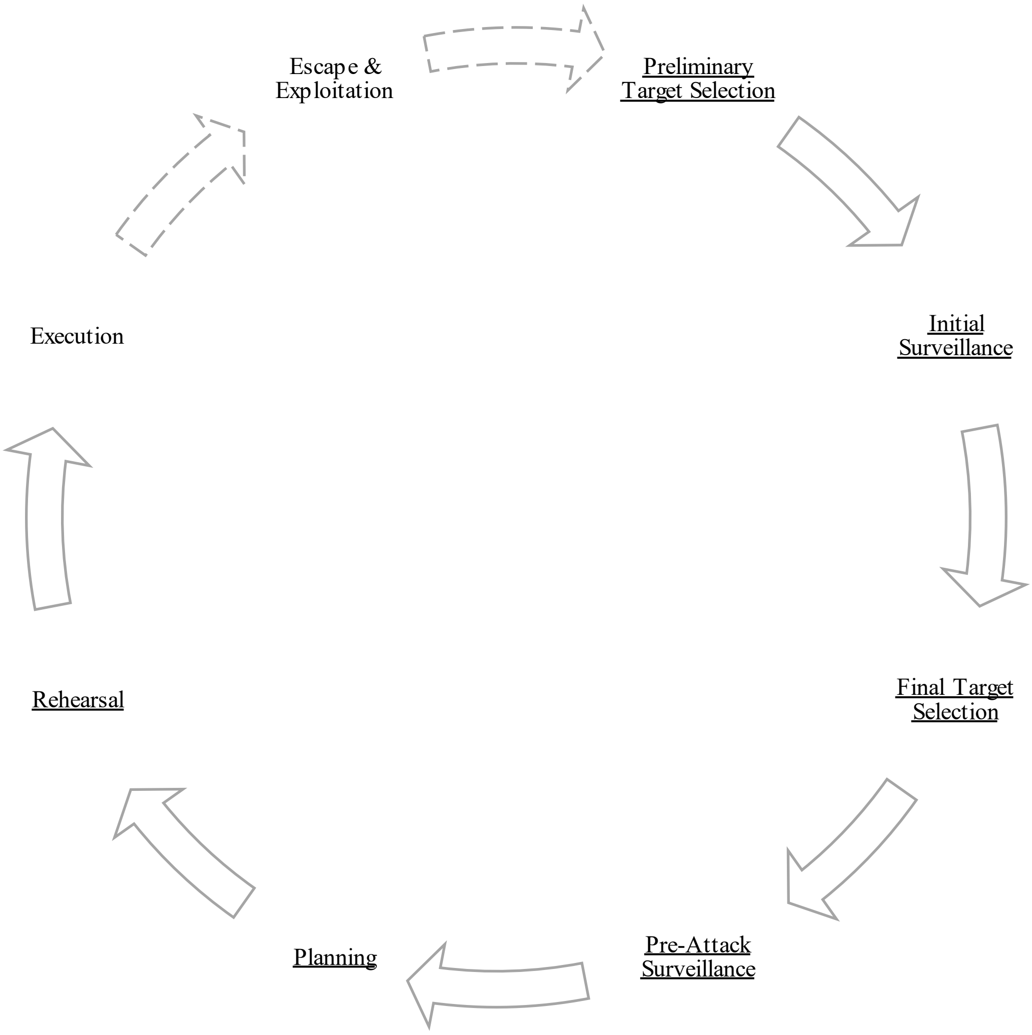
Appendix

Fig. 1



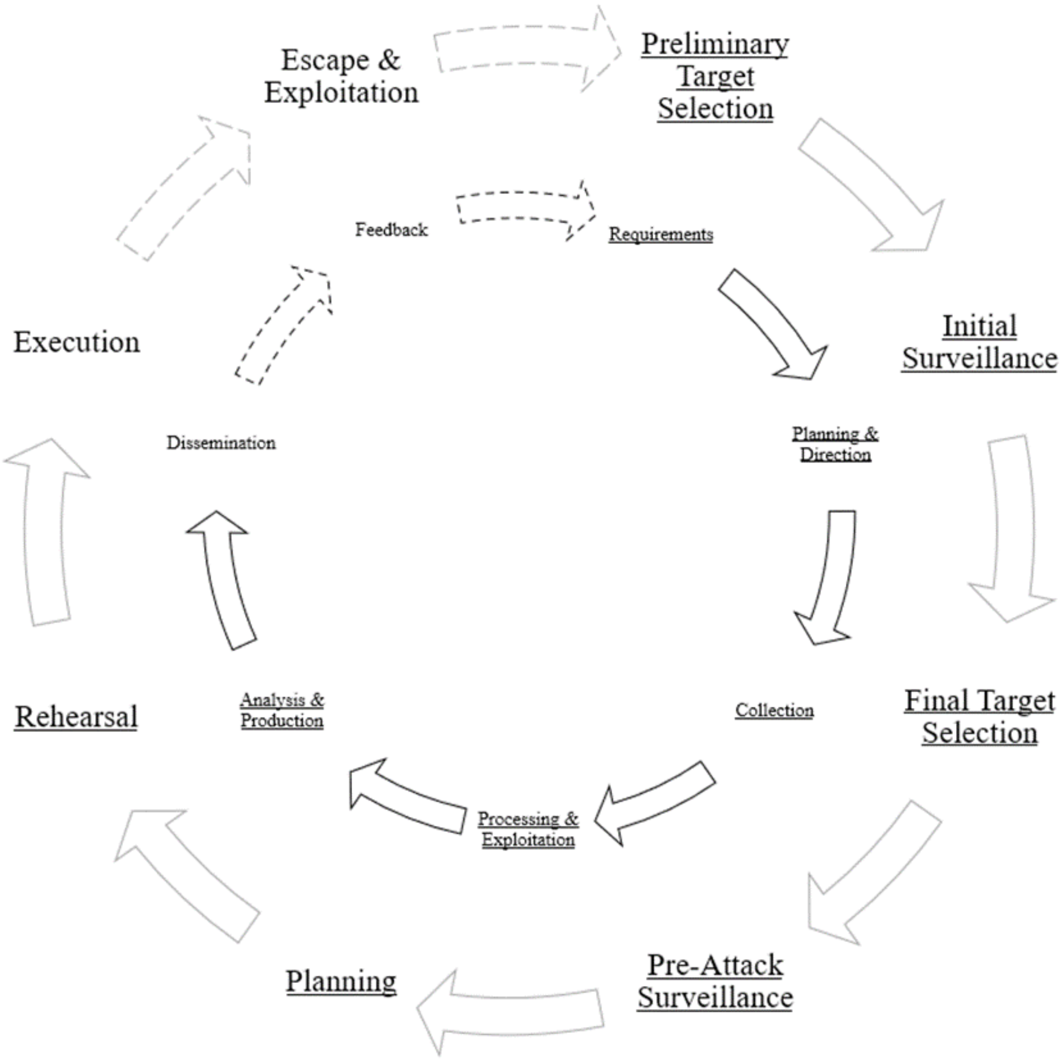
Source: *Author. Traditional Intelligence Cycle*

Fig. 2



Source: *Author. Terrorist Attack Cycle*

Fig. 3



Source: *Author. Correlations between the Intelligence Cycle (IC) (inner) and the Terrorist Attack Cycle (TAC) (outer)*

Fig. 4

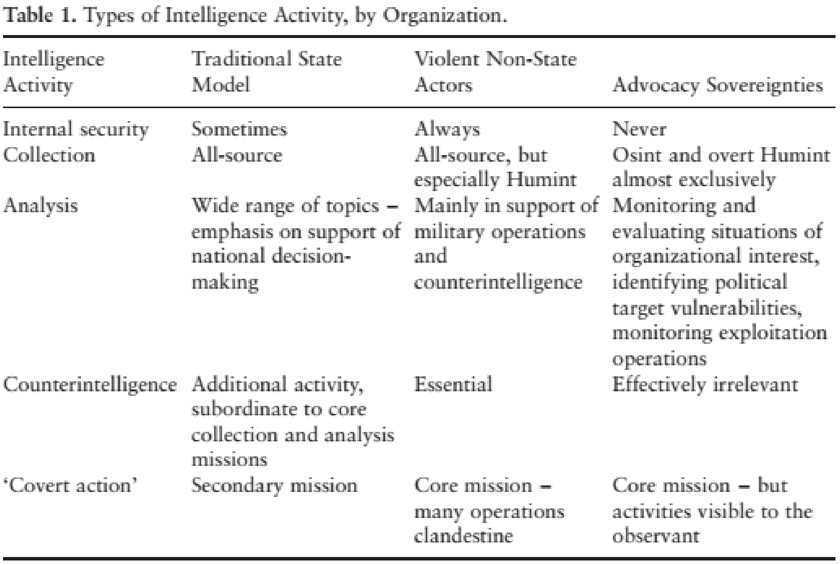
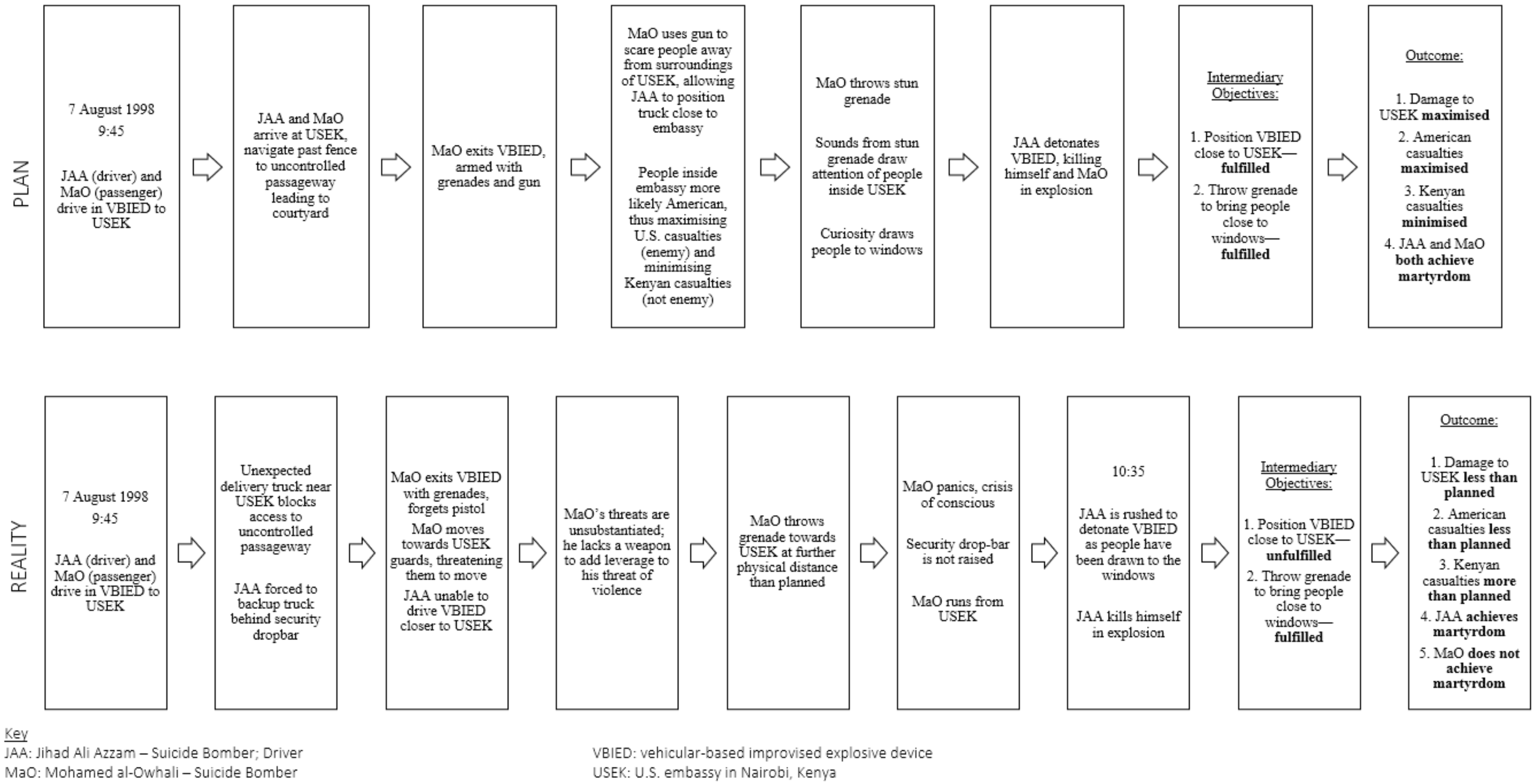


Table 1. Types of Intelligence Activity, by Organization.

Intelligence Activity	Traditional State Model	Violent Non-State Actors	Advocacy Sovereignties
Internal security	Sometimes	Always	Never
Collection	All-source	All-source, but especially Humint	Osint and overt Humint almost exclusively
Analysis	Wide range of topics – emphasis on support of national decision-making	Mainly in support of military operations and counterintelligence	Monitoring and evaluating situations of organizational interest, identifying political target vulnerabilities, monitoring exploitation operations
Counterintelligence	Additional activity, subordinate to core collection and analysis missions	Essential	Effectively irrelevant
'Covert action'	Secondary mission	Core mission – many operations clandestine	Core mission – but activities visible to the observant

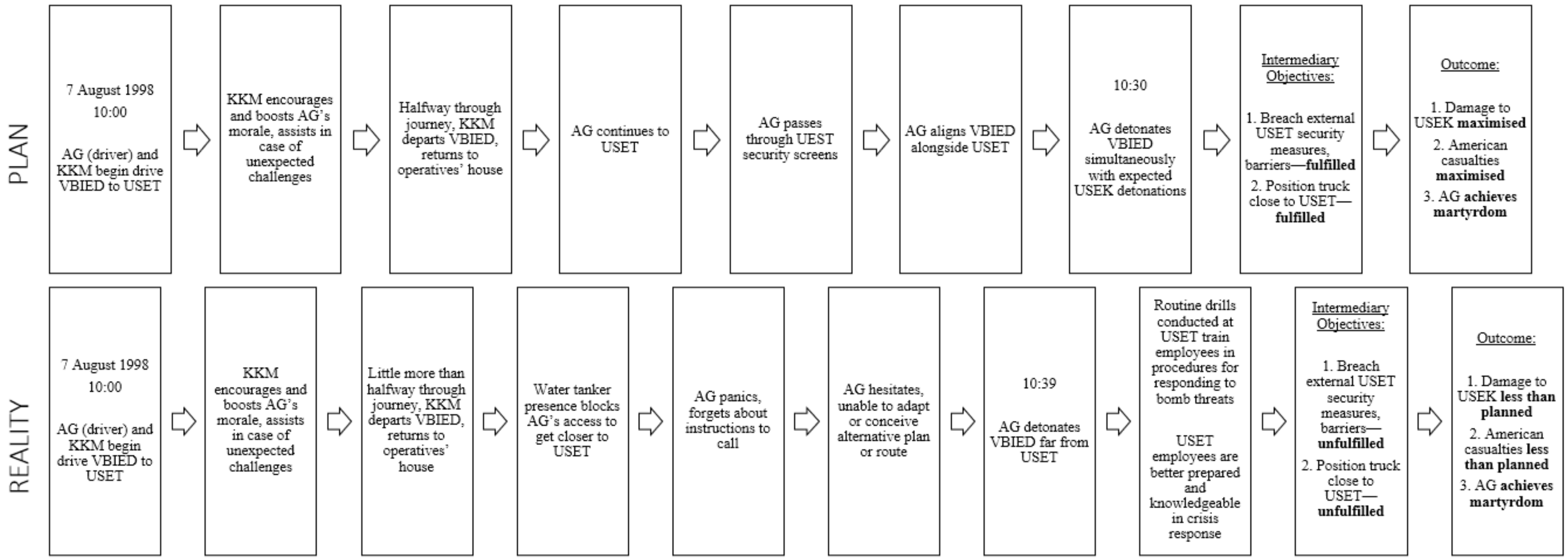
Source: *Gentry, J. A., 2016. Toward a Theory of Non-State Actors' Intelligence. Intelligence and National Security, 4, pp. 465-489.*

Fig. 5


PLAN
7 August 1998 9:45 JAA (driver) and MaO (passenger) drive in VBIED to USEK
JAA and MaO arrive at USEK, navigate past fence to uncontrolled passageway leading to courtyard
MaO exits VBIED, armed with grenades and gun
MaO uses gun to scare people away from surroundings of USEK, allowing JAA to position truck close to embassy
People inside embassy more likely American, thus maximising U.S. casualties (enemy) and minimising Kenyan casualties (not enemy)
MaO throws stun grenade
Sounds from stun grenade draw attention of people inside USEK
Curiosity draws people to windows
JAA detonates VBIED, killing himself and MaO in explosion
Intermediary Objectives:
1. Position VBIED close to USEK—fulfilled
2. Throw grenade to bring people close to windows—fulfilled
Outcome:
1. Damage to USEK maximised
2. American casualties maximised
3. Kenyan casualties minimised
4. JAA and MaO both achieve martyrdom
REALITY
7 August 1998 9:45 JAA (driver) and MaO (passenger) drive in VBIED to USEK
Unexpected delivery truck near USEK blocks access to uncontrolled passageway
JAA forced to backup truck behind security dropbar
MaO exits VBIED with grenades, forgets pistol
MaO moves towards USEK guards, threatening them to move
JAA unable to drive VBIED closer to USEK
MaO's threats are unsubstantiated; he lacks a weapon to add leverage to his threat of violence
MaO throws grenade towards USEK at further physical distance than planned
MaO panics, crisis of conscious
Security drop-bar is not raised
MaO runs from USEK
10:35
JAA is rushed to detonate VBIED as people have been drawn to the windows
JAA kills himself in explosion
Intermediary Objectives:
1. Position VBIED close to USEK—unfulfilled
2. Throw grenade to bring people close to windows—fulfilled
Outcome:
1. Damage to USEK less than planned
2. American casualties less than planned
3. Kenyan casualties more than planned
4. JAA achieves martyrdom
5. MaO does not achieve martyrdom
Key
JAA: Jihad Ali Azzam – Suicide Bomber; Driver
MaO: Mohamed al-Owhali – Suicide Bomber
VBIED: vehicular-based improvised explosive device
USEK: U.S. embassy in Nairobi, Kenya

Source*: Author. The Attacks on the Kenyan U.S. Embassy as Planned and Executed*

Fig. 6


PLAN
7 August 1998 10:00 AG (driver) and KKM begin drive VBIED to USET
KKM encourages and boosts AG's morale, assists in case of unexpected challenges
Halfway through journey, KKM departs VBIED, returns to operatives' house
AG continues to USET
AG passes through UEST security screens
AG aligns VBIED alongside USET
10:30 AG detonates VBIED simultaneously with expected USEK detonations
Intermediary Objectives: 1. Breach external USET security measures, barriers—fulfilled 2. Position truck close to USET—fulfilled
Outcome: 1. Damage to USEK maximised 2. American casualties maximised 3. AG achieves martyrdom
REALITY
7 August 1998 10:00 AG (driver) and KKM begin drive VBIED to USET
KKM encourages and boosts AG's morale, assists in case of unexpected challenges
Little more than halfway through journey, KKM departs VBIED, returns to operatives' house
Water tanker presence blocks AG's access to get closer to USET
AG panics, forgets about instructions to call
AG hesitates, unable to adapt or conceive alternative plan or route
10:39 AG detonates VBIED far from USET
Routine drills conducted at USET train employees in procedures for responding to bomb threats USET employees are better prepared and knowledgeable in crisis response
Intermediary Objectives: 1. Breach external USET security measures, barriers—unfulfilled 2. Position truck close to USET—unfulfilled
Outcome: 1. Damage to USEK less than planned 2. American casualties less than planned 3. AG achieves martyrdom

Key

AG: Ahmed the German, real name Hamden Khalif Allah Awad – Suicide Bomber; Driver

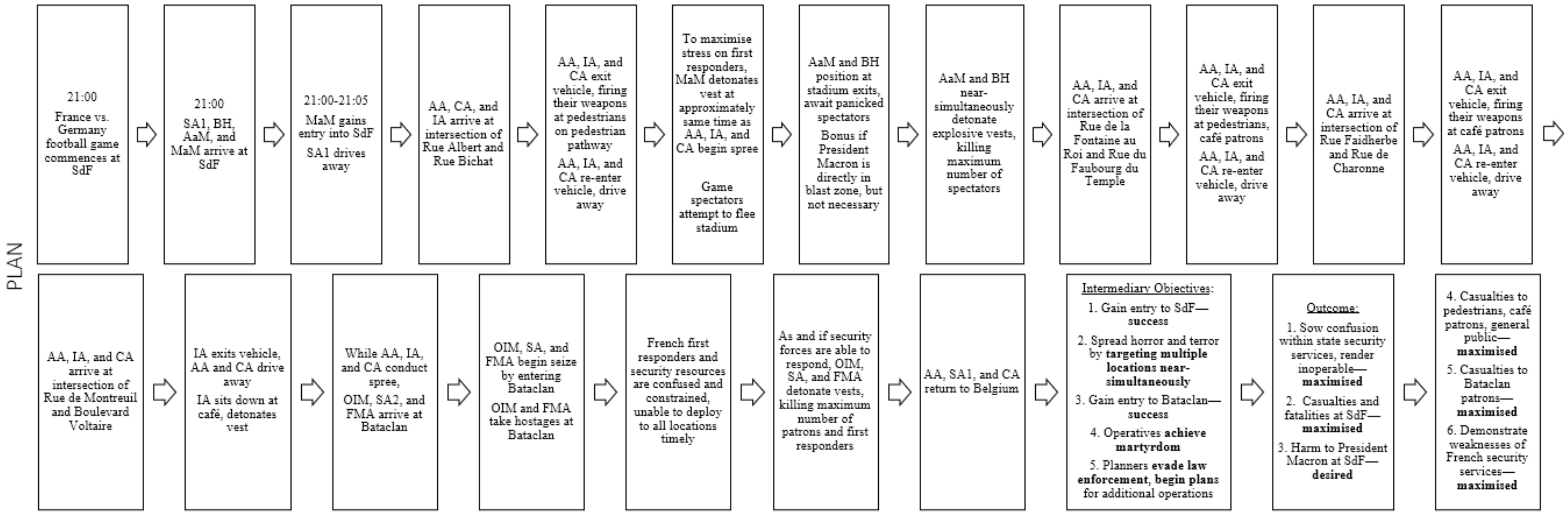
KKM: Khalfan Khamis Muhamed; Driver

VBIED: vehicular-based improvised explosive device

USET: U.S. embassy in Dar es Salaam, Tanzania

Source*: Author. The Attacks on the Tanzanian U.S. Embassy as Planned and Executed*

Fig. 7


PLAN
21:00 France vs. Germany football game commences at SdF
21:00 SA1, BH, AaM, and MaM arrive at SdF
21:00-21:05 MaM gains entry into SdF SA1 drives away
AA, CA, and IA arrive at intersection of Rue Albert and Rue Bichat
AA, IA, and CA exit vehicle, firing their weapons at pedestrians on pedestrian pathway AA, IA, and CA re-enter vehicle, drive away
To maximise stress on first responders, MaM detonates vest at approximately same time as AA, IA, and CA begin spree Game spectators attempt to flee stadium
AaM and BH position at stadium exits, await panicked spectators Bonus if President Macron is directly in blast zone, but not necessary
AaM and BH near-simultaneously detonate explosive vests, killing maximum number of spectators
AA, IA, and CA arrive at intersection of Rue de la Fontaine au Roi and Rue du Faubourg du Temple
AA, IA, and CA exit vehicle, firing their weapons at pedestrians, café patrons AA, IA, and CA re-enter vehicle, drive away
AA, IA, and CA arrive at intersection of Rue Faidherbe and Rue de Charonne
AA, IA, and CA exit vehicle, firing their weapons at café patrons AA, IA, and CA re-enter vehicle, drive away
AA, IA, and CA arrive at intersection of Rue de Montreuil and Boulevard Voltaire
IA exits vehicle, AA and CA drive away IA sits down at café, detonates vest
While AA, IA, and CA conduct spree, OIM, SA2, and FMA arrive at Bataclan
OIM, SA, and FMA begin seize by entering Bataclan OIM and FMA take hostages at Bataclan
French first responders and security resources are confused and constrained, unable to deploy to all locations timely
As and if security forces are able to respond, OIM, SA, and FMA detonate vests, killing maximum number of patrons and first responders
AA, SA1, and CA return to Belgium
Intermediary Objectives: 1. Gain entry to SdF—**success** 2. Spread horror and terror by **targeting multiple locations near-simultaneously** 3. Gain entry to Bataclan—**success** 4. Operatives **achieve martyrdom** 5. Planners **evade law enforcement, begin plans** for additional operations
Outcome: 1. Sow confusion within state security services, render inoperable—**maximised** 2. Casualties and fatalities at SdF—**maximised** 3. Harm to President Macron at SdF—**desired**
4. Casualties to pedestrians, café patrons, general public—**maximised** 5. Casualties to Bataclan patrons—**maximised** 6. Demonstrate weaknesses of French security services—**maximised**

Key

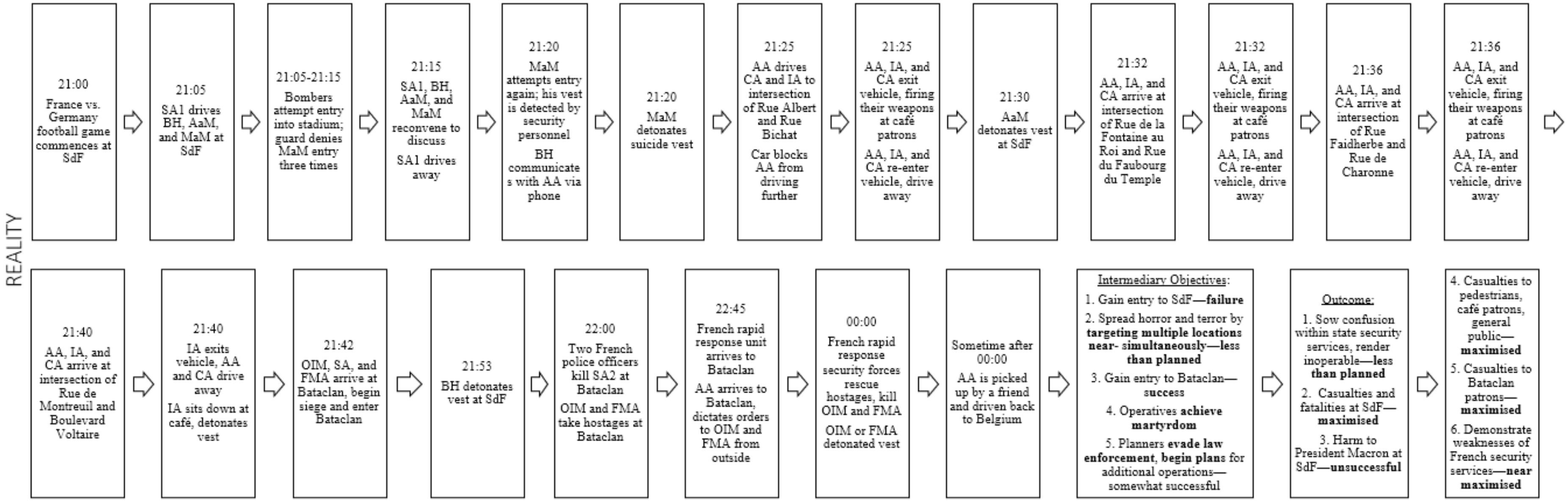
SdF: Stade de France
SA1: Salah Abdeslam; Driver
BH: Bilal Hadfi; Suicide Bomber
AaM: Ahmad al-Mohammed; Suicide Bomber

MaM: M al-Mohammed; Suicide Bomber
AA: Abdelhamid Abaaoud; Planner; Driver; Shooter
CA: Chakib Akrouh Shooter
IA: Ibrahim Abdeslam; Shooter; Suicide Bomber

OIM: Omar Ismail Mostefai; Shooter; Suicide Bomber
SA2: Samy Amimour; Shooter; Suicide Bomber
FMA: Foued Mohamed-Aggad; Shooter; Suicide Bomber

Source*: Author. The Paris Attacks as Planned*

Fig. 8



21:00 France vs. Germany football game commences at SdF

21:05 SA1 drives BH, AaM, and MaM at SdF

21:05-21:15 Bombers attempt entry into stadium; guard denies MaM entry three times

21:15 SA1, BH, AaM, and MaM reconvene to discuss

SA1 drives away

21:20 MaM attempts entry again; his vest is detected by security personnel

BH communicates with AA via phone

21:20 MaM detonates suicide vest

21:25 AA drives CA and IA to intersection of Rue Albert and Rue Bichat

Car blocks AA from driving further

21:25 AA, IA, and CA exit vehicle, firing their weapons at café patrons

AA, IA, and CA re-enter vehicle, drive away

21:30 AaM detonates vest at SdF

21:32 AA, IA, and CA arrive at intersection of Rue de la Fontaine au Roi and Rue du Faubourg du Temple

21:32 AA, IA, and CA exit vehicle, firing their weapons at café patrons

AA, IA, and CA re-enter vehicle, drive away

21:36 AA, IA, and CA arrive at intersection of Rue Faidherbe and Rue de Charonne

21:36 AA, IA, and CA exit vehicle, firing their weapons at café patrons

AA, IA, and CA re-enter vehicle, drive away

21:40 AA, IA, and CA arrive at intersection of Rue de Montreuil and Boulevard Voltaire

21:40 IA exits vehicle, AA and CA drive away

IA sits down at café, detonates vest

21:42 OIM, SA, and FMA arrive at Bataclan, begin siege and enter Bataclan

21:53 BH detonates vest at SdF

22:00 Two French police officers kill SA2 at Bataclan

OIM and FMA take hostages at Bataclan

22:45 French rapid response unit arrives to Bataclan

AA arrives to Bataclan, dictates orders to OIM and FMA from outside

00:00 French rapid response security forces rescue hostages, kill OIM and FMA

OIM or FMA detonated vest

Sometime after 00:00 AA is picked up by a friend and driven back to Belgium

Intermediary Objectives:

1. Gain entry to SdF—**failure**
2. Spread horror and terror by **targeting multiple locations near- simultaneously—less than planned**
3. Gain entry to Bataclan—**success**
4. Operatives **achieve martyrdom**
5. Planners **evade law enforcement**, **begin plans** for additional operations—somewhat successful

Outcome:

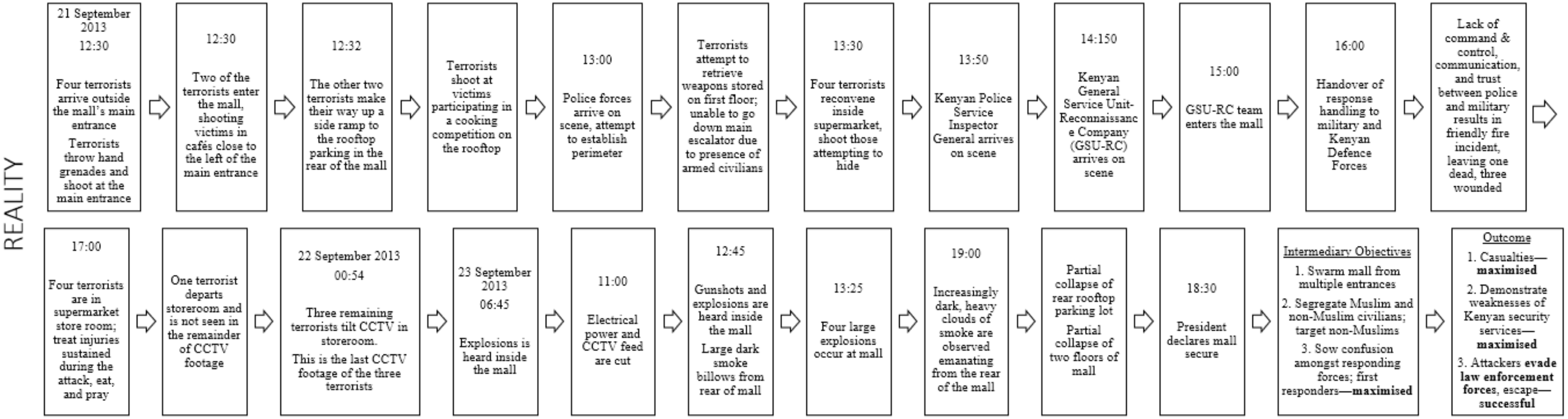
1. Sow confusion within state security services, render inoperable—**less than planned**
2. Casualties and fatalities at SdF—**maximised**
3. Harm to President Macron at SdF—**unsuccessful**
4. Casualties to pedestrians, café patrons, general public—**maximised**
5. Casualties to Bataclan patrons—**maximised**
6. Demonstrate weaknesses of French security services—**near maximised**

Key

SdF: Stade de France
SA1: Salah Abdeslam; Driver
BH: Bilal Hadfi; Suicide Bomber
AaM: Ahmad al-Mohammed; Suicide Bomber
MaM: M al-Mohammed; Suicide Bomber
AA: Abdelhamid Abaaoud; Planner; Driver; Shooter
CA: Chakib Akrouh Shooter
IA: Ibrahim Abdeslam; Shooter; Suicide Bomber
OIM: Omar Ismail Mostefai; Shooter; Suicide Bomber
SA2: Samy Amimour; Shooter; Suicide Bomber
FMA: Foued Mohamed-Aggad; Shooter; Suicide Bomber

Source*: Author. The Paris Attacks as Executed*

Fig. 9

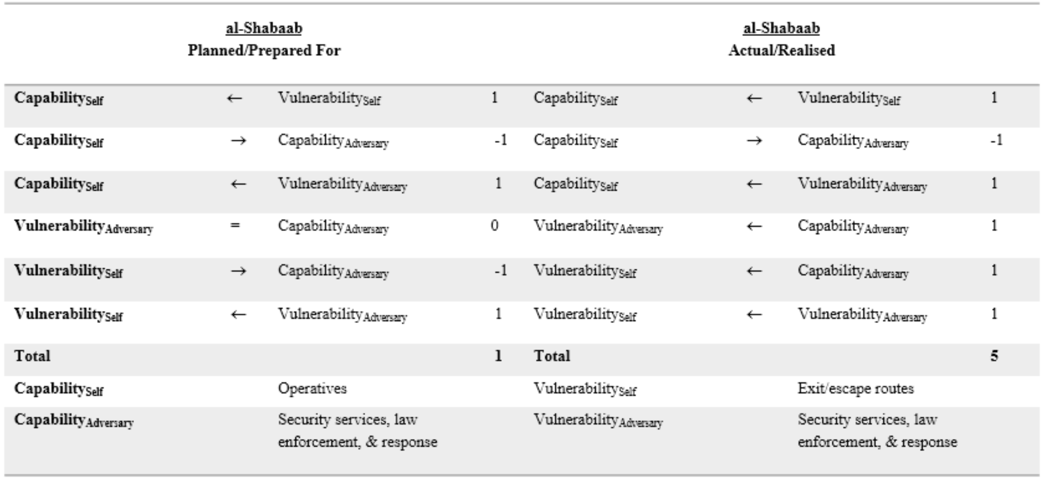

REALITY
21 September 2013 12:30 Four terrorists arrive outside the mall's main entrance Terrorists throw hand grenades and shoot at the main entrance
12:30 Two of the terrorists enter the mall, shooting victims in cafés close to the left of the main entrance
12:32 The other two terrorists make their way up a side ramp to the rooftop parking in the rear of the mall
Terrorists shoot at victims participating in a cooking competition on the rooftop
13:00 Police forces arrive on scene, attempt to establish perimeter
Terrorists attempt to retrieve weapons stored on first floor; unable to go down main escalator due to presence of armed civilians
13:30 Four terrorists reconvene inside supermarket, shoot those attempting to hide
13:50 Kenyan Police Service Inspector General arrives on scene
14:150 Kenyan General Service Unit-Reconnaissance Company (GSU-RC) arrives on scene
15:00 GSU-RC team enters the mall
16:00 Handover of response handling to military and Kenyan Defence Forces
Lack of command & control, communication, and trust between police and military results in friendly fire incident, leaving one dead, three wounded
17:00 Four terrorists are in supermarket store room; treat injuries sustained during the attack, eat, and pray
One terrorist departs storeroom and is not seen in the remainder of CCTV footage
22 September 2013 00:54 Three remaining terrorists tilt CCTV in storeroom. This is the last CCTV footage of the three terrorists
23 September 2013 06:45 Explosions is heard inside the mall
11:00 Electrical power and CCTV feed are cut
12:45 Gunshots and explosions are heard inside the mall Large dark smoke billows from rear of mall
13:25 Four large explosions occur at mall
19:00 Increasingly dark, heavy clouds of smoke are observed emanating from the rear of the mall
Partial collapse of rear rooftop parking lot Partial collapse of two floors of mall
18:30 President declares mall secure
Intermediary Objectives 1. Swarm mall from multiple entrances 2. Segregate Muslim and non-Muslim civilians; target non-Muslims 3. Sow confusion amongst responding forces; first responders—**maximised**
Outcome 1. Casualties—**maximised** 2. Demonstrate weaknesses of Kenyan security services—**maximised** 3. Attackers **evade law enforcement forces**, escape—**successful**

Source*: Author. The Westgate Mall Attack as Executed*

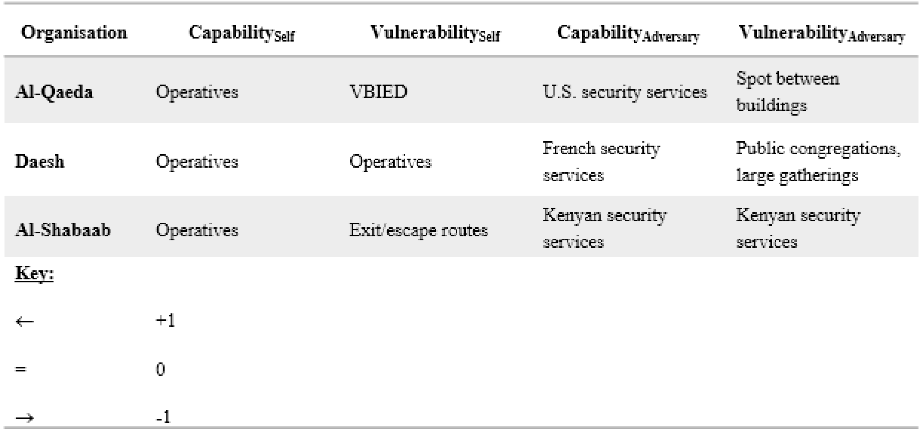
Fig. 10

al-Qaeda **Planned/Prepared For**				al-Qaeda **Actual/Realised**			
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Self}}$	1	Capability$_{\text{Self}}$	→	Vulnerability$_{\text{Self}}$	-1
Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Capability$_{\text{Self}}$	→	Vulnerability$_{\text{Adversary}}$	-1
Vulnerability$_{\text{Adversary}}$	←	Capability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Adversary}}$	→	Capability$_{\text{Adversary}}$	-1
Vulnerability$_{\text{Self}}$	←	Capability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	←	Capability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	→	Vulnerability$_{\text{Adversary}}$	-1
Total			**5**	**Total**			**-4**
Capability$_{\text{Self}}$		Operatives		Vulnerability$_{\text{Self}}$		VBIED	
Capability$_{\text{Adversary}}$		Security services, law enforcement, & response		Vulnerability$_{\text{Adversary}}$		Passageways/close access to buildings	

Daesh **Planned/Prepared For**				Daesh **Actual/Realised**			
Capability$_{\text{Self}}$	=	Vulnerability$_{\text{Self}}$	0	Capability$_{\text{Self}}$	→	Vulnerability$_{\text{Self}}$	-1
Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Capability$_{\text{Self}}$	=	Vulnerability$_{\text{Adversary}}$	0
Vulnerability$_{\text{Adversary}}$	←	Capability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Adversary}}$	=	Capability$_{\text{Adversary}}$	0
Vulnerability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Vulnerability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	→	Vulnerability$_{\text{Adversary}}$	0
Total			**1**	**Total**			**-3**
Capability$_{\text{Self}}$		Operatives		Vulnerability$_{\text{Self}}$		Operatives	
Capability$_{\text{Adversary}}$		Security services, law enforcement, & response		Vulnerability$_{\text{Adversary}}$		Public, large congregations people	



al-Shabaab Planned/Prepared For				al-Shabaab Actual/Realised			
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Self}}$	1	Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Self}}$	1
Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Capability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1
Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Capability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Adversary}}$	=	Capability$_{\text{Adversary}}$	0	Vulnerability$_{\text{Adversary}}$	←	Capability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Self}}$	→	Capability$_{\text{Adversary}}$	-1	Vulnerability$_{\text{Self}}$	←	Capability$_{\text{Adversary}}$	1
Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1	Vulnerability$_{\text{Self}}$	←	Vulnerability$_{\text{Adversary}}$	1
Total			**1**	**Total**			**5**
Capability$_{\text{Self}}$		Operatives		Vulnerability$_{\text{Self}}$		Exit/escape routes	
Capability$_{\text{Adversary}}$		Security services, law enforcement, & response		Vulnerability$_{\text{Adversary}}$		Security services, law enforcement, & response	



Organisation	Capability$_{\text{Self}}$	Vulnerability$_{\text{Self}}$	Capability$_{\text{Adversary}}$	Vulnerability$_{\text{Adversary}}$
Al-Qaeda	Operatives	VBIED	U.S. security services	Spot between buildings
Daesh	Operatives	Operatives	French security services	Public congregations, large gatherings
Al-Shabaab	Operatives	Exit/escape routes	Kenyan security services	Kenyan security services
Key:				
←	+1			
=	0			
→	-1			

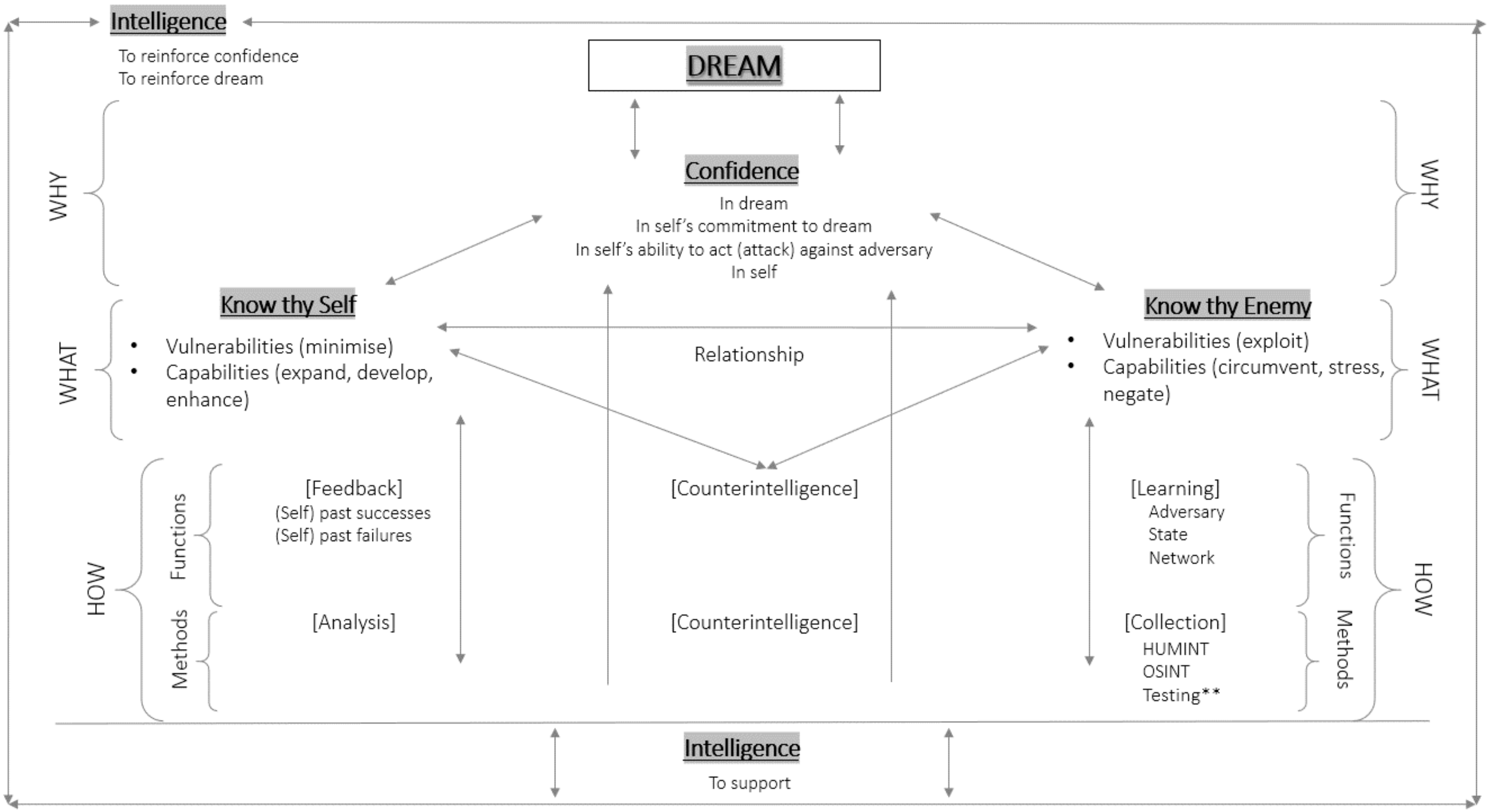
Source*: Author. Perceptions of Capabilities and Vulnerabilities in Terrorist Attacks*

Fig. 11

	Simultaneous	Cascading
Intent to Escape	**Target Market** Where: Local marketplace, outdoor bazaar When: Daily peak times How: Prepositioned VBIEDs or IEDs hidden in shopping bags, crates, boxes Why: IED/VBIED 'planters' able escape by assimilating into chaos of panicked crowd. IEDs hidden in shopping bags/crates will garner less suspicion. Fewer security personnel expected at a weekly/regular marketplace. Possibility to target multiple locations within marketplace Effects: Shoppers across marketplace affected, community in prolonged anxiety and fear of future attacks. Security services in the future will need to weigh devoting additional resources to tightening security at marketplaces (eg. bag and vehicle searches, metal detectors) with the public's concerns and desires to shop easily and in peace	**Moving Shot** Where: Multiple locations across region When: Night, Thursday-Sunday How: Use of firearms, grenades, throwable pipe-bombs or small IEDs; supported by getaway vehicles Why: Night offers potential of fewer obstacles (eg. vehicular traffic) barring movement in the attempt to escape and cascade the attack; darkness offers obscurity of identity, defining features of attackers/vehicle. Private 'getaway vehicle' likely offers greater security, speed, and flexibility in attack execution. More likely fewer security/emergency services available at night. Thursday-Sunday possibility for more people out of home, compared to work nights (note, varies by geographic/cultural contexts) Effects: Security services strained in effort to disperse across temporal region (inability to swarm) and possibility for confusion as reports of explosions in multiple areas appear to contradict one another/gain clarity of where to allocate resources most effectively and efficiently
No Intent to Escape	**Bull's Eye** Where: Government facility, military base When: Late morning, after start of standard operating hours; added benefit if hosting foreign guests/political leaders How: VBIED, IEDs, explosive belts/vests Why: Suicide attack more likely as escape is not a factor for consideration, as heightened presence of (armed) security personnel is expected. If foreign guests/political leaders are expected, multiple adversaries can be targeted, however, there will likely be greater security services, making access and escape challenging, hence suicide operations are seen as more strategic. Prior reconnaissance and/or positioning of barricades, weapons will be challenged Effects: Security services face embarrassment, ridicule, and critique as public perceptions question the ability of a government to provide security for its citizens if it is unable to protect its own assets/facilities	**Next Stop** Where: Bus, train, metro, other public transport infrastructures When: Rush hour, peak travel times How: Barricades to block escape; IEDs, explosive belts/vests Why: Public transport system will likely be a contained target (eg. bus, carriage) and/or block passages/routes for escape for both operatives and victims. Rush hour/peak travel times more likely opportunity for maximum degree of physical damage and psychologically disrupts public's routines. Suicide attack more likely as escape is not a factor for consideration, especially as exit routes will make escape less likely Effects: Disrupts and halts transportation networks as officials fear additional attacks. Security services strained in attempt to 'sweep' public transportation networks and remain one step ahead of an attack as it continues to unfold

Source*: Author. Terrorist Attack Options on the Considerations of the Sequence of Events and Intent to Escape*

Fig. 12



**"Testing" is understood as a method by which VNSA-Ts operate below the threshold of violence, yet, directly engage with a target or enemy prior to an attack, in a 'trial' to collect information. This includes any active, direct action that probes to acquire more information in particular about a particular target or audience. Examples include carrying weapons in the vicinity of a target site to gauge security guards' reactions, dropping/abandoning items to judge the public's reaction.

Source*: Author. Terrorist Intelligence and Confidence (TIC)*

IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

International Master in Security, Intelligence and Strategic Studies 2019/2021

Dissertation Archive Permission Form

I give the University of Glasgow and Charles University permission to archive an e-copy of my Master dissertation in a publicly available folder and to use it for educational purposes in the future.

Student Name (BLOCK LETTERS) OLIVIA (LIV) DORAK

Student Number: 2486209D

Student Signature: **Date: 20 July 2021**