# Emergent Teams for Complex Threats

*May 15th, 2020*

*Richard J. Cordes* [1,2]

(1) Remotor Consulting Group,
(2) Cognitive Security and Education Forum
richardj.cordes@gmail.com

*Daniel A. Friedman, PhD* [1,3]

(1) Remotor Consulting Group,
(3) University of California, Davis, Dept. of Entomology
danielarifriedman@gmail.com

A B S T R A C T

*While the underlying, fundamental principles of warfare have long remained unchanged, recent social and technological developments have necessitated new approaches to conflict management. Specifically, the introduction of nuclear weapons and the maintenance of large military budgets during peacetime in the latter half of the 20th century have changed the risk calculus of conflict among state and non-state actors. Consequently, the operating environment has changed. Extant, centralized actors have experienced new adversities such as ideological warfare and sustained low-intensity and gray zone conflict while new, decentralized participants have emerged and evolved. Nation states, as a part of normal operations, now have to contend with the potential for novel, emergent hazards from a myriad of Complex Threat Surfaces in littoral and other environments. We highlight how Complexity Science has been of use in the analysis of Complex Threat Surfaces in the military and within civilian organizations, particularly High Reliability Organisations or HROs. This paper discusses the intersection of Complexity Science and Military Science by focusing on analysis of counterinsurgency and counterterrorism operations. We highlight rapid reorganization, pooling collective expertise, and the assembly of novel organizational components as a potential basis for developing spontaneous expertise, actionable intelligence, and solutions to the aforementioned novel, emergent hazards.*

## Introduction

This paper uses a Complexity Science framework to understand how the rapid assembly of teams and successful counterinsurgency and related efforts are linked. Beginning with a vignette of the 2008 attack on Mumbai by Lashkar-e-Taiba, general ideas and trends in Military Science related to counterinsurgency efforts and Complex Threat Surfaces will be discussed. This introduction to Complex Threat Surfaces will be followed by a discussion of Complexity Science as an approach for modeling and de-risking Complex Threats. In alignment with literature on both High Reliability Organizations and Complexity Science, reorganization and adaptation are addressed as potential avenues for responding to novel, emergent problems. Finally, Rapid Team Assembly is presented at the intersection of Complexity and Military

Science as a basis for developing spontaneous expertise, actionable intelligence, and solutions to novel, emergent problems. We conclude with a discussion of best practices and opportunities for future work.

## Lessons from Mumbai

To understand how Complexity Science, the rapid assembly of teams, counterterrorism, counterinsurgency, and other related efforts are linked, we begin with a recollection of the 2008 attack on Mumbai. On November 23rd, 2008, ten men in their early twenties left the Pakistani port city of Karachi by boat. They carried light armament, some fire-starting material, fake passports, and satellite phones (Haberfeld & Hassell, 2009; PTI, 2020). They set out for Mumbai, the seventh most populous city in the world, a mega-city of more than fourteen million people, the capital of the Indian State Maharashtra (United Nations, 2018). Enroute, they hijacked a fishing vessel registered in Mumbai, murdered its crew (Haberfeld & Hassell, 2009; Marwaha, 2017), and forced the captain to re-introduce the vessel into normal fleet traffic (Kilcullen, 2012). On November 26th, seven kilometers from Mumbai's coastline, the captain was killed. With the vessel fully under control, the ten men begin their approach toward the shore. By 8:10 p.m. that evening, the group of ten split into two groups, one going ashore and the other continuing by boat. By 8:30 p.m., both groups have split again, resulting in five teams. Now dressed in casual clothes to blend with the local population, each of the five teams make their approach toward their respective targets (Haberfeld & Hassell, 2009; Marwaha, 2017; Shahrzad Rizvi & Kelly, 2015). By 9 p.m., IEDs (improvised explosive devices) had been left in the taxis which transported the individuals to these locations (Ministry of External Affairs India, 2009). Upon arriving, they maneuvered and fired indiscriminately into restaurants, train stations, and social establishments near their respective locations. At 9:38 p.m., a pair assaulted the Taj Mahal Hotel from the main lobby, twenty non-combatants were left dead within the first few minutes (Ministry of External Affairs India, 2009).

By 10 p.m. there were explosions at gas stations, civilians had been taken hostage, and police, accompanied by three senior counterterrorism agents, had not only been counterattacked but successfully ambushed before even arriving on the scene. The van they were ambushed in was then hijacked and used to carry out attacks with a surviving officer sitting paralyzed in the backseat (Burton & West, 2008; Haberfeld & Hassell, 2009). It is around this time that Zabiuddin Ansari, a phone-operator working from a command post in Pakistan made a call by satellite phone to a subunit which was hardening its position in a hotel. It is on this call that he states the following:

> *"Tell [the Indian Media] this is just the trailer. The real movie is yet to come"*

This message, in retrospect, could be viewed as hauntingly accurate . (Glanz et al., 2014; Haberfeld & Hassell, 2009; Ministry of External Affairs India, 2009;

PTI, 2020; Shahrzad Rizvi & Kelly, 2015). Despite the deployment of a counterterrorism force which had superior training, equipment, and support, the attackers, acting as semi-autonomous groups with minimal equipment, managed to keep a city of over fourteen million people under siege for three days. By the end of the conflict, 172 people were dead and 308 were wounded (Haberfeld & Hassell, 2009). Some background on the group and the basis for their relative success will be discussed.

The group responsible for training the young men in the attack was Lashkar-e-Taiba (Haberfeld & Hassell, 2009), meaning "The Army of the Pure" (Spindlove & Simonsen, 2010; Tankel, 2013). Lashkar-e-Taiba is primarily concerned with removing Indian military presence from Jammu and Kashmir and is composed of religious radicals affiliated with an ultra-orthodox form of Sunni Islam. In compliance with their beliefs, the group is known for foregoing suicide missions, in favor of "dare-devil" missions (Haberfeld & Hassell, 2009). Despite being a banned terrorist organization within Pakistan, they maintain multiple training and operational camps in the Pakistan-controlled sub-regions within Kashmir (Spindlove & Simonsen, 2010) and their operations frequently result in links to the ISI, or Inter-Services Intelligence, the primary intelligence agency of Pakistan (Dill, 2012; Fair, 2011; Kambere et al., 2011; Rotella, 2012; Wirsing, 1998). This is unsurprising, given the ISI's involvement in the dismantling of the Soviet occupation of Afghanistan and the resulting close ties with liberation movements and guerilla operations in the region (Kambere et al., 2011; Sen, 1992).

ISI has nurtured a thriving market for illegally trafficked goods for decades, even going as far as using the National Logistic Cell (NLC), a logistics company nationalized by the Pakistani Army which was used to supply arms to the Mujahideen in Afghanistan, to run drugs over the same routes (Haq, 1996; Sen, 1992). Intelligence estimates in 1992 suggested that Pakistani drug dealers had amassed the world's largest stockpile of opium and heroin (Kambere et al., 2011; Sen, 1992). As indicated by their use of the NLC, ISI does not just passively allow this environment of criminality, they are an active part of it. Apprehended drug traffickers and scouts from Norway and Japan admitted that their handlers had close ties with generals in the region (Haq, 1996; Sen, 1992). The insurgencies in the neighboring regions made the arms trade lucrative, and, as stated earlier, ISI has been involved in trafficking directly. While access to funding, munitions, and armament and lack of meaningful government oversight in the regions in which they operated enabled Lashkar-e-Taiba's operations in 2008 (Haberfeld & Hassell, 2009; Spindlove & Simonsen, 2010), they were not the primary factors in the group's success. Across all notable analyses reviewed, there was a conclusion in common regarding the causes of their success: superior information and exploitation of OSINT, or open-source intelligence, as a basis for rapid, spontaneous planning and for reorganization (Burton & West, 2008;

Goodman, 2011; Haberfeld & Hassell, 2009; Ministry of External Affairs India, 2009; Shahrzad Rizvi & Kelly, 2015).

The group made notable efforts prior to the event to develop actionable intelligence and a working knowledge of the intended area of operations. The terrorists applied for jobs in the kitchen, booked rooms at the hotel, and visited and mapped buildings. Most of the information they used to plan and modify operations was open-source and available to the public. The groups made use of back entrances and corridors not open to civilians and barely known by the reacting counterterrorism force and used these areas, discovered in prior reconnaissance, to counterattack the counterterrorists, ambush civilians, and escape and evade when outmatched (Burton & West, 2008; Haberfield & Hassell, 2009; Shahrzad Rizvi & Kelly, 2015). During the event, a command center in Pakistan was in contact with the group using satellite phones. The command center used live news and Twitter to inform decision-making and to inform personnel on the ground of counterterrorism operations (Goodman, 2011). In one notable incident, a tweet with a picture posted by the BBC revealed the position and intent of a counterterrorism unit on the ground in real-time, resulting in a counterattack (Shahrzad Rizvi & Kelly, 2015). Marc Goodman, an authority on terrorist use of open-source data, in a talk on the topic, noted that while terrorists had used public-access tools such as Twitter and Google Earth before, this was the first notable event in which they mined social media data in real time and did so at such a scale (Goodman, 2011). The groups confirmed potential high value targets by using Google and social media, remapped operations using tweets, GPS devices, and Google Earth, and even intercepted communications at the hotel, alerting the terrorists to room numbers of high-value targets (Goodman, 2011; Haberfield & Hassell, 2009; Ministry of External Affairs India, 2009).

In contrast to Lashkar-e-Taiba's OSINT-informated improvisation and spontaneous planning, counterterrorist forces were continuously delayed by lack of flexibility. The Indian emergency planners had planned for events like the 2008 Mumbai attack, but "lacked a modular and flexible structure when it came to communicating and responding in a non-routine fashion" (LaRaia & Walker, 2009). In some cases, the lack of a QRF (quick reaction force) in Mumbai was noted as a basis for failure (Shahrzad Rizvi & Kelly, 2015), however, the Indian Navy was actually stationed in Mumbai at the time of the attack but lacked the necessary signed release to use military assets in civilian domain. A special forces unit with the Indian Army was delayed as well because they did not have "their own air assets" to travel to the site (Kronstadt, 2008; Shahrzad Rizvi & Kelly, 2015). It may be important to note that the Indian Government had access to all of the same information the terrorists did but failed to attempt to assemble specialists who could have made use of the data (Goodman, 2011; Haberfeld & Hassell, 2009; Shahrzad Rizvi & Kelly, 2015). Shivshankar Menon, India's Prime Minister at the time of the attack, noted

that "[the key was rapid analysis]... we didn't have it." (Glanz et al., 2014).

While traditional metrics for readiness and capability might indicate that the conflict was significantly asymmetric in favor of the counterterrorists (e.g. monetary value of equipment, personnel count, extent of training), this vignette supports the findings of other analyses on asymmetry, which indicate that the stated metrics may not necessarily be representative of the balance of power or indicate probability of outcomes (Arreguín-Toft, 2001; Berglund & Souleimanov, 2020). Asymmetry in resources having little correlation with success in conflict is acknowledged as a recurring phenomenon and is an important characteristic of conflict which developed in the latter half of the 20th century, (Arreguín-Toft, 2001) the reasons for this emergent characteristic will be discussed further.

## Complex Threats in the Gray Zone

More broadly, the introduction of nuclear weapons and the maintenance of large military budgets by the remaining geopolitical superpowers after the conclusion of World War Two (Roser & Nagdy, 2013) created an environment which changed the risk calculus of conventional conflict (Rauchhaus, 2009; Treverton & Posen, 1992). This shift in risk is sometimes interpreted as a cause of a "Long Peace" (Pinker, 2012) or "Nuclear Peace" (Rauchhaus, 2009), which, at a glance may be supported by data on battle deaths per year (Peace Research Institute Oslo, 2020). Though this may be true of direct, conventional, interstate warfare, this has not necessarily been true for military conflict in general. Instead, its "timing, intensity. and [outcomes]" have changed (Arreguín-Toft, 2001; Rauchhaus, 2009). Governments have adapted the way they conduct conflict, and as a result, nurtured a new domain of operations often referred to as "The Gray Zone" (McCarthy et al., 2019; Troeder, 2019). Actions which are aggressive in nature but moderated in order to prevent triggering discrete change in diplomatic status (e.g. declarations of war) vis-a-vis Article 5 of the North Atlantic Treaty or Article 51 of the United Nations Charter are classified as Gray Zone Warfare (McCarthy et al., 2019; NATO, 1949; United Nations, 1945; Votel et al., 2016). Intelligence agencies of many nations, not just superpowers, managed conflicts through proxy warfare and by sponsoring non-state actors with aligned goals (Acharya & Marwah, 2010). Often assisted by training from state actors, non-state actors used guerilla tactics and operated in a decentralized, networked fashion in the interest of self-preservation. One of the results of this decentralization has been a deep embedding of these non-state actors in local networks, including Governments, illicit trafficking operations, and religious groups; this embedding blurs the line between licit, criminal, and guerilla networks, allowing groups to use this embedding as a form of camouflage and a basis to acquire resources without sponsors (Haberfeld & Hassell, 2009; Haq, 1996; Kambere et al., 2011; Kilcullen, 2012; Sen, 1992; Spindlove & Simonsen, 2010). As centralized state

actors learned to react to the new tactics being used against them and to practice deterrence, decentralized non-state actors continued to evolve, solving complex informational problems such as the imperfect monitoring of cells, inter and intragroup communication of activities, and reducing risk and cost of operations (Dale E. Lichtblau, Brian A. Haugh, Gregory N. Larson, Terry Mayfield, 2006; Naftali, 2009). The smaller size and limited resources of non-state actors required them to become resilient and adapt where larger nations may have reinforced. More importantly, it required them to become more innovative in finding opportunities and exploiting weaknesses (Dolnik, 2007).

Based on analyses of the events in Mumbai, the attack can be characterized as a successful exploitation of Complex Threat Surfaces. In hardware security, attack surfaces can be defined as "the sum of all possible security risk exposures" (Bhunia & Tehranipoor, 2011) and in practice refer to domains of risk exposure often described in layers (Torkura et al., 2019). The term may have equal value in describing surfaces of attack in Military Science and the study of counterterrorism, sometimes described as "The Long War on Terrorism" (LeRoy, 2008). However, non-adversarial events are also of interest to National Security, such as the response to natural disasters, pandemics, or even post-terrorism clean-up operations such as hazardous material removal post-9/11 (McEntire, 2014). Thus, for the purposes of this paper we discuss "Complex Threat Surfaces" rather than "attack surfaces" to emphasize the need for an integrated management approach to various kinds of non-linear failure modes. As stated earlier, terror and insurgent groups have become more innovative in their approach to exploiting weaknesses. Groups are incentivized to maximize impact while minimizing risk and cost. This has resulted in targeting Complex Threat Surfaces which cannot be effectively defended linearly, intuitively, or by using certain established legacy measures (Dolnik, 2007; Haberfeld & Hassell, 2009; LaRaia & Walker, 2009; Troeder, 2019; Votel et al., 2016), as evidenced by the failure of counterterrorism measures which successfully red flagged behavior by Lashkar-e-Taiba (Shahrzad Rizvi & Kelly, 2015) to deter or reduce the efficacy of the Mumbai Attack, and those which, if successfully compromised, represent opportunities for cascading, non-linear failure (Lee et al., 2016; Salmeron et al., 2004; Sims, 2018). We now turn to a discussion of the interdisciplinary paradigm of Complexity Science and highlight the role of rapidly assembled teams in responding to Complex Threat Surfaces.

## From Complex Threats to Complexity Science

The science of Complexity, or Complexity Science, is the study of systems that are composed of many interacting subunits (Gershenson, 2013; Gordon, 2014; Lawson, 2013; Mantri & Thomas, 2019). Such systems, for example brains or battlefields, often exhibit characteristics such as adaptive capacity, radical historicity, self-organization, non-linear dynamic

behaviour. To manage and de-risk these challenging attributes of Complexity Science is an interdisciplinary field that studies the patterns and principles of complex adaptive systems (CAS) in general and specific (Gershenson, 2013; Mantri & Thomas, 2019; Massari, 2019; Mitchell, 2009). Robert Maxfield, a trustee of the Santa Fe Institute, which was founded to study complexity, at a symposium on complexity for the National Defense University stated that: "The scientifically significant results [of Complexity Science] are so far mostly in the physical and biological domain, but the metaphors have proven to have tremendous appeal and utility in studying humans and human social systems" (Maxfield, 1996). Indeed, recent decades have seen increased interest in research and applications of Complexity approaches in Military, Informational, and Geopolitical contexts (Dittmer, 2014; Rosenberg, 2017). Specific examples here illustrate the point that Complexity Science approaches can add significant value, reflected by unique explanations or predictions, when considering Military Science (Lawson, 2013; Williamson, 2009), counterinsurgency approaches specifically (Ford, 2012; Miralles Canals, 2009), and team formation approaches.

Complexity Science has been used to help model and characterize the behavior and structure of insurgencies and terrorist organizations. Results of these analyses provide utility in understanding their nature, as noted by Maxfield and others (Maxfield, 1996). Work has been done to model insurgencies and terrorist organizations as complex adaptive systems, revealing evolutionary tendencies already modeled in natural and computational systems (Dale E. Lichtblau, Brian A. Haugh, Gregory N. Larson, Terry Mayfield, 2006; Ilachinski, 2012). Beyond terrorist groups, Complexity Science has been used to model domestic military forces as well, such as interpreting frigate crews, littoral (coastal) forces, and air forces as complex adaptive systems (Bar-Yam, 2003; Ellis, 2017; Murphy, 2014).

Across different types of military forces, the manifested behavior or "phenotype" of a group arises emergently from the interaction between the guiding principles of the group, and the specifics of the environmental context. The variable expression of underlying characteristics of terrorist groups provides them with adaptive flexibility across environmental context. In order to help predict surfaces of attack and tactics, strategists must identify both essential characteristics of a group and relevant elements of the environment. For example, terrorist groups with similar characteristics are more likely to engage in frequent violence in regions which have higher press access (Chai, 1993). Here there are striking parallels to the findings and implications in the literature on genetics and epigenetics (Frisch, 2011; Grisogono & Ryan, 2003; Maleszka, 2016; Weyrich et al., 2018). This "epigenetic" spread of insurgencies thus may be modeled as following principles found in collective behavior models (Friedman et al., 2020; Gordon, 2016), resulting in patterns of spread and behavior that look remarkably similar to the results of ant-colony

optimization algorithms (Dorigo & Stützle, 2019; Shiwakoti et al., 2011; Vodák et al., 2018; Wood, 2015).

Decentralized terrorist groups appear to have self-organizing and autopoietic (self-meaning-generating (Allen & Friston, 2018; Dos Santos, 2018)) characteristics. These attributes are especially apparent in recruiting spaces, littoral environments, and volatile battlefield situations (Kilcullen, 2012). Destroying central leadership of terrorist groups in cases where leadership is highly centralized may result in the collapse of the organization. For example, the offer of an amnesty deal to the leaders of Al Aqsa by the Israeli Government caused a nearly immediate, systemic collapse of the organization (Chai, 1993). However, destroying central leadership when the organization is decentralized may just result in fracture and increased complexity, as groups may fracture along hidden or pre-existing ideological lines just as easily as they may fracture on a basis of geography or methodology (Abdallah, 2019; Chai, 1993; Nessel, 2012). Separation from intellectual or political leadership can result in groups over-imitating their parent organizations, resembling well-studied social and psychological phenomena such as cargo cults and over-imitation. This over-imitation can lead to senseless violence detached from any notable purpose (Chai, 1993; Eliade, 1965; Lyons et al., 2007; Nessel, 2012; Stanner, 1958). Understanding the autopoietic and self-organizing nature of these groups prevents a false sense of security which can so often come from material victories, such as the breaking of a stronghold or the assassination of leaders (Abdallah, 2019), as fractured groups or groups which remain despite fractured leadership or the completion of the explicit goals they were formed with are not uncommon. For example the Stern Gang (LEHI) remained active after the creation of the state of Israel, as did the IRA after the establishment of the Irish Free State, and the Ku Klux Klan in the United States after leadership left the organization (Chai, 1993).

Future work in the spirit of Complexity Science could elaborate and formalize the intersection of well-modeled natural phenomena (epigenetics, collective behavior), modern computational techniques (network analysis, machine learning) and counterinsurgency efforts. Such a cross-sector framework for understanding behaviors may lead to the ability to influence outcomes (e.g. through the use of control theoretic approaches) and eventually even the ability to design distributed counterinsurgency systems (Newkirk et al., 2012; Shahrzad Rizvi & Kelly, 2015; Sofea Azrina Azizan, Izzatdin Abdul Aziz, Bandar Seri Iskandar, 2017). We hold that Complexity Science can thus provide useful direction to those who hold responsibility for operations and force design to be mindful of the complexity of the operating environment (Maxfield, 1996; Murphy, 2014; Saperstein, 1996). We now turn to an investigation of rapid team assembly in located, remote, and hybrid contexts, from the perspective of Complexity.

## Emergent Teams and Rapid Reorganization

Within various civilian domains, some of which overlap with military, High-Reliability Organizations (HRO) have to contend with Complex Threat Surfaces as well (Porte & Consolini, 1998; Weick & Sutcliffe, 2015). These domains include air traffic control, power grid management, wildland firefighting, and intensive care units (Christianson et al., 2011; McKeon et al., 2006; Porte & Consolini, 1998). Similar to their military counterparts, these domains are often areas where failures cascade and victories accumulate, where small errors can create macro-level impacts that are not necessarily proportionate to the perceived severity of the error viewed in isolation (De Bruijne & Van Eeten, 2007; See et al., 2014; Szumilas et al., 2011). In these environments where minimizing chance of failure is key, optimization can be interpreted to come at the cost of fragility (Mamouni Limnios et al., 2014). As a consequence of the importance of reliably managing Complex Threat Surfaces, a robust literature exists on these environments (Weick & Sutcliffe, 2015). Work from a Complexity perspective on collective behavioral algorithms highlights the relevance of ecological factors such as degree and type of variability, and threat of catastrophic disruption (Flaherty, 2019; Gordon, 2014; Smith & Jenks, 2006).

While most early work on strategies within HROs focuses on co-located groups, HRO research has adapted over the years to include remote and hybrid paradigms. Work has been done to integrate remote organizational components and even nonhuman or unmanned assets into HRO frameworks (Brooker, 2013; Dalamagkidis et al., 2011; Grabowski & Roberts, 2019). In a modern information workspace and battlefield, AI-augmented human actors, and autonomous AI systems, play an increasingly important role. A key strategy found in the analysis of HROs and related work on emergency response is the maintenance of organizational fluidity or the ability to rapidly pool collective expertise, share information, and reorganize in order to respond to emergent problems in the operating environment (Grabowski & Roberts, 2019; McEntire, 2014; Rigaud & Hollnagel, 2006; Weick & Sutcliffe, 2015). In oil and gas production, flexible, horizontal mechanisms are used to rapidly reorganize and integrate operators and supervisors into “tiger teams”, groups of experts that are assigned to solve specific problems relevant to the background of personnel (Grabowski & Roberts, 2019). In Toyota, “swift market analysis response teams” (SMART) were organized around customer complaint content based on background relevance and reorganized on completion to greatly increase turnover on errors and handle recalls safely, this was successful to such an extent that elements of the role reorganization process were built into SCRUM, a widely used project management framework (Weick & Sutcliffe, 2015). It is important to note that in both cases personnel were not required to be co-located in order to participate (Grabowski & Roberts, 2019; Weick & Sutcliffe, 2015). This

transition toward more distributed frameworks aligns research on civilian HROs with research on complex adaptive systems, the challenges militaries face, and potential best practice. These same attributes of organizational fluidity and flexibility are echoed in military literature on force design, counterterrorism, doctrine, and counterinsurgency as well (Bar-Yam, 2003; Ellis, 2017).

In respect to force design, organizational fluidity has been acknowledged as essential in modern militaries. Special attention has been paid to littoral warfare, where land, water, and amphibious forces are faced with the paradox of maintaining flexibility while being composed of assets which are the result of decades-long investment cycles (Ellis, 2017; Royal Canadian Navy, 2016). Modern littoral environments are often characterized by the myriad of Complex Threat Surfaces that can be exploited by local insurgencies and related groups. These Complex Threat Surfaces include the surface of the water itself in the form of mines, unmanned vehicles, and submerged vessels, as well as attacks from the air via drones (Bar-Yam, 2003; Hill, 2009).

To this end, it is difficult to design a perfect system to ensure that any specific vessel, given any single configuration of crew and equipment, would be capable of deterring every threat (Ellis, 2017; LaGrone, 2017; Royal Canadian Navy, 2016; Shaul, 2019). As described in a Complexity-informed analysis of rapidly-assembling teams on frigate ships, "it is not reasonable to expect a linear response as circumstances will dictate specific actions" – in such cases, operators on the ship operate semi-autonomously and teams emerge in response to threat assessments (Bar-Yam, 2003; Ellis, 2017). For such situations, pre-planned responses help maneuver the crew into positions from which they can confidently follow or diverge from doctrine. This ability to rapidly reorganize is especially important given terror and insurgent groups' tendency toward mimetic transfer and copy-cat attacks, trading and adapting strategies that worked for other groups (Hill, 2009). Organizations in this space have had notable successes in the exploitation of Complex Threat Surfaces present when military and civilian ships operate in littoral environments (Burton & West, 2008; Hill, 2009). In response to these dangers are projects like STANFLEX, which is a modular ship design implemented by the Danish Navy, offering the capability of hot-swapping modular weapons, sensor, and staging platforms while in port in order to rapidly reorganize equipment and crew configurations (Ellis, 2017; Mun, 2018).

Rapid Reorganization of leadership in counterinsurgency efforts has been documented to be impactful. The Malayan Emergency (Malay Peninsula, 1948-1960) is frequently looked to as a successful counterinsurgency (Hack, 2009; Robinson, 2008) and will be discussed briefly. Though the counterinsurgency had many failures at the beginning, there was a reorganization of top leadership to include civilians. This structure, once

allowed to proceed, quickly replicated at provincial and district levels resulting in a decentralization of intelligence and local operations (Robinson, 2008). With increased information sharing and the inclusion of locals, less focus was given to combatting the rebels and organizations took significant steps to begin addressing the social, economic and political problems which drove rebel support instead (Hack, 2009; Komer, 1972; Robinson, 2008). These emergent, cohesive civilian and military management apparatuses robbed rebels of public support and contributed significantly to the war effort at remarkably low costs (Komer, 1972). This style of reorganization and rapid assembly of organizations or teams with the inclusion of populations in the area of operations was replicated in Iraq in 2003 and was viewed as imperative to operations in the region, especially due to the complexity of the operating environment (Grabowski & Roberts, 2019; Green, 2007; McChrystal et al., 2015; Ricks, 2006).

To close, as well as provide an optimistic contrast with the Mumbai events, we relate a vignette from 1993, when a group of terrorists affiliated with Al Qaeda planned to put into action a multistage attack to exploit Complex Threat Surfaces across the island of Manhattan in New York City (Dahl, 2014; United Nations, 2018). The terrorists intended to storm the island in watercraft (Burton & West, 2008) and split into several tactical teams. The group's plan included bombs at key locations like landmarks and transport infrastructure such as the Lincoln and Holland tunnels and the ferries in lower Manhattan. Simultaneously, other teams were to raid hotels such as the Waldorf-Astoria, St. Regis, and U.N. Plaza with the intention of finding high-value targets and inflicting as much damage to soft-targets as possible (Burton & West, 2008; Dahl, 2014). Similar to the pre-planning in Mumbai, the group in New York did on-site reconnaissance in advance, taking detailed notes of stairwells, cameras, and security personnel location and attire (Burton & West, 2008). The FBI, upon discovery of the plot, began to coordinate multiple previously-unconnected individuals, such as controlled informants from previous operations, terrorism task forces, and local government and police. With this reorganization in place, it was decided that they would allow the group to centralize their operation in relative safety in order to prevent fracture. When the group began building explosives, their safe house was raided, eight arrests were made, and the plot was foiled with no loss of life (Dahl, 2014). This New York vignette, contrasted with the eerily similar Attack on Mumbai, illustrates how rapid reorganization and assembly of teams in response to novel, emergent threats can meaningfully impact outcomes in counterinsurgency operations.

## Conclusion

In this paper we have used the interdisciplinary approach of Complexity Science to highlight Complex Threat Surfaces as a key variable for counterinsurgency efforts and other gray zone efforts in today's cyberphysical battlefield. We have highlighted key principles that

differentiated event outcomes, such as the ability of opposing forces to rapidly reorganize, propagate information, and reassemble teams. As teams in the modern operating environment become increasingly remote, new challenges are presented, but also new advantages can become realized (Grabowski & Roberts, 2019). The complex threat surface approach highlights the need for further work at the intersection of information sharing system design (Rigaud & Hollnagel, 2006), decentralized intelligence or OSINT (Brafman & Beckstrom, 2006; Green, 2007), and other topics. Conceptual models and innovation technologies arising from this integrative approach may prove useful in service of counterinsurgency efforts now and in the future.

# Works Cited


Abdallah, R. (2019). ISIL is not dead, it just moved to Africa. Al Jazeera. https://www.aljazeera.com/indepth/opinion/isil-dead-moved-africa-191126152156781.html

Acharya, A., & Marwah, S. (2010). Nizam, la Tanzim (System, not Organization): Do Organizations Matter in Terrorism Today? A Study of the November 2008 Mumbai Attacks. Studies in Conflict and Terrorism, 34(1), 1–16.

Allen, M., & Friston, K. J. (2018). From cognitivism to autopoiesis: towards a computational framework for the embodied mind. Synthese, 195(6), 2459–2482.

Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. International Security, 26(1), 93–128.

Bar-Yam, Y. (2003). Complexity of Military Conflict: Multiscale Complex Systems Analysis of Littoral Warfare (No. F30602-02-C-0158). New England Complex Systems Institute. https://static1.squarespace.com/static/5b68a4e4a2772c2a206180a1/t/5c09552e352f53aaa5645aa1/1544115504973/SSG_NECSI_3_Litt.pdf

Berglund, C., & Souleimanov, E. A. (2020). What is (not) asymmetric conflict? From conceptual stretching to conceptual structuring. Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide, 13(1), 87–98.

Bhunia, S., & Tehranipoor, M. (2011). Introduction to Hardware Security. ScienceDirect. https://www.sciencedirect.com/topics/computer-science/attack-surface

Brafman, O., & Beckstrom, R. A. (2006). The spider and the starfish: The unstoppable power of leaderless organizations. New York: Portfolio.

Brooker, P. (2013). Introducing Unmanned Aircraft Systems into a High Reliability ATC System. Journal of Navigation, 66(5), 719–735.

Burton, F., & West, B. (2008). From the New York Landmarks Plot to the Mumbai Attack. Stratfor. https://worldview.stratfor.com/article/new-york-landmarks-plot-mumbai-attack

Chai, S.-K. (1993). An Organizational Economics Theory of Antigovernment Violence. Comparative Politics, 26(1), 99.

Christianson, M. K., Sutcliffe, K. M., Miller, M. A., & Iwashyna, T. J. (2011). Becoming a high reliability organization. Critical Care / the Society of Critical Care Medicine, 15(6), 314.

Dahl, E. J. (2014). Preventing a Day of Terror: Lessons Learned from an Unsuccessful Terrorist Attack. CTX, 4(1), 71–77.

Dalamagkidis, K., Valavanis, K. P., & Piegl, L. A. (2011). On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations. Springer Science & Business Media.

Dale E. Lichtblau, Brian A. Haugh, Gregory N. Larson, Terry Mayfield. (2006). Analyzing Adversaries as Complex Adaptive Systems. Institute for Defense Analysis. https://doi.org/IDA Paper P-3868

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. Journal of Contingencies and Crisis Management, 15(1), 18–29.

Dill, E. (2012). Lashkar-e-Taiba: A Global Threat Today, a Threat to Pakistan Tomorrow. https://apps.dtic.mil/sti/citations/ADA600455

Dittmer, J. (2014). Geopolitical assemblages and complexity. Progress in Human Geography, 38(3), 385–401.

Dolnik, A. (2007). Understanding Terrorist Innovation: Technology, Tactics and Global Trends. Routledge.

Dorigo, M., & Stützle, T. (2019). Ant Colony Optimization: Overview and Recent Advances. In M. Gendreau & J.-Y. Potvin (Eds.), Handbook of Metaheuristics (pp. 311–351). Springer International Publishing.

Dos Santos, W. D. (2018). Carrying pieces of information in organocatalytic bytes: Semiopoiesis-A new theory of life and its origins. Bio Systems, 164, 167–176.

Eliade, M. (1965). Mephistopheles and the Androgyne: Studies in Religion Myth and Symbol. Sheed and Ward.

Ellis, P. (2017). Implications of the Complex Adaptive Systems Paradigm. International Safety Research. https://doi.org/6070-01-02

Fair, C. C. (2011). Lashkar-e-Tayiba and the Pakistani State. Survival, 53(4), 29–52.

Flaherty, E. (2019). Conclusion: A Complexity-Informed Approach to the Study of Social-Ecological Systems. In E. Flaherty (Ed.), Complexity and Resilience in the Social and Ecological Sciences (pp. 213–230). Palgrave Macmillan UK.

Ford, M. C. (2012). Finding the target, fixing the method: methodological tensions in insurgent identification. Studies in Conflict and Terrorism, 35(2), 113–134.

Friedman, D. A., Johnson, B. R., & Linksvayer, T. A. (2020). Distributed physiology and the molecular basis of social life in eusocial insects. Hormones and Behavior, 104757.

Frisch, E. (2011). Insurgencies are Organizations Too: Organizational Structure and the Effectiveness of Insurgent Strategy. The Peace and Conflict Review, 6, 1–23.

Gershenson, C. (2013). The Implications of Interactions for Science and Philosophy. Foundations of Science, 18(4), 781–790.

Glanz, J., Rotella, S., & Sanger, D. E. (2014). In 2008 Mumbai attacks, piles of spy data, but an uncompleted puzzle. New York Times. http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html

Goodman, M. (2011). The Business of Illegal Data. Strata Summit 2011. https://www.youtube.com/watch?v=6ueKilyThQg

Gordon, D. M. (2014). The ecology of collective behavior. PLoS Biology, 12(3), e1001805.

Gordon, D. M. (2016). The Evolution of the Algorithms for Collective Behavior. Cell Systems, 3(6), 514–520.

Grabowski, M., & Roberts, K. H. (2019). Reliability seeking virtual organizations: Challenges for high reliability organizations and resilience engineering. Safety Science, 117, 512–522.

Green, D. (2007). Counterinsurgency Diplomacy: Political Advisors at the Operational and Tactical Levels. Military Review, 87(3), 24.

Grisogono, A.-M., & Ryan, A. (2003). Designing complex adaptive systems for defence. Systems Engineering Test and Evaluation Conference, Canberra. http://militaryepistemology.com/wp-content/uploads/2003/10/2003-Ryan-Grisogono_Designing-CAS-for-Defence_SETE.pdf

Haberfeld, M. R., & Hassell, A. (Eds.). (2009). A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned. Springer, New York, NY.

Haberfield, M. R., & Hassell, A. von. (2009). A New Understanding of Terrorism. Springer Science & Business Media.

Hack, K. (2009). The Malayan Emergency as Counter-Insurgency Paradigm. Journal of Strategic Studies, 32(3), 383–414.

Haq, I. (1996). Pak-Afghan Drug Trade in Historical Perspective. Asian Survey, 36(10), 945–963.

Hill, B. P. (2009). Maritime terrorism and the small boat attack threat to the United States : a proposed response [Monterey, California. Naval Postgraduate School]. https://calhoun.nps.edu/handle/10945/4929

Ilachinski, A. (2012). Modelling insurgent and terrorist networks as self-organised complex adaptive systems. International Journal of Parallel, Emergent and Distributed Systems, 27(1), 45–77.

Kambere, G., Goh, P. H., Kumar, P., & Msafir, F. (2011). The Financing of Lashkar-e-Taiba. Combating Terrorism Exchange, 1(1), 18.

Kilcullen, D. J. (2012). The City as a System: Future Conflict and Urban Resilience. The Fletcher Forum of World Affairs, 36(2), 19–39.

Komer, R. W. (1972). The Malayan Emergency in Retrospect: Organization of A Successful Counterinsurgency Effort (No. R-957-ARPA). Advanced Research Projects Agency. https://apps.dtic.mil/dtic/tr/fulltext/u2/748988.pdf

Kronstadt, K. A. (2008). Terrorist attacks in Mumbai, India, and implications for US interests. https://apps.dtic.mil/docs/citations/ADA492902

LaGrone, S. (2017). Navy : Saudi Frigate Attacked by Unmanned Bomb Boat , Likely Iranian. USNI News. https://news.usni.org/2017/02/20/navy-saudi-frigate-attacked-unmanned-bomb-boat-likely-iranian

LaRaia, W., & Walker, M. C. (2009). The Siege in Mumbai: A Conventional Terrorist Attack Aided by Modern Technology. In M. R. Haberfeld & A. Hassell (Eds.), A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned (pp. 309–340). Springer US.

Lawson, S. T. (2013). Nonlinear Science and Warfare: Chaos, complexity and the U.S. military in the information age. Routledge.

Lee, R., Assante, M., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center (E-ISAC), 1–26.

LeRoy, B. D. (2008). Fourth Generation Warfare: The Need for a Comprehensive Approach. School of Advanced Military Studies, US Army Command and General Staff College. https://apps.dtic.mil/dtic/tr/fulltext/u2/a484763.pdf

Lyons, D. E., Young, A. G., & Keil, F. C. (2007). The hidden structure of overimitation. Proceedings of the National Academy of Sciences of the United States of America, 104(50), 19751–19756.

Maleszka, R. (2016). Epigenetic code and insect behavioural plasticity. Current Opinion in Insect Science, 15, 45–52.

Mamouni Limnios, E. A., Mazzarol, T., Ghadouani, A., & Schilizzi, S. G. M. (2014). The Resilience Architecture Framework: Four organizational archetypes. European Management Journal, 32(1), 104–116.

Mantri, P., & Thomas, J. (2019). Nature's Design's: The Biology of Survival. MATEC Web of Conferences. https://www.matec-conferences.org/articles/matecconf/abs/2019/50/matecconf_icad2019_00023/matecconf_icad2019_00023.html

Marwaha, N. (2017). 26 / 11 Mumbai Attacks: The Night India Won 't Forget - A Timeline. NDTV. https://www.ndtv.com/mumbai-news/26-11-mumbai-attacks-anniversary-the-night-india-wont-forget-a-timeline-1779897

Massari, G. F. (2019). Teams as complex adaptive systems: Collective Intelligence and Adaptive Behaviors (G. P. Demelio (Ed.)) [MECHANICAL AND MANAGEMENT ENGINEERING, Politecnico di Bari]. https://www.dmmm.poliba.it/dottorati/pluginfile.php/261/mod_folder/content/0/PhDThesisMassariGiovanniF.pdf

Maxfield, R. R. (1996). Complexity and Organization Management. Symposium on Complexity, Global Politics and National Security. http://www.dodccrp.org/html4/bibliography/comch08.html

McCarthy, M. C., Moyer, M. A., & Venable, B. H. (2019). Deterring Russia in the Gray Zone. Strategic Studies Institute. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1407

McChrystal, G. S., Collins, T., Silverman, D., & Fussell, C. (2015). Team of Teams: New Rules of Engagement for a Complex World. Penguin.

McEntire, D. A. (2014). Disaster Response and Recovery: Strategies and Tactics for Resilience (p. 368). Wiley.

McKeon, L. M., Oswaks, J. D., & Cunningham, P. D. (2006). Safeguarding patients: complexity science, high reliability organizations, and implications for team training in healthcare. Clinical Nurse Specialist CNS, 20(6), 298–304; quiz 305–306.

Ministry of External Affairs India. (2009). Ministry of External Affairs India, Mumbai Dossier. Ministry of External Affairs India.

Miralles Canals, J. J. (2009). Fourth-generation warfare: Jihadist networks and percolation. Mathematical and Computer Modelling, 50(5), 896–909.

Mitchell, M. (2009). Complexity: A Guided Tour. Oxford University Press.

Mun, J. (2018). Flexible Ship Options (No. NPS-AM-18-235). https://nps.edu/documents/105938399/112603206/NPS-AM-18-235.pdf/6669f6e7-eb71-4ba1-9b9e-d43c2c095693?version=1.0

Murphy, E. M. (2014). Complex Adaptive Systems and the Development of Force

Structures for the United States Air Force. https://media.defense.gov/2017/Nov/21/2001847257/-1/-1/0/DP_0018_MURPHY_COMPLEX_ADAPTIVE_SYSTEMS.PDF

Naftali, T. (2009). Blind Spot: The Secret History of American Counterterrorism. Basic Books.

NATO. (1949). The North Atlantic Treaty. NATO. http://www.nato.int/cps/en/natohq/official_texts_17120.htm

Nessel, R. A. (2012). WHY FAILING TERRORIST GROUPS PERSIST: THE CASE OF AL-QAEDA IN THE ISLAMIC MAGHREB [Naval Postgraduate School]. https://apps.dtic.mil/dtic/tr/fulltext/u2/a563498.pdf

Newkirk, R. W., Bender, J. B., & Hedberg, C. W. (2012). The potential capability of social media as a component of food safety and food terrorism surveillance systems. Foodborne Pathogens and Disease, 9(2), 120–124.

Peace Research Institute Oslo. (2020, May 13). UCDP/PRIO Armed Conflict Dataset. Peace Research Institute Oslo (PRIO). https://www.prio.org/Data/Armed-Conflict/UCDP-PRIO/

Pinker, S. (2012). The Better Angels of Our Nature: Why Violence Has Declined. Penguin Books.

Porte, T. L., & Consolini, P. (1998). Theoretical and operational challenges of "high-reliability organizations": air-traffic control and aircraft carriers. International Journal of Public Administration, 21(6-8), 847–852.

PTI. (2020, February 18). Lashkar-E-Taiba Planned To Portray 26/11 Attack "Hindu terror": Ex-Mumbai Top Cop. Https://www.outlookindia.com/. https://www.outlookindia.com/website/story/india-news-lashkar-e-taiba-planned-to-make-2611-attack-look-like-hindu-terror-ex-mumbai-top-cop/347506

Rauchhaus, R. (2009). Evaluating the Nuclear Peace Hypothesis: A Quantitative Approach. The Journal of Conflict Resolution, 53(2), 258–277.

Ricks, T. E. (2006). Fiasco: The American Military Adventure in Iraq, 2003 to 2005. Penguin.

Rigaud, E., & Hollnagel, E. (2006). Proceedings of the Second Resilience Engineering Symposium: 8-10 November, 2006, Antibes-Juan-les-Pins, France. Presses des MINES.

Rizvi, S., & Kelly, J. (2015). The Continued Relevance Of The November 2008 Mumbai Terrorist Attack: Countering The Next Attack. Homeland Security Affairs, 11(6). https://www.hsaj.org/articles/4541

Rizvi, S., & Kelly, J. L. (2015). The continued relevance of the November, 2008 Mumbai terrorist attack: Countering new attacks with old lessons. Homeland Security Affairs, 11. http://www.academia.edu/download/38271312/The_Continued_Relevance_of_the_November_2008_Mumbai_Terrorist_Attack_Countering_New_Attacks_With_Old_Lessons.pdf

Robinson, W. (2008). Eradicating Organized Criminal Gangs in Jamaica: Can Lessons be Learnt From A Successful Counterinsurgency? https://apps.dtic.mil/dtic/tr/fulltext/u2/a491587.pdf

Rosenberg, M. (2017). Strategy and Geopolitics: Understanding Global Complexity in a Turbulent World. Emerald Group Publishing.

Roser, M., & Nagdy, M. (2013). Military Spending. Our World in Data. https://ourworldindata.org/military-spending

Rotella, S. (2012). Captured Militant Reaffirms Role of Pakistan in Mumbai Attacks. PBS Frontline; PBS Frontline. https://www.pbs.org/wgbh/frontline/article/captured-militant-reaffirms-role-of-pakistan-in-mumbai-attacks/

Royal Canadian Navy. (2016). Canada in a New Maritime World. http://www.navy-marine.forces.gc.ca/assets/NAVY_Internet/docs/en/rcn_leadmark-2050.pdf

Salmeron, J., Wood, K., & Baldick, R. (2004). Analysis of electric grid security under terrorist threat. IEEE Transactions on Power Systems, 19(2), 905–912.

Saperstein, A. M. (1996). Complexity, Chaos, and National Security Policy: Metaphors or Tools? Symposium on Complexity, Global Politics, and National Security, National

Defense University. http://www.dodccrp.org/html4/bibliography/comch05.html

See, K. C., Phua, J., Mukhopadhyay, A., & Lim, T. K. (2014). Characteristics of distractions in the intensive care unit: How serious are they and who are at risk? Singapore Medical Journal, *55*(7), 358–362.

Sen, S. (1992). Heroin Trafficking in the Golden Crescent. The Police Journal: Theory, Practice and Principles, *65*(3), 251–256.

Shaul, D. S. (2019, October 2). The threat of Houthi unmanned explosives-laden boats. ICT.org. https://www.ict.org.il/Article/2456/The_threat_of_Houthi_unmanned_explosives-laden_boats

Shiwakoti, N., Sarvi, M., Rose, G., & Burd, M. (2011). Animal dynamics based approach for modeling pedestrian crowd egress under panic conditions. Procedia - Social and Behavioral Sciences, 17, 438–461.

Sims, A. (2018). The Rising Drone Threat from Terrorists. Georgetown Journal of International Affairs, 19, 97–107.

Smith, J., & Jenks, C. (2006). Qualitative Complexity: Ecology, Cognitive Processes and the Re-Emergence of Structures in Post-Humanist Social Theory. Routledge.

Sofea Azrina Azizan, Izzatdin Abdul Aziz, Bandar Seri Iskandar. (2017). Terrorism Detection Based on Sentiment Analysis Using Machine Learning. Journal of Engineering and Applied Sciences, 12(3), 961–698.

Spindlove, J. R., & Simonsen, C. E. (2010). Terrorism Today: The Past, The Players, The Future (4th ed.). Prentice-Hall.

Stanner, W. E. H. (1958). On the Interpretation of Cargo Cults. Oceania; a Journal Devoted to the Study of the Native Peoples of Australia, New Guinea, and the Islands of the Pacific, 29(1), 1–25.

Szumilas, A., Swerhun, B., & Lye, J. (2011). Watts at Stake?: Protecting North America's energy infrastructure from cascading failure and terrorist threats. Dalhousie Journal of Interdisciplinary Management, 7(2). https://doi.org/10.5931/djim.v7i2.66

Tankel, S. (2013). Storming the World Stage: The Story of Lashkar-e-Taiba. Oxford University Press.

Torkura, K. A., Sukmana, M. I. H., Kayem, A. V. D. M., Cheng, F., & Meinel, C. (2019). A cyber risk based moving target defense mechanism for microservice architectures. Proceedings - 16th IEEE International Symposium on Parallel and Distributed Processing with Applications, 17th IEEE International Conference on Ubiquitous Computing and Communications, 8th IEEE International Conference on Big Data and Cloud Computing, 11t, September, 932–939.

Treverton, G. F., & Posen, B. R. (1992). Inadvertent Escalation: Conventional War and Nuclear Risks. In Foreign Affairs (Vol. 71, Issue 3, p. 170). https://doi.org/10.2307/20045251

Troeder, E. G. (2019). A Whole of Government Approach to Gray Zone Warfare. Strategic Studies Institute. https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1411

United Nations. (1945). Repertory of Practice of United Nations Organs — Codification Division Publications. Legal.un.org/. https://legal.un.org/repertory/art51.shtml

United Nations. (2018). The World's Cities in 2018. In Statistical Papers - United Nations (Ser. A), Population and Vital Statistics Report. https://doi.org/10.18356/c93f4dc6-en

Vodák, R., Bíl, M., & Křivánková, Z. (2018). A modified ant colony optimization algorithm to increase the speed of the road network recovery process after disasters. International Journal of Disaster Risk Reduction, 31, 1092–1106.

Votel, J. L., Cleveland, C. T., Connett, C. T., & Irwin, W. (2016). Unconventional Warfare in the Gray Zone. Joint Force Quarterly. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/

Weick, K. E., & Sutcliffe, K. M. (2015). Managing the Unexpected (3rd ed.). Wiley.

Weyrich, A., Lenz, D., & Fickel, J. (2018). Environmental Change-Dependent Inherited Epigenetic Response. Genes, 10(1). https://doi.org/10.3390/genes10010004

Williamson, S. C. (2009). From fourth generation warfare to hybrid war. ARMY WAR COLL CARLISLE BARRACKS PA. https://apps.dtic.mil/docs/citations/ADA498391

Wirsing, R. (1998). India, Pakistan, and the Kashmir dispute: On regional conflict and its resolution. Macmillan.

Wood, G. (2015, February 15). What ISIS Really Wants. The Atlantic. http://www.theatlantic.com/features/archive/2015/02/what-isis-really-wants/384980/