Role of Non-State Actors in the Landscape of Intelligence: The Comprehensive Insights

Zunaira Ali Khan

Salford University, United Kingdom

Zunikhan96@hotmail.com

Abstract

This article purposes to examine an emerging area of intelligence studies in how non-state actors are disrupting traditional state-centric practices of intelligence. It argues that intelligence is no longer solely the domain of nation states as both violent and non-violent non-state actors actively consume and produce intelligence to further their goals; thus, they become equal stakeholders along states. The paper first looks at non-violent groups like NGOs, hacktivists and cyber militias. It demonstrates how they conduct activities analogous to state intelligence services, such as indications and warning, cyber espionage, and influence the process of policymaking. Their flexibility and unconventional approaches often complement nation-state intelligence requirements. The paper further analyzes violent non-state actors, namely insurgents and terrorist groups. Through case studies, it shows how they adeptly use intelligence to intercept communication, plan surveillance and counter adversaries. Their adaptive structures mirror clandestine state operations. In essence, the paper reflects that the effectiveness of non-state actors in leveraging intelligence as they are significant players in the intelligence community alongside states. Recognition of the emerging role of non-state actors is vital to fully understand the contemporary intelligence landscape.

Keywords: Non-state Actors, Security threats, Intelligence Community, State Actors, New Trends in Intelligence

El papel de los actores no estatales en el panorama de la inteligencia: una perspectiva integral

Resumen

Este artículo se propone examinar un área emergente de los estudios de inteligencia, en la que se analiza cómo los actores no estatales están alterando las prácticas tradicionales de inteligencia centradas en

doi: 10.18278/si.9.2.10

el Estado. Se sostiene que la inteligencia ya no es dominio exclusivo de los Estados nacionales, ya que tanto los actores no estatales violentos como los no violentos consumen y producen inteligencia de forma activa para promover sus objetivos; por lo tanto, se convierten en partes interesadas en igualdad de condiciones con los Estados. El artículo examina primero a los grupos no violentos como las ONG, los hacktivistas y las milicias cibernéticas. Demuestra cómo llevan a cabo actividades análogas a los servicios de inteligencia estatales, como indicaciones y advertencias, espionaje cibernético e influencia en el proceso de formulación de políticas. Su flexibilidad y sus enfoques no convencionales a menudo complementan los requisitos de inteligencia de los Estados nacionales. El artículo analiza además a los actores no estatales violentos, a saber, los insurgentes y los grupos terroristas. A través de estudios de casos, muestra cómo utilizan hábilmente la inteligencia para interceptar comunicaciones, planificar la vigilancia y contrarrestar a los adversarios. Sus estructuras adaptativas reflejan operaciones estatales clandestinas. En esencia, el artículo refleja la eficacia de los actores no estatales a la hora de aprovechar la inteligencia, ya que son actores importantes en la comunidad de inteligencia junto con los Estados. Reconocer el papel emergente de los actores no estatales es vital para comprender plenamente el panorama de inteligencia contemporáneo.

Palabras clave: Actores no estatales, Amenazas a la seguridad, Comunidad de inteligencia, Actores estatales, Nuevas tendencias en inteligencia

非国家行动者在情报领域中的作用：全面洞察

摘要

本文旨在研究一个新兴的情报研究领域，即非国家行动者正如何颠覆以国家为中心的传统情报实践。本文论证，情报不再仅仅是民族国家的领域，因为暴力和非暴力的非国家行动者都积极消费和生产情报以实现其目标；因此，它们成为与国家平等的利益攸关方。本文首先研究非暴力团体，如非政府组织、黑客活动分子和网络民兵。本文展示了这类团体如何开展类似于国家情报服务的活动，例如指示和警告、网络间谍活动，并影响决策过程。他们的灵活性和非常规方法通常补充了民族国家的情报要求。本文随后分析了暴力的非国家行动者，即叛乱分子和恐怖组织。通过案例研究，本文展示了他们如何熟练使用情报来拦截通信、计划监视和对抗对

手。他们的适应性结构反映了秘密的国家操作。从本质上讲，本文反映了非国家行动者在利用情报方面的有效性，因为他们与国家一样是情报界的重要参与者。承认非国家行动者的新兴作用对于充分了解当代情报形势至关重要。

关键词：非国家行动者，安全威胁，情报界，国家行动者，情报新趋势

Introduction

The dissection of global affairs reveals that intelligence has captivated the attention of global players while conducting offensive as well as defensive activities. In the Neo-classical era, while the world assesses intelligence as a state-centric phenomenon, non-state actors (NSA) appear to be savvy consumers of intelligence, shaping the existing patterns of the intelligence community. Intelligence consumers are perceived as "sovereignties," or independent political activists who use intelligence to achieve broader strategic, tactical, and operational goals (Bozeman 1988). State and non-state actors seem to be in the same ball-pack for advancing of their goals, in devising strategies, containing aggressive operations, and furthering counterinsurgency. While sketching the structural and operational phenomenon of the NSAs, it is evident that non-state actors are sharply shaving off the settled norms of the intelligence community and seeking to affect the typical setup, challenging the existing hegemony. The flow of the paper will pass through the two variants of non-state actors, Non-violent Non-state Actors (NVNSAs) and Violent Non-state Actors (VNSAs), reflecting the stream of activities of non-state entities in the intelligence community. A comprehensive framework of intelligence-based activities of two categories of non-state actors will exhibit how they have shared space in the intelligence community with state actors and are now equally critical in international affairs.

Navigating the Various Trails of Non-state Actors

Non-state actors have multiple shades and pursue tasks of violent and non-violent nature to achieve their designed goals. The objectives of these actors have shifted drastically over time, from large-scale covert operations to nationalist freedom movements against authoritarian masters, to a traditional Marxist approach, to state-sponsored military/political actors, to Islamic Jihadists, to democratic socialist in contemporary world, to the conservative ideological supporting individuals or groups (Finnemore and Barnett 2004). They identify and manipulate the security holes of key targets through modified intelligence initiatives that commonly employ established or irregular methods to accomplish their conventional goals. Such activities are remarkably identical in practice to state-led intelligence operations and sometimes blur the states' intelligence-based initiatives.

A Glance at Intelligence Beyond Traditional Lens

From the extensive categories of Non-State Actors (NSAs), Non-Violent Non-State Actors (NVNSA) have emerged in the complex global realm. These actors sometimes alert or protect the world against the prevailing threats, and often sabotage the other party to achieve social, political, ideological, economic, and cultural objectives. The strategic intelligence-based contributions of such actors frequently serve broader perspectives that often help in flattening the growing adventurous curves. Widely known as players in the global "battleground of information," NSAs are influencing issue assessment, agenda-setting, policy-making, and execution to the maximum extent. This section will highlight the intelligence-based activities of non-violent non-state actors such as International Organizations (United Nations), Non-Governmental Organizations (NGOs,) and private individuals (hackers, cyber-militia), often take birth in the lap of the sovereign states but are autonomous bodies, which attempt to perform voluntary functions that states cede to them; thus, they efficiently share space with states in the intelligence sphere.

Non-violent actors traditionally have secured a narrow space in intelligence studies and research. Nevertheless, many NGOs, such as Amnesty International, and the International Crisis Group (ICG), make significant contributions to intelligence-oriented operations and disseminate collected and analyzed information to key decision-makers to transform global trends. NGOs collaborate with states and international organizations and aim to eschew violence. Sharing a large amount of sensitive information across vast network is a key characteristic of non-violent actors. In some cases, these actors either advocate for foreign intervention by deploying national power tools which commonly comprise offensive actions and or give detailed instructions. Due to extensive reliance on intelligence, organizations such as the ICG are often referred to as think tanks or knowledge providers, and work directly to influence state policies. The non-state actors follow a "crisis recipe" in matters of uncertainty and utmost urgency (Simons 2014). In such cases, through the efficient delivery of information, non-violent entities actively participate as prominent actors, similar to states' intelligence agencies, and consistently meet the broader social democratic norms, and standards of international law. For instance, the ICG, as an autonomous non-state entity, has engaged in carving out peaceful ways to prevent and resolve Rwanda's lethal genocide conflict (Grigat 2014).

Non-violent non-state actors perform the role of watchdog in international affairs by monitoring the governmental policies on conflicts, altering the perception of major players, and serving as crisis knowledge brokers. In 1992, the successful intelligence-based reporting of the CARE urged the U.S. authorities under President Bush to intervene in Somalia. The comprehensive details by the CARE highlighted that the services of international organizations and NGOs remained undelivered as eighty percent of food was lost to criminals and warring factions; thus, the U.S. decided to intervene. Such impactful humanitarian assistance has become possible only due to the effective utilization of intelligence by non-state actors (Terry 2003). Hence, they have mastered the consumer-producer relationship through efficient delivery of information, which often confounds the analytic arms of state intelligence services.

Moreover, some non-violent non-state actors engage in warning practices, analogous to regular state intelligence indications and warning (I&W) process, which essentially necessitate actors to discover opponents' warfare strategies to identify, monitor, and issue warnings before the real threat appears. For example, Genocide Watch concentrates on issuing cautions of approaching massacre and has established a 10-step predictor setup to assist its structurally similar warning and advocacy functions. The intelligence-based organizational goals of NGOs help to influence the patterns and practices of states in global affairs. Human Rights Watch (HRW), for example, is an offshoot of the Helsinki Accords established in 1975 to keep track of human rights violations in the Soviet Union. Today, it analyses human rights worldwide and publishes 100 reports annually on approximately 90 countries, the majority of which assess core issues that HRW seeks to address. HRW's primary mission is to investigate government infractions of international law, particularly those perpetuated by their security forces. In such cases, networked intelligence operations are also functionally equivalent to states' covert operations (Human Rights Watch 2015). Thus, non-state entities' efficient use of intelligence supports the state system against imminent threats and enables them to hold prominent space in the international community.

Furthermore, non-violent non-state actors interact with violent entities, frequently as covert allies for achieving specific goals. After determining that the fundamental principle requires direct participation in a conflict, primary non-state advocates often embrace militancy. In this regard, during the 1980s, Salvadoran rebels in Honduras and Afghan insurgents in Pakistan were combat allies with the legitimate states' authorities. Similarly, non-violent sovereigns influence national offensive actions in conflicts, utilizing advanced intelligence schemes. The constant pressure of NGOs on the U.S. authorities, depicting that American bombing curtailed their actions in reaching out to affected civilians and alerting them about the proliferation of human rights as a result of aggressive operations (Rumsfeld 2011, 390). NSAs revealed the politicization of the U.S. assistance in Iraq, as well as the U.S. inability to safeguard the masses, and in-adequate support to workers during the operational period (De Torrente 2004). Thus, the active eye of NSAs challenges states' strategic operations, and also provides details of conflict zones.

Non-state actors, like state intelligence services, rely on ostensibly adequate research and logical evaluation to engage with consumers, and support in achieving ideologically motivated organizational goals. Scholars have pointed out the effective role of NSAs in influencing and altering authoritative tendencies, while, highlighting the concerns of state intelligence services about the subtle influence of their information assessment on state policy and decision-making. For instance, non-violent actors indirectly adopt unconventional schemes to convince national and international governments to work in ways best suited to national interests (Keck and Sikkink 1999).

Furthermore, non-state actors employ intelligence capabilities and consume intelligence in ways similar to states. For example, both state and non-state actors are increasingly using cyber intelligence in hybrid conflicts and co-exist in the digital world to advance their agendas that often overlap with those of national goals. The complexities of the tangible world prompted a slew of state-sponsored intelligence operations, most of which took place in the late 1990s when internet access was widely available. Non-state groups at odds with one another and with international governments were responsible for conducting such intelligence-based operations. The moderate literature highlights the potential of NSAs such as hacktivists, patriot hackers, and cyber militia in state-to-state and state-to-individual operations, an effective model for conducting and concluding successful cyber-intelligence attacks.

Correspondingly, NSAs are increasingly being approached by state governments and military officials worldwide, who seek to utilize their cyber expertise to gain an advantage in wartime operations. Non-state actors intercept information that resides in or passes through computer networks of particular interest by using advanced intelligence techniques of decryption and decoding, software/hardware tools for surveillance, and other modes of intelligence gathering. IT experts and hackers may be formally or informally employed in electronic warfare army units, such as the Israeli Defence Forces Unit 8200 or the Chinese People's Liberation Army (PLA) Unit 61398. As a matter of fact, vulnerabilities are extremely important from an economic and military standpoint. The so-called "bug hunters" either sell vulnerabilities directly to governments or to private businesses like Tipping Point, i-Defense, Revuln, and Netragard, who can then resell them to other purchasers. For example, the well-known malware Stuxnet relied on the exploitation of multiple vulnerabilities that were probably purchased from bug hunter in the digital marketplace (darknet) (Bussolati,2015). Through the gathered and analyzed data, non-state actors actively contribute to shaping political domains; thus, they have become key players in world affairs along with state actors.

Cyber espionage is commonly identified as an act of national intelligence service, military units, or other institutions linked to nation-states; however, these roles have been independently performed by non-state actors as rouge entities. The "GhostNet" cyber-espionage network was an intriguing development that showcased the emerging roles of NSAs in the intelligence community alongside state actors. The discovery of the confidential information of public and private agencies of about 100 countries across the world in 2009, as part of an intelligence-based operation carried out by Chinese private individuals, demonstrates the effective use of intelligence by non-state actors. Similarly, the WANK worm was most likely created in 1989 by Australians to raise voices against NASA's consumption of radioactive material and the development of nuclear weapons to boost Galileo's crafted booster system, which, if blown up, could cause widespread damage to Florida residents. The Strano Network Sit-In in 1995, a "Netstrike" against French Government computer networks to protest nuclear and social models, was another non-violent but prominent contribution by non-state actors. Similarly, the Urban Ka0 Hackings in 1998 were an attempt to vandalize Indonesian government websites to draw attention to the marginalization of the people of East Timor.

Moreover, the cyber insiders act as cyber-espionage operators, assembling and overtly revealing confidential content or supplying national secrets to a competitor or foreign intelligence agency. CINDER (The Cyber Insider Threat) is a program of the U.S. Defense Advanced Research Projects Agency that aims to tackle intelligence leaks caused by cyber-insiders such as the "Afghan War archives" and "Cablegate" diplomatic cables disclosed by Julian Assange and Wikileaks.

The nationalist individuals through intelligence-based actions often bring forth impactful details that are helpful for state actors. Individuals or groups with patriotic tendencies target foreign countries in cyberspace, usually to support national governments; therefore, they share a prominent position in the intelligence community with state actors. During the Kosovo conflict, for instance, Black Hand, a group of Serbian-based patriotic hackers, vandalized a Kosovo Albanian website and intimidated the military computer networks of NATO states. Likewise, following the bombing of the Chinese embassy in Belgrade during airstrikes in May 1999, Patriot hackers support their nation-states in traditional conflicts by engaging in a variety of digital operations against the state's adversary. Patriotic hacking has been especially prevalent among Chinese hackers. The "Red Hacker Alliance" or "Honker Union of China" has painted itself on the broad canvas of patriotism. Russia, like Communist China, has an active patriotic hacking network. During the 1999 Kosovo conflict, Russian hackers engaged in web detection and mutilation and furthered cyber-attacks against Israel, Chechnya, Belarus, Kyrgyzstan, and others in the previous years.

Moreover, states approach Hacktivists to gain services in cyberspace that promote a perceived ideology or political agenda, either legally or illegally. Hacktivists help in achieving underlying political, military, or commercial goals in an indirect manner. Non-state actors employ tools such as internet resource redirections, data theft, website parodies, digital sit-ins, and other forms of cyber subversion. These non-state actors have twisted the curves of the intelligence community towards themselves by participating in various intelligence-based cyber operations in recent years. For instance, the "war" on Scientology, the revolutionary initiatives of Arab Spring, and attacks on companies such as Mastercard and the U.S. government websites.

The trends of independent actors' involvement in covert government-orchestrated campaigns, motivated by nationalistic goals to further strategic objectives, have become a new norm. Cyber-attacks can be launched via proxy, proving that nation-state participation in cyber warfare is inherently complex; thus, it enhances the position of non-state actors in the intelligence community. However, these non-state actors receive no monetary compensation and are not bound by any legal arrangements. Cyber-militias are suspected of carrying out several recent high-profile cyber operations sanctioned by a few countries. Iran, Turkey, Israel, and North and South Korea are engaged in political hacking. They often adopt offensive approaches toward targeted states or groups; however, through their intelligence-based engagement, they serve the national interests most appropriately and successfully gain the intelligence community's attention as a key player along with state actors.

In addition, states seek non-state sovereign intelligence expertise to advance covert missions, gain first-hand information about the frontlines, or perform volunteer functions that states cede to them to potentially accomplish their goals without brazenly breaching the Law of Armed Conflict. Non-state cyber actors are likely to be an appealing option, especially while striving to achieve restricted strategic objectives. The intelligence-based services of these entities provide a significant asymmetric edge, particularly for Dwarf nations which cannot take precedence on kinetic grounds. As a result, intelligence has shifted the focus from a state-centric theme to the web of non-state actors.

Violent Non-State Actors, States Actors and Intelligence

Violent non-state actors (VNSAs) are individuals or groups who aim to advance their actions in the world through violence and insurgency; therefore, they utilize intelligence resources to achieve maximum outcomes. Militias, insurgent groups, terrorists, specific organized crime groups, or warlords (Williams 2008) vary significantly in terms of ambition (succession, revolution, restoration), local conditions (geography, demographics, leadership), strategy (Maoist, Castroite), and organizational structure (political, military, tribal) (Krause 1996). This section will display various shades of violent non-state actors by highlighting the information operations of state-sponsored or insurgent/terrorist groups.

From the Classical Era to Modern times of insurgency, through intelligence, insurgents have acquired a prominent position in the intelligence community. David Galula, a French infantry officer, argued that intelligence had shifted power from states to non-state actors in global affairs, and explained the critical characteristics of a successful insurgency; the cause (gaining popular support), institutional vulnerabilities in the political and security infrastructure, geography that favors insurgents, and population (Buffaloe 2006). Human Intelligence and Open Source Intelligence have remained significant sources of intelligence collection for insurgents during the insurgency procedures. The Cypriote insurgency against the British in the 1950s employed HUMINT and benefited from the local population for the realization of their strategic goals. Similarly, through its draconian rule over controlled territories, the Islamic State of Iraq and the Levant (ISIL) took advantage of the widespread availability of HUMINT (Wege 2018).

From planning traditional military operations to extending counter-insurgency against targeted domestic or international states, avoiding penetrations, and shaping the overall operational atmosphere, NSAs are impacting large swathes of global affairs only through intelligence. Violent non-state actors, typically conduct offensive operations against adversaries similar to, paramilitary operations of state intelligence services and special operations forces (SOF), while slipping deeper into the mechanisms of security to protect themselves against the prevailing threats with competence, deception, and operational security.

The sophisticated information-gathering process by NSAs highlights the extensive themes of intelligence embedded in the movements of insurgents (NSAs). The North Vietnamese use of intelligence during the Second Indochina War is a classic example of challenging the state-centric phenomenon of intelligence. Through tactical intelligence, NSAs combated efficiently against the compelling strategic and operational level intelligence of Anti-Communist Forces. The North Vietnamese could only win at the end of the war because their intelligence infrastructure was synchronized with their conventional capabilities. Moreover, the troubles in Northern Ireland provide an in-depth view of insurgents' use of intelligence to achieve desired outcomes, run successful campaigns, and conduct effective offensive operations. The insurgent paramilitaries relied heavily on HUMINT and OSINT to collect information against the state's authoritative apparatus. Furthermore, the Greek Communist's intelligence network perfectly illustrates insurgent tactics during the Greek Civil War. Intelligence was an essential component of the Greek Communist operational strategy as it paved the way for successful military operations with far-reaching consequences despite their fragile military structure. In fact, at one point for the first time, the Greek government and its allies prioritized destroying the intelligence networks of insurgents, considering the potential threats from the intelligence-based initiatives of non-state actors. Therefore, NSAs have continued to calibrate violence not only through conventional methods, but also have taken full advantage of intelligence to share space in intelligence circle along with states.

NSAs overtly collaborate with allied organizations, or individuals, and further military assistance to pursue ideological, political, and other objectives, similar to the practices of states' intelligence services. The interaction among global terrorist networks is expanding as these non-state entities aim to transmit information to other hostile groups to shave off the dominance of adversaries and achieve mutual objectives. From Afghanistan and Iraq to Colombia, insurgents often share information as a mutual interest in undermining governmental efforts to thwart their mutual enterprises. Through virtual and in-person interactions, Islamic militants in Iraq have shared tactical information with the Taliban, HIG (Hezb-i-Islami Gulbuddin, an Afghan terrorist group), and freedom fighters from eastern and southern Afghanistan, and Pakistan's tribal areas to proceed mutual objectives.

The actions of terrorist groups also fall within the broad range of non-state actors, which through their traditional and advanced intelligence methods, are challenging the state-centric themes of intelligence. Over the years, Al Qaeda has evolved and developed a sophisticated intelligence doctrine, cell structure, advanced communication network, and extensive operational security measures that challenge the penetration by foreign actors. Through an adaptive organizational setup, VNSAs operate intelligence operations from different geo-strategic locations, leaving no clues of their models and existence, and making an effective use of intelligence resources. The group has repeatedly accessed cover agents in Five Eyes intelligence agencies like the FBI (Ilardi 2009). Al Qaeda has prioritized identifying vulnerabilities of targets and gathering information to understand the adversary's approach for operational security and offensive purposes. Following 9/11, the surveillance of the insurgents (NSAs) centered on discovering specific exploitable defects in the aircraft delivery system, which astounded the Western intelligence community with its advanced surveillance approach. Similarly, the trend in the national intelligence community of initiating covert operations is followed by insurgents to plan successful military combat. Al Qaeda, for example, in 1994, established a fishing business in Kenya to prepare for the 1998 bombings of the U.S. embassies in East Africa. Such operations find their link with those conducted by national military or intelligence-led SOF. Thus, Al-Qaeda, as a non-state actor, proved remarkably to be adaptable, and responsive, identifying a critical gap in its primary adversary's defense mechanisms that could be ruthlessly exploited through intelligence-based operations.

Moreover, insurgents (NSAs) design their emerging desires of revolution, console allies, protect the state's sovereignties, and entice neutral parties to voice their perception in real-time conflict through a broader intelligence framework. The episode of Kosovo's independence in the mid-1990s fits into the critical lens of the intelligence community. The Kosovo Liberation Army (KLA) realized their material inferiority to the Yugoslav army and Serbian republic security forces and opted to devise a derivative intelligence-based strategy to entice NATO into its war, an approach similar to Bosnian Muslims in 1994–95 which urged the U.S. authorities and NATO to intervene in the Bosnian civil war. Although the KLA had irregular intelligence services, it utilized the intelligence resources in analyzing the Western political vulnerabilities, and to expose the exploitation of civilians in wartime. The KLA intelligence-based information necessitated Western military forces to intervene in the war to protect Kosovo Albanian civilians under the Responsibility-to-Protect (R2P) norm. Thus, international intervention, military conflict and negotiations helped in achieving the goal of independence, which were largely influenced by intelligence.

NSAs employ intelligence to bend the curves of full-fledged traditional confrontation with their stronger adversaries. In addition, non-state actors supported by states, such as Hezbollah, act as mediators to bridge the gaps between the hostile parties and carve out ways for negotiations. In this regard, the intelligence capabilities of Hezbollah, and its advanced offensive arsenals, outweigh the intelligence potential of a few states. During the Syrian civil war, the world witnessed the intelligence-based capabilities of Hezbollah. It employs all basic intelligence-gathering methods, as evidenced by its use of advanced SIGINT equipment during the 2006 war while launching campaigns against Israel and Jews. The use of drones to gather visual intelligence over Israeli territory on several occasions reveals details about the extensive employment of intelligence by NSAs at regular and irregular times. Hence, the display of prominent intelligence-based practices of non-state actors indicates the emergence of new actors in the intelligence community along with state actors.

A Critical Recap

While navigating the trails of the intelligence community, it is definite that both state and non-state actors employ intelligence to influence adversaries' actions and achieve their vested interests. Though, NSAs frequently aim to produce similar results as states' intelligence-based operations, however, in being overly certain in their strategic assessments that resemble authoritarian patterns, non-state actors often are prone to error. The intelligence services of states are formally organized to achieve goals in the long run and often collaborate with legal intelligence agencies worldwide to maximize their outcomes, contrary to the narrowly developed structures of non-state actors. In addition, overly zealous cyber-militias cannot be restricted, unlike the governed legal military organization, and opt to target civilian, causing collateral damage. NSAs can pose a challenge after the successful accomplishment of intelligence-based missions by attempting to exploit sensitive data and can defect the entire state machinery. The absence of calculated strategic analysis, the presence of a monolithic approach, and the role of ideology in shaping the worldview of insurgents often lead to an unwillingness to accept non-state actors fit for the intelligence community along with state actors (Bell 1994).

However, as a collection, the literature demonstrates the existence of factual flaws about the insurgents' significant intelligence services, particularly among practitioners. Simply focusing on the "what" of non-state actors' intelligence is, it is worth noting that if a state's behavior and use of intelligence reveal political and social outlooks, then insurgent movements do as well. Non-state entities, through intelligence services, produce a variety of analytic intelligence mechanisms to impact a significant proportion of individuals, including key authority holders and those with less but still considerable influence. Non-state sovereigns' intelligence services navigate the ways to maintain co-existence between liberal and illiberal states in the modern era of confrontation, exploitation, and adventurism. They also assist in advancing new avenues for the analysis of intelligence studies by evaluating the existing practices and providing guidelines for future courses of action. Likewise, intelligence operations of non-state actors benefit from a flexible organizational structure with a focus on "whatever works," contrary to the rigid "make no mistake" concept of national actors. The emergence of new actors on global intelligence stage is taking new heights in modern digital age which needs to be better utilized for national interests and diplomatically handled in case of conflicts.

Conclusion

To encapsulate, a growing number of non-state actors use intelligence for various purposes and gaining popularity in global affairs. Non-state sovereigns are shaking dogmas, urging the world to rethink and reconstruct the existing structures, and express unconventional ideas; thus, they are challenging the long-standing occupied role of states in the intelligence community. However, the experts should also thoroughly examine the broad spectrum of intelligence-based activities of NSAs to hammer them on the contemporary global sheet, and to fill the existing gaps. The contemporary conventional model, used by state agencies, seems to be simple to capture the nature and complexities of threats posed by NSAs. The intelligence experts and analysts need to take more pain to analyze the emerging but tough consumers of intelligence. In order to successfully adapt to a rapidly evolving environment, states need to include some of these non-traditional, transnational actors in their sphere to successfully meet the evolving security threats outside the traditional security context.

References

Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation.

Bozeman, A. (1988). Political intelligence in non-western societies. *Comparing Foreign lntelligence (Washington, D.C.: National Strategy Information Center, 1985)*, 115-55.

Bell, J. B. (1994). The armed struggle and underground intelligence: an overview. *Studies in Conflict & Terrorism*, *17*(2), 115-150. https://doi.org/10.1080/10576109408435949

Buffaloe, D. L. (2006). *Defining asymmetric warfare*. Arlington, VA: Institute of Land Warfare, Association of the United States Army.

Bussolati, N. (2015). "The Rise of Non-State Actors in Cyberwarfare." *Cyber War: Law and Ethics for Virtual Conflicts,* (Oxford University Press, 2015), pp. 102-126.

Clough, C. (2004). Quid pro quo: The challenges of international strategic intelligence cooperation. *International journal of intelligence and counterintelligence*, *17*(4), 601-613. https://doi.org/10.1080/08850600490446736

De Torrente, N. (2004). Humanitarian action under attack: reflections on the Iraq war. *Harv. Hum. Rts. J.*, *17*, 1.

Finnemore, M., and Barnett, M.N. (2004). *Rules for the world: international organizations in global politics*. Cornell University Press.

Gentry, J. A. (2016). Toward a Theory of Non-State Actors' Intelligence. *Intelligence and National Security*, *31*(4), 465-489.https://doi.org/10.1080/02684527.2015.1062320

Grigat, S. (2014). Educating into liberal peace: the International Crisis Group's contribution to an emerging global governmentality. *Third World Quarterly*, *35*(4), 563-580. https://doi.org/10.1080/01436597.2014.924061

Human Rights Watch. (2015). *World Report 2015: Events of 2014*. Policy Press.

Harber, J. R. (2009). Unconventional spies: The counterintelligence threat from non-state actors. *International Journal of Intelligence and CounterIntelligence*, *22*(2), 221-236.https://doi.org/10.1080/08850600802698200

Krause, K., and Williams, M.C. (1996). Broadening the agenda of security studies: Politics and methods. *Mershon international studies review*, *40*(Supplement_2), 229-254.

Keck, M. E., and Sikkink, K. (1999). Transnational advocacy networks in international and regional politics. *International social science journal*, *51*(159), 89-101.

Rumsfeld, D. (2011). *Known and unknown: A memoir*. Penguin, p. 390.

Strachan-Morris, D. (2019). Developing theory on the use of intelligence by non-state actors: five case studies on insurgent intelligence. *Intelligence and National Security*, *34*(7), 980-984. https://doi.org/10.1080/02684527.2019.1672034

Simons, G. (2014). The International Crisis Group and the manufacturing and communicating of crises. *Third World Quarterly*, *35*(4), 581-597.

Terry, F. (2013). Condemned to Repeat? In *Condemned to Repeat?* Cornell University Press. https://doi.org/10.7591/9780801468643

Williams, P. (2008). Violent non-state actors and national and international security. *International Relations and Security Network*, *25*, 1-21.

Wege, C. A. (2018). The Changing Islamic State Intelligence Apparatus. *International Journal of Intelligence and CounterIntelligence*, *31*(2), 271-288.

Bibliography

Applegate, S. (2011). Cybermilitias and political hackers: Use of irregular forces in cyberwarfare. *IEEE Security & Privacy*, *9*(5), 16-22.

Bitton, R. (2019). Getting the right picture for the wrong reasons: intelligence analysis by Hezbollah and Hamas. *Intelligence and National Security*, *34*(7), 1027-1044.https://doi.org/10.1080/02684527.2019.1668717

Bamford, B. W. (2005). The role and effectiveness of intelligence in Northern Ireland. *Intelligence and National Security*, *20*(4), 581-607. https://doi.org/10.1080/02684520500425273

Bitton, R. (2013). The legitimacy of spying among nations. *Am. U. Int'l L. Rev.*, *29*, 1009.

Craig, T. (2018). "You will be responsible to the GOC." Stovepiping and the problem of divergent intelligence gathering networks in Northern Ireland, 1969–1975. *Intelligence and National Security*, *33*(2), 211-226. https://doi.org/10.1080/02684527.2017.1349036

Crenshaw, M., Dahl, E., & Wilson, M. (2017). Jihadist terrorist plots in the United States.

Dijkzeul, D. (2003). Fiona Terry, Condemned to Repeat: The Paradox of Humanitarian Action. *Ethics, Policy and Environment*, *6*.

DeLuca, C. D. (2013). The need for international laws of war to include cyber attacks involving state and non-state actors. *Pace Int'l L. Rev. Online Companion*, ii.

Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. M. F. (2009). Tracking ghostnet: Investigating a cyber espionage network.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, *239*, 288.

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). IGI Global.

Finnemore, M., and Sikkink, K. (1998). International norm dynamics and political change. *International organization*, *52*(4), 887-917.

Feinstein, B. A. (1985). The Legality of the use of Armed Force by Israel in Lebanon—June 1982. *Israel Law Review*, *20*(2-3), 362-396.

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security & Privacy*, *6*(1), 61-64. https://doi.org/10.1109/MSP.2008.8

Gill, P., and Phythian, M. (2018). *Intelligence in an insecure world*. John Wiley & Sons.

Grabo, C. (2010). *Handbook of warning intelligence: Assessing the threat to National Security* (Vol. 12). Scarecrow Press.

Gentry, J. A., & Spencer, D. E. (2010). Colombia's FARC: A Portrait of Insurgent Intelligence. *Intelligence and National Security*, *25*(4), 453-478. https://doi.org/10.1080/02684527.2010.537024

Greenberg, A. (2010). WIKILEAKS' JULIAN ASSANGE HE WANTS TO SPILL YOUR CORPORATE SECRETS The latest giant data dump, of American diplomatic cables, has stunned the world. Now he's threatening leaks of damaging documents on companies. *Forbes*, 70.

Gentry, J. A. (2015). Warning Analysis: Focusing on Perceptions of Vulnerability. *International Journal of Intelligence and CounterIntelligence*, *28*(1), 64-88. https://doi.org/10.1080/08850607.2014.962354

Hvistendahl, M., (2010). China's Hacker Army, Foreign Policy. https://foreignpolicy.com/2010/03/03/chinas-hacker-army/

Ilardi, G. J. (2009). Al-Qaeda's counterintelligence doctrine: the pursuit of operational certainty and control. *International Journal of Intelligence and CounterIntelligence*, *22*(2), 246-274. https://doi.org/10.1080/08850600802698226

Jervis, R. (2010). Why intelligence and policymakers clash. *Political Science Quarterly*, *125*(2), 185-204. https://www.jstor.org/stable/25698994

Keck, M. E., & Sikkink, K. (1998). *Activists beyond borders: Advocacy networks in international politics*. Cornell University Press.

Karatzogianni, A. (2013). Blame it on the Russians: tracking the portrayal of Russian hackers during cyber conflict incidents. In *Violence and War in Culture and the Media* (pp. 237-262). Routledge.

Krause, L. B. (1996). Insurgent intelligence: The guerrilla grapevine. *International Journal of Intelligence and CounterIntelligence*, *9*(3), 291-311: https://doi.org/10.1080/08850609608435319

Maguire, K. (1990). The Intelligence War in Northern Ireland. *International Journal of Intelligence and CounterIntelligence*, *4*(2), 145-165. https://doi.org/10.1080/08850609008435136

Metasploit. Available: http://www.metasploit.com/

Mobley, B. W., and Ray, T. (2019). The cali cartel and counterintelligence. *International Journal of Intelligence and CounterIntelligence*, *32*(1), 30-53. https://doi.org/10.1080/08850607.2018.1522218

Reynolds, G. H. (2004). The Blogs of War: How the Internet is reshaping foreign policy. *The National Interest*, (75), 59-64.

Schaller, D. J. (2008). From the Editors: Kenya—another Rwanda? https://doi.org/10.1080/14623520802305651

Strachan-Morris, D. (2019). 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), 985-998. https://doi.org/10.1080/02684527.2019.1668714

Staniland, P. (2012). Organizing insurgency: Networks, resources, and rebellion in South Asia. *International Security*, *37*(1), 142-177.

Tantalakis, E. (2019). Insurgents' intelligence network and practices during the Greek Civil War. *Intelligence and National Security*, *34*(7), 1045-1063. https://doi.org/10.1080/02684527.2019.1668718

Warner, M. (2007). Wanted: A Definition of. "*Intelligence, Understanding our Craft.*" *Studies in Intelligence*, *46*.

Williams, P. (2008). Violent non-state actors and national and international security (Zurich: International Relations and Security Network).

Zegart, A. B. (2009). Spying blind. In *Spying Blind*. Princeton University Press.

Zisser, E. (2003). Syria and the United States: Bad habits die hard. *Middle East Quarterly*.

About the Author

Zunaira Ali Khan has completed her masters in Intelligence and Security Studies from Salford University, United Kingdom. As a policy and intelligence analyst, security consultant, and counter-terrorism specialist, her focus has been on developing target-oriented strategies to produce innovative solutions to existing challenges and threats. In addition, she will be the first Pakistani female to work on the role of women in intelligence in post-Cold War and 9/11 era and how they are working beyond traditional setting today. She has also completed her project on "Vetting Process" with Royal Air Force and Ministry of Defense at United Kingdom and become the Alumni of Common Mission Project where she delivers about Hacking for Ministry of Defense. https://www.salford.ac.uk/news/students-develop-solutions-for-real-life-defence-scenarios-for-the-ministry-of-defence