1

Contemporary Conflict: The Role of Hybrid and Asymmetric Threats

Matthew PIERRO

Abstract: In recent decades, the international stage has witnessed warfare's evolution away from conventional tactics. Whereas historically rivaling nation-states dueled on rigid battlefields to declare a winning power, modern tactics have blurred the lines between war and peace while removing definite fronts, actors, and necessary capabilities. This is representative of modern-day asymmetric threats: used generally by weaker actors in conflict to exploit vulnerabilities in a more powerful opponent, these strategies circumvent direct confrontation while being unconventional, irregular, and difficult to combat. In unison with traditional war tactics, these characterize hybrid warfare which combines asymmetric and conventional aspects of conflict. This paper will examine asymmetric and hybrid threats, their status modeling conflict in the 21st century, and the actors, both state and non-state, that drive their use. Further, a variety of case studies will be examined from which recommendations to combat asymmetric and hybrid tactics will be made.

Keywords: asymmetric threats, hybrid warfare, state, non-state actors, conventional warfare, cyber attacks

Introduction

In the most elementary sense, warfare can be framed by the notion of opposition and the clash of opposing ideological blocs. This concept is neither new nor uniform: warfare has long been subject to evolutionary forces and its existence has been defined according to a variety of historical and present perspectives. Carl von Clausewitz, a Prussian general and military theorist active during the Napoleonic Wars,[1] provided several definitions of **warfare**: once as "*the continuation of politics by other means*"[2], while later as "*...nothing but a duel on an extensive scale...an act of violence intended to compel our opponent to fulfill our will",*[3] and "*...a natural part of human life.*"[4]. This implication of warfare as state-dominated[5] was a product of conventional tactics prominent in Clausewitz's era. Nonetheless, to many, the prevailing perception of warfare is similarly conventional in nature. Military historian John Keegan proposed this in his **political-rationalist theory of war**[6], saying "*[warfare] is assumed to be an orderly affair in which states are involved, in which there are declared beginnings and ends, easily identifiable combatants, and high levels of obedience by subordinates*."[7]. Per Keegan, this theory deals poorly with non-state and non-conventional tactics, the subject of this paper[8].

The rationalist theory finds company in academic literature. Jean-Jacques Rousseau, a Genevan philosopher and enlightenment thinker[9], argued warfare as "*...a relation, not between a man and a man, but between State*

---

[1] Beatrice Heuser. *Reading Clausewitz*. London: Pimlico, 2002.

[2] Alexander Mosely. "The Philosophy of War". Internet Encyclopedia of Philosophy. Accessed August 24, 2020. https://iep.utm.edu/war/.

[3] Jordan Lindell. "Clausewitz: War, Peace and Politics". E-International Relations, November 26, 2009. https://www.e-ir.info/2009/11/26/clausewitz-war-peace-and-politics/.

[4] Ibid.

[5] Alexander Mosely. "The Philosophy of War".

[6] Alexander Mosely. "The Philosophy of War".

[7] Ibid.

[8] Ibid.

[9] Christopher Bertram,. "Jean Jacques Rousseau". Stanford Encyclopedia of Philosophy. Stanford University, May 26, 2017. https://plato.stanford.edu/entries/rousseau/.

and State."[10]. Even Webster's Dictionary, a supposed arbitrator of word usage, defines war as "*a state...of conflict between states or nations.*"[11]. Conventional warfare fits within these classifications: global security has historically evolved around the clashes of nation-states and their militaristic ventures. The end of the 20th century and notably the Cold War, however, has demonstrated a dramatic shift in the sphere of conflict.

Witness to increasingly powerful nation-states with numerically extravagant armies and weapon arsenals, pure conventional warfare has lost its position as a viable means of completing political goals. As of January 2019, the United States military budget exceeded $700 billion dollars[12]. When accounting for inflation, this exceeds the Cold War average for the United States by over $100 billion[13]. Boasting a military of this strength, conventional warfare with the United States is not a practical strategy. The disparity is blatant in the on-going conflict in Iraq: in 2019, Iraq's military budget valued roughly $6.7 billion in US dollars, a fraction of the resources wielded by the United States[14]. As such, counters to U.S. offensive attacks (such as the assassination of Iranian commander Qassem Soleimani[15], asymmetrical itself) include mass demonstrations and a rocket attack on the U.S. Embassy in Baghdad[16]. In sum, warfare has been forced to adapt to the powers that participate in it. Nonetheless, warfare represents more than the individuals or weapons involved: it is the theatre in which oppos-

---

[10] Alexander Mosely. "The Philosophy of War".

[11] "War". Merriam-Webster. Merriam-Webster. Accessed August 24, 2020. https://www.merriam-webster.com/dictionary/war.

[12] Miller, James N., and Michael O'Hanlon. "Quality over Quantity: U.S. Military Strategy and Spending in the Trump Years". *Foreign Policy at Brookings*, January 2019, 1–9.

[13] Ibid, 2.

[14] "Iraqi Defense Market Outlook to 2024 – Iraqi Defense Expenditure Expected to Record a CAGR of 5.5% Over 2020–2024". GlobeNewswire News Room. Research and Markets, December 16, 2019. https://www.globenewswire.com/news-release/2019/12/16/1961172/0/en/Iraqi-Defense-Market-Outlook-to-2024-Iraqi-Defense-Expenditure-Expected-to-Record-a-CAGR-of-5-5-Over-2020-2024.html.

[15] Felbab-Brown, Vanda. "Stuck in the Middle: Iraq and the Enduring Conflict between United States and Iran". Brookings. Brookings Institute, January 29, 2020. https://www.brookings.edu/blog/order-from-chaos/2020/01/29/stuck-in-the-middle-iraq-and-the-enduring-conflict-between-united-states-and-iran/.

[16] Ibid.

ing values clash, and in modern society it has morphed into a path around the stalemate between powerful national armies.

Definitions: Asymmetric Threats

Referenced above, select nation-states dominate military spending (and generally global conflict). A prominent example is the United States, whose national defense budget constitutes nearly 40% of global military spending while their allies account for (roughly) another third.[17] This accumulation of force proves counter to deterrent efforts: according to the Serbian *Report of the Quadrennial Defense Review*, released in May 1997[18], U.S. dominance in the conventional military arena may encourage adversaries to use such asymmetric means[19]. Thus, the concept of **asymmetric threats** was introduced, proposed as *a strategy to avoid direct military confrontation with the U.S. or to disrupt U.S. commands, controls, communication systems, and alliances*[20]. Steven Metz, an American national security expert at the U.S. Army War College[21], critiqued this nation-specific definition and proposed a more complete definition of asymmetric strategy: "*[in military affairs] asymmetry is acting, organizing, and thinking differently than opponents to maximize relative strengths, exploit opponent's weaknesses or gain greater freedom of action*."[22]. Contrary to nation-states in the upper echelons of military spending, weaker sides in conflict must circumvent direct attacks in favor of unexpected tactics, due both to their own shortcomings and to the superiority of their opponent[23]. These

---

[17] James Miller, N., Michael O'Hanlon. "Quality over Quantity", 2.

[18] Milica Ćurčić. "Asymmetric Threats in Security Studies". *Thematic Collection of Articles – Asymmetry and Strategy*, 2018, 17–29.

[19] Ibid, 20.

[20] Ibid, 20.

[21] "Steven Metz". Strategic Studies Institute. US Army War College. Accessed August 24, 2020. https://ssi.armywarcollege.edu/faculty-staff/author-bio-metz/?q=543.

[22] Milica Ćurčić. "Asymmetric Threats", 21.

[23] Nikola Brzica. "Understanding Contemporary Asymmetric Threats". *Croatian International Relations Review* 24, no. 83 (October 29, 2018): 34–51. https://doi.org/10.2478/cirr-2018-0013.

asymmetric approaches employ innovative, nontraditional tactics, and weapons or technologies that are irregular in nature.

Asymmetric threats vary across a multitude of platforms, including disinformation campaigns, terrorism, and cyberattacks. Importantly, these tactics exist under the threshold for conventional conflict while still destabilizing governments, alliances, or organizations[24]. According to the Ministry of Defense in Serbia, certain characteristics are inherently asymmetric when:

1. considered unusual from a conventional point of view (i.e. torture);
2. irregular in the sense that they violate treaties or laws of armed conflict;
3. depart from war as previously understood, (as in flying planes into buildings);
4. leveraged or specialized against assets;
5. difficult to respond to proportionally, creating a situation where military intervention in response seems inhumane or cruel;
6. having unforeseen circumstances, typical of an event or attack not previously used[25].

Stephen Blank, a Senior Fellow at the Foreign Policy Research Institute and published author on asymmetric threats, presents another interpretation of asymmetry, labeled "Blank's Theory."[26]. This classifies asymmetric threats within five dimensions:

1. they are threats of non-conventional nature;
2. they are designed to mislead the opponent;
3. they can be used by both state and non-state actors;
4. they do not imply confrontation, and;
5. they reflect the opponent's strategy[27].

---

[24] Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence". *Alliance for Securing Democracy*, no. 031 (June 2018): 1–7.

[25] Milica Ćurčić. "Asymmetric Threats", 24.

[26] "Stephen Blank". Foreign Policy Research Institute, April 24, 2020. Accessed August 24, 2020. https://www.fpri.org/contributor/stephen-blank/.

[27] Iskren Ivanov, Velizar Shalamanov. "NATO and Partner Countries Cooperation in Countering Asymmetric and Hybrid Threats in South Eastern Europe's Cyberspace". *Towards Effective Cyber Defense in Accordance with the Rules of Law* 149 (2020): 59–70.

In both scenarios, these tactics are intangible and entirely flexible, creating military action that is unpredictable, irregular, and difficult to combat.

Definitions: Hybrid Warfare

Hybrid warfare exists in concert with asymmetric threats, blending conventional and irregular tactics[28]. In this sense, **hybrid warfare** *combines military and non-military as well as covert and overt means, fusing conventional capabilities with less-conventional ones* such as terrorist acts and criminal activities[29]. Franck Hoffman, a Distinguished Research Fellow with the Institute for National Strategic Studies[30], builds from this definition: hybrid warfare incorporates different modes of warfare (both conventional and asymmetric capabilities), therefore utilizing synergistic efforts that are simultaneous, fused, and subordinated to one command unit[31].

According to some military experts, this unconventional theatre of conflict can further be described as the "**Gray Zone**" of warfare, characterized by "*intense political, economic, informational and military competition more fervent than steady-state diplomacy, yet short of conventional war*"[32], while employing *small-footprint, low-visibility operations often of a covert or clandestine nature*[33]. This hybrid zone utilizes operations below internationally recognized thresholds and conventional, on-the-ground tactics. Though hybrid tactics are traditionally linked to non-state actors (terrorist organizations, for example) waging wars against more powerful foes,

---

[28] Brittany Beaulieu, David Salvo. "NATO and Asymmetric Threats", 2.

[29] Laura-Maria Herta. "Hybrid Warfare – A Form of Asymmetric Conflict". *International conference KNOWLEDGE-BASED ORGANIZATION* 23, no. 1 (July 20, 2017): 135–43. https://doi.org/10.1515/kbo-2017-0021.

[30] "Frank G. Hoffman". Foreign Policy Research Institute, May 7, 2020. https://www.fpri.org/contributor/frank-hoffman/.

[31] Laura-Maria Herta. "Hybrid Warfare", 138.

[32] Charles T. Cleveland, Charles T. Connett, Will Irwin, Joseph L. Votel,. "Unconventional Warfare in the Gray Zone". Joint Force Quarterly. National Defense University Press, January 1, 2016. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

[33] Ibid.

Hoffman argues that hybrid wars do not supplant conventional warfare nor relegate future threats to sub-state actors[34]. To this point, the Russian annexation of Crimea in 2014 and subsequent cyberattacks, media manipulation, and criminal agitation have been increasingly cited by policy experts (and contested by many others) as a prominent nation-state fusing conventional and asymmetric means under one command[35]. Additionally, operating in the Gray Zone, the United States countered the September 11th terrorist attacks with small special operation forces (SOF), carrier and land-based airstrikes, and indigenous Afghan fighters to depose the illegitimate Taliban government giving refuge to al-Qaeda[36]. Alongside their asymmetric means, the U.S. "boots on the ground" presence of roughly 350 SOF and other operatives made this a hybrid approach[37]. Either state or non-state, consensus acknowledges hybrid warfare's combination of tactics utilized, some conventional and some asymmetric, and the strategically and simultaneously coordinated efforts unlike wars of the past[38].

The History of Conventional Warfare

At the beginning of the 21st century, **conventional warfare** was loosely defined as the *confrontation of two or more countries to defeat the other through the use of armed forces*[39]*.* More specifically, conventional warfare can be examined as *military action supported by economic pressure, information relations, and diplomacy from the state*. Through conventional political channels the government guides operations, the population provides the productive means, and the military uses them in conflict[40].

---

[34] Laura-Maria Herta,. "Hybrid Warfare", 138.

[35] Ibid, 135.

[36] Charles T. Cleveland, et al. "Unconventional Warfare".

[37] Ibid.

[38] Ahmed Salah Hashim. "State and Non-State Hybrid Warfare". Oxford Research Group, May 21, 2018. https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare.

[39] Huseyin Kuru. "Evolution of War and Cyber-Attacks in the Concept of Conventional Warfare". *Journal of Learning and Teaching in Digital Age*, 2018, 12–20.

[40] Nikola Brzica. "Understanding Contemporary Asymmetric Threats", 39.

This strategy has largely defined historical warfare. In 1945, United States forces, under the command of General Douglas MacArthur, approached Manila, the capital of the Philippines, in an attempt to eradicate Japanese presence from the island[41]. Japanese forces intended to defend the city, and in the face of tremendous ground casualties, American air commanders persisted in requesting General MacArthur to approve aerial bombardment to assist U.S. ground troops. MacArthur repeatedly denied the request, stating that while Japanese forces would likely be killed, so too would innocent Filipino civilians[42]. Without aerial support, both sides suffered heavy casualties, though the United States prevailed in capturing the city. Nonetheless, as MacArthur argued, the world would have reacted in horror had the U.S. employed aerial forces[43]. Circumventing the principles of conventional warfare was an unacceptable cost.

The complex history of conflict provides context for this reluctance to engage in any tactics deemed "irregular." Constructed in academic literature, the classification of warfare strategy divides warfare into four "generations", (five phases)[44]. Each generation features radically different warfare strategy: tactics conveyed in Manila have few parallels to methods embraced by the Greeks or modern Iraqi fighters. The generations include:

1. Wars before nation-states;
2. "Classical Warfare" (Generation 1), including the Napoleon wars and embracing lined arrangements of musketmen on battlefields;
3. "All Together Industry" (Generation 2), including World War I as the industrial revolution and wider railroad availability ushered in auxiliary and infantry units;
4. "Maneuver Wars" (Generation 3), extending back to WWII and embracing "blitzkrieg" strategies targeting the weakest part of an enemy;
5. "Unconventional Wars" (Generation 4), including the aftermath of September 11th and the Iraq and Afghanistan occupations[45].

---

[41] William J. Fenrick. "The Rule of Proportionality and Protocol in Conventional Warfare". *Hein Online*, 1982, 91.

[42] Ibid, 91.

[43] Ibid, 91.

[44] Huseyin Kuru. "Evolution of War", 13.

[45] Ibid, 13.

Evident above, the fourth generation departs quite extremely from prior wars and encompasses asymmetric and hybrid methods unique to modern conflict. A 1989 article in the Marine Corps Gazette (a professional journal for the US Marines disseminating military art and science)[46] introduced the concept of "**fourth generation warfare**" as *warfare that is widely dispersed and undefined, a vanishing distinction between war and peace, non-linear to the point of no definable fronts, and losing the distinction between "civilian" and "soldier."*[47]. This centers on the ability of weaker powers to combine conventional and irregular tactics to pose a legitimate threat to an opponent's political will. As such, the fourth generation (constituting hybrid warfare) does not attempt to win by defeating an enemy's military forces, but through hybrid tactics aimed at an enemy's political will[48].

Warfare's Transition

As warfare progresses, the question remains: why are asymmetric and hybrid strategies dominating global conflict? Curiously, the answer lies in defensive efforts against these tactics: extreme discrepancies between actors' military capabilities has incentivized the use of asymmetric and hybrid threats[49]. In other words, there is a disparity between actors with the capacity to accumulate large armies, and those without. This has created an environment where less powerful actors must engage in hybrid tactics to eradicate inequality[50]. The U.S. and its allies best represent this, with their national budgets constituting 40% and roughly a third of global spending[51]. "Weaker" nation-states, which qualifies nearly the entire world in comparison, cannot compete through conventional channels with the west. Thus, historical wars pitting two nations against each other on a battlefield have been rendered obsolete.

---

[46] "Marine Corps Gazette". Marine Corps Gazette | Small Wars Journal. Accessed August 24, 2020. https://smallwarsjournal.com/author/marine-corps-gazette.

[47] Herta, Laura-Maria. "Hybrid Warfare", 137.

[48] Ibid, 137.

[49] Huseyin Kuru. "Evolution of War", 14.

[50] Ibid, 14.

[51] James N. Miller and Michael O'Hanlon. "Quality over Quantity", 2.

Inequality in military capacity is not the lone transforming force: **the doctrine of mutually assured destruction (MAD)** is an *evolutionary defense policy based on the logic that neither the United States nor its adversaries would start a nuclear war as the other would retaliate massively, with nuclear weapons potentially destroying the entire world*[52]. This doctrine applies narrowly to nations of nuclear capacity, yet serves as an additional deterrent to conventional war. In sum, post-Cold War society has forced non-state and nation-state actors to pursue irregular tactics in warfare to combat an escalating arms race between opposing ideological blocs. These conditions are directly responsible for the transition away from conventional warfare, and their maintenance on a global scale will only serve as additional encouragement of the usage of asymmetric threats and hybrid tactics.

Though conventional war has seen a decline in modern conflict, it remains in use for global powers against weaker nations and vice versa. Demonstrated by trends outlined above, this type of warfare is becoming difficult, outdated, and ineffective. Nonetheless, especially alongside hybrid tactics, conventional warfare can be advantageous. The U.S. government has engaged in aspects of conventional warfare against the Ba'ath Party government in Iraq[53]. This nation-state against nation-state, enemy-specific attack was replicated to an extent in Crimea in 2014, where Russian troops invaded the peninsula and combined hybrid with conventional tactics[54]. These examples demonstrate increasing hybrid tactics, but also the need for nations to remain vigilant against conventional ones.

Actors of Warfare

From the perspective of conflict analysis, **actors** in warfare are *all those engaged in or being affected by conflict,* otherwise considered "*who*

---

[52] Alan J. Parrington. "Mutually Assured Destruction Revisited". *Airpower Journal*, 1997, 4–19.

[53] David L. Buffaloe. "Defining Asymmetric Warfare". Association of the United States Army, November 15, 2017. https://www.ausa.org/publications/defining-asymmetric-warfare.

[54] Taras Kuzio and Paul D'Anieri. "Annexation and Hybrid Warfare in Crimea and Eastern Ukraine". E-International Relations, July 5, 2018. https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/.

intervenes"[55]. John McDonald, a former U.S. Ambassador, diplomat, and peacebuilding expert[56]. introduced the concept of "Multi-Track Diplomacy" which distinguished nine tracks of actors. From this, two significant sub-groups emerged: "states/governments" and "non-state actors", with several broad categories stemming below each[57]. For the purpose of this paper, actors will refer to these large sub-groups, characterizing each actor as being tied (or not being tied) to a sovereign nation, therefore as "state", or "non-state." Though state actors are capable (and willing) to organize asymmetric efforts, their position on asymmetric conflict generally opposes non-state's and therefore are considered separately.

The **state** *contains traditional military and political authority which relies on its own economic and diplomatic power*[58]. Comparatively, **non-state actors** *employ a non-hierarchical structure of motivated "cells" with common motivations and political goals*[59]. This compartmentalization works in favor of organizations such as terrorist groups that must leave potential vulnerabilities decentralized. These actors are inherently different, crucially so in regards to sovereignty: according to a report released by the National Intelligence Council, non-state actors are non-sovereign entities and therefore are not legitimized on a global stage[60]. Nonetheless, comprehension of both actors is vital to discussion surrounding asymmetric and hybrid warfare. Russia, a powerful nation-state, and the Islamic State, a terrorist non-state actor, operate vastly differently despite both engaging in hybrid and asymmetric tactics, and both must be understood in prospective defensive efforts.

---

[55] "Actors and Tactics of Conflict Interventions (Civilian Intervention and Nonviolent Intervention)". Irénées: A Website of Resources for Peace. Accessed August 25, 2020. http://www.irenees.net/bdf_fiche-analyse-659_en.html.

[56] "In Memoriam: Ambassador John W. McDonald". United States Institute of Peace, May 30, 2019. https://www.usip.org/press/2019/05/memoriam-ambassador-john-w-mcdonald.

[57] "Actors and Tactics" Irénées.

[58] Nikola Brzica. "Understanding Contemporary Asymmetric Threats", 41.

[59] Ibid, 41.

[60] "Non-State Actors: Impact on International Relations and Implications for the United States". National Intelligence Council. National Intelligence Officer for Economics and Global Issues, August 23, 2007. https://www.dni.gov/files/documents/nonstate_actors_2007.pdf.

State Actors

State-actors represent the traditional consolidation of authority and the central elements of the international system[61]. A **state** is defined as *a politically organized body of people at an established territory with public authority and the legal use of force and violence*[62]. This monopoly on violence differentiates sovereign states from other actors that lack similar territory or authority[63]. Importantly, nations must be recognized by other sovereign states through international channels, such as the United Nations, to achieve this status. Further, the state must have public authority, governing tools, and territory and population to rule[64]. Legality aside, certain states exercise conflict beyond their borders, wielding armies large enough to warrant conventional conflict or relying on hybrid and asymmetric means to circumvent international laws that would inflict potential consequences.

State Actors: Libya and Russia

Nation-states are capable of abusing asymmetric tactics to achieve political goals, as exemplified by the Libyan Civil War between the internationally recognized Government of National Accord and the Libyan national Army[65]. Neighboring nations and global powers have become increasingly involved through asymmetric tactics. For example, both Turkey and Russia have trained mercenaries to be dispatched in Libya[66]. Elsewhere, Turkey and the UAE have continued devastating airstrikes, jockeying over (what

---

[61] "State Actors – Actors in International Relations". Coursera. International Relations Theory. Accessed August 16, 2020. https://www.coursera.org/lecture/international-relations-theory/state-actors-0GRQe.

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] Nathan Vest and Colin P. Clarke. "Is the Conflict in Libya a Preview of the Future of Warfare?" Defense One. Defense One, June 2, 2020. https://www.defenseone.com/ideas/2020/06/conflict-libya-preview-future-warfare/165807/.

[66] Ibid.

some consider) the largest drone war in the world[67]. Disinformation campaigns have increased alongside physical strikes, particularly through bots and trolls in favor of the Libyan national Army deployed by Russia, the UAE, and Saudi Arabia[68]. These developments demonstrate modern "wars at distance": technology, social media, proxy wars, and private armies of mercenaries allow states to participate in conflict and destabilize opposing governments without actively engaging in the carnage.

Whereas the Libyan conflict featured nation-states and non-state actors in coordination, Russia's aggressive international actions have demonstrated the capability for a state to execute hybrid and asymmetric attacks without international assistance and without a pre-existing conflict. Through tactics of disinformation, cyberwarfare, and support for foreign political movements, Russia has tactfully played the line below conventional war[69]. In 2017, a disinformation campaign (widely believed to originate in Russia) falsely accused German soldiers deployed in Lithuania of raping a teenage girl, stirring anti-soldier sentiments[70]. Elsewhere, Russian disinformation efforts have targeted North Atlantic Treaty Organization (a political and military alliance seeking freedom and security for its members, shortened as NATO)[71] partner countries to undermine citizen's support for joining the alliance, in addition to cyberattacks targeting the Democratic National Convention in the United States, leaking vulnerable information online that jeopardized U.S election security[72]. In these scenarios, Russian efforts sought destabilization, manipulation of citizens, and vulnerability in nations Russia considers as global foes. This is evident further in Russian overt and covert support for political groups, funding a French far-right national group and supporting networks of non-governmental organizations shifting European public opinion towards a positive view of Russian politics[73].

---

[67] Ibid.

[68] Ibid.

[69] Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats", 2.

[70] Ibid, 3.

[71] "NATO / OTAN". What is NATO? North Atlantic Treaty Organization. Accessed August 25, 2020. https://www.nato.int/nato-welcome/index.html.

[72] Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats", 3.

[73] Ibid, 3.

Russia is just one example of a prominent nation-state engaging in hybrid tactics. Both in states with the capabilities for conventional warfare and those who fight proxy wars abroad, asymmetric threats have proven effective in causing mass disruption to national governments and supra-national organizations. Thus, as their effectiveness remains consistent on a global stage and their methods remain under the threshold for conventional war, defense strategies must be adjusted to fully combat asymmetric means and security experts must acknowledge the threat that nation-states pose.

Non-State Actors

Non-state actors are defined as *non-sovereign entities that exercise political, economic, or social control at either a national or international level*[74]. These actors operate outside the confines of a conventional state, pursuing their political agendas through means more difficult to contain or regulate. Forming a consensus on non-state actors has proven difficult for scholars and national governments alike. Nonetheless, a flexible list includes the following, per the United States National Intelligence Council:

1. multinational corporations and organizations;
2. nongovernmental organizations (NGOs);
3. super-empowered individuals;
4. terrorist organizations;
5. criminal networks[75].

This is not a summative list, but rather an introduction to several non-state actors in global politics. However, in the context of hybrid warfare, terrorist organizations and criminal networks participate as the most important actors.

In examining conflict, two main groups of non-state actors can be identified in accordance with their operating tendencies. **Non-violent non-state actors,** including multinational corporations, *can have profound effects on a nation's economic or political state, with the potential to also exert*

[74] "Non-State Actors" National Intelligence Council.

[75] "Non-State Actors" National Intelligence Council.

harmful influence or undue control over a region[76]. **Violent non-state actors**, however, generally *present national and international consequences of extreme magnitude*, and are *characterized by their ability to rely on violence and force through asymmetrical channels*[77]. Inclusion as a violent non-state actor ranges from militias and warlords, to terrorist and criminal gangs, and insurgents and transnational criminal groups[78]. As previously theorized, the usage of asymmetric and hybrid threats stems from a disadvantaged military position, where non-state actors or weaker states must approach warfare through irregular and unexpected tactics to sustain victory. This becomes evident when examining specific examples of non-state actors and their methods, such as terrorist organizations operating in the Middle East, Africa, or South East Asia.

Non-State Actors: Terrorist Organizations

On September 11th, 2001, the actualization of asymmetric threats posed by non-state actors was realized. Hijacking commercial aircrafts and piloting them towards buildings symbolizing the global authority of the U.S. departed quite extremely from warfare in the trenches, and this shifted U.S. foreign policy to the primary role of counterterrorism[79]. The administration of President George W. Bush declared a "War on Terror", gathering information and targeting the terrorist non-state actors responsible, which represented the United States' own effort in hybrid warfare and dealing with non-state actors[80]. U.S. forces operated in the previously defined

---

[76] Ibid.

[77] Ibid.

[78] Thomas Risse, Tanja A. Börzel and Anke Draude. *The Oxford Handbook of Governance and Limited Statehood*, 2018.

[79] Anthony H. Cordesman. "The Lessons and Challenges of September 2011 – the New '9/11.'" The Lessons and Challenges of September 2011 – the New "9/11" | Center for Strategic and International Studies. Center for Strategic and International Studies, August 14, 2020. https://www.csis.org/analysis/lessons-and-challenges-september-2011-%E2%80%93-new-911.

[80] Anthony H. Cordesman. "The Lessons and Challenges of September 2011 – the New '9/11.'" The Lessons and Challenges of September 2011 – the New "9/11" | Center for Strategic and International Studies. Center for Strategic and International Studies, August 14, 2020. https://www.csis.org/analysis/lessons-and-challenges-september-2011-%E2%80%93-new-911.

"Gray Zone", deploying special operation forces (SOF), carrier and land-based airstrikes, and irregular Afghan fighters to depose the illegitimate Taliban government giving refuge to al-Qaeda[81].

Despite fighting occurring largely in nation-states of Iraq and Afghanistan, the perceived threats from U.S. strategy were al-Qaeda and the Taliban, emphasizing the role that non-state actors can play in global conflict and their complicated relationship with nation-states[82].

The September 11th terrorist attacks and subsequent geopolitical consequences modeled an increasing fusion of non-state and state forces. This created a gap in contemporary military terminology and strategy, filled today by the widely utilized "asymmetric and hybrid threats"[83]. Neither terrorism, the organizations behind these attacks, nor the following U.S. invasion were "new concepts" in 2001. However, combining conventional "on the ground" military action (such as the deployment of U.S. SOFs) with irregular methods of insurgency, war on information, and cyberattacks represented a departure from previous military strategy[84]. Further, despite frequent terrorist activity both prior to and since September 11th, this awoke much of the world to potential threats posed by terrorist (and generally non-state) actors such as al-Qaeda, and presently the Islamic State.

Platforms of Warfare

After the dramatic arrival of asymmetric threats in global conflict, national defense strategies eagerly rushed to identify and address potential tactics. This proclivity ran counter to an actual comprehension of the term: asymmetry quickly came to define every threat faced in international conflict and this careless application rendered the concept useless[85]. Substantive critique from academics contested the label of threats themselves as

---

81 Charles T. Cleveland, et al. "Unconventional Warfare".

82 Anthony H. Cordesman. "The Lessons and Challenges".

83 Milica Ćurčić. "Asymmetric Threats in Security Studies". 23.

84 David L. Buffaloe, "Defining Asymmetric Warfare".

85 Stephen J. Blank, *Rethinking Asymmetric Threats*. Commonwealth Institute, 2003.

asymmetric, instead of the nature of strategies utilized[86]. In reference to "platforms" of asymmetric and hybrid warfare, this paper seeks to identify and address this complaint.

The idea of "platforms of warfare" is not widely addressed in academia, and this makes asymmetric tactics difficult to reliably quantify. Therefore, this paper seeks to introduce the concept of **platforms of warfare** as *an overarching classification of asymmetric threats characterized by the nature of the threat utilized.* This definition relies on the logic that asymmetric and hybrid tactics, or "means" exist within a greater conceptual platform. For example, a cyberattack is an asymmetric threat dependent on computer technology and communication networks. From this, cyberattacks can be determined to exist within the platform of information warfare.

Beyond this, this paper acknowledges a platform widely utilized today and referenced above: information warfare. This example is not an all-encompassing list; several other platforms exist, notably terrorist activity. To maintain the scope of this paper, however, information warfare will be briefly explored while cyberattacks, a central asymmetric threat within that platform, will receive an in-depth case study.

Platforms: Information Warfare

The past few decades have revolutionized information and communication technologies in society, introducing modern telephones, radio signals, and satellites. To optimize military strategy, warfare has shifted alongside technology: broadly, **information warfare** is *a struggle over these information and communication systems*, and *the application of destructive force on a large scale against information assets and systems and against the computers and networks that support this critical infrastructure*[87]. These increased communication systems have created a societal reliance on them, leaving organizations potentially vulnerable

[86] Ibid.

[87] Brian C. Lewis, "Information Warfare". *Federation of American Scientists*, Accessed August 17, 2020. https://fas.org/irp/eprint/snyder/infowarfare.htm

to information warfare damaging or freezing their networks. However, increased communication systems can be similarly favorable to offensive information attacks: whereas once information was a tool of the state, (in certain nations it remains that way) asymmetric opponents today wield the power to make and distribute their own information to much wider audiences[88]. This ability has ushered in new areas of conflict operation, enabled states to engage in mass disinformation campaigns, and allowed wars to be fought remotely behind a monitor[89].

Commonly utilized by rogue nations or non-state actors seeking destabilization, cyberattacks and cyberwarfare are central to information warfare. These tactics represent a particularly advantageous strategy due to the limited assets they require: with secure networks and infrastructure, actors can leverage massive disruption and destabilize government networks, elections, or the networks of supranational organizations from abroad[90]. This capability of "warfare from abroad" allows states to conceal their actions or motives, avoid international consequences (such as sanctions) or prevent the carnage possible in conventional intervention.

During the Kosovo War in 1999, Serbian hackers, in concert with their Eastern European sympathizers, launched global attacks aimed at shutting down key computer systems in NATO countries[91]. Despite knowledge that this attack was not sufficient to win the war, the Serbs successfully stalled the NATO offensive and disabled temporary response and communication systems[92]. These cyberattacks are rudimentary compared to information warfare of today: among other nation-states and non-state actors, China and Russia are capable of waging catastrophic cyberattacks

---

[88] Rod Thornton, *Asymmetric Warfare: Threat and Response in the 21st Century*. Polity Press, 2007.

[89] Ibid, 62.

[90] Ray Song. Publication. *The Hermit Threat: A Historical Analysis of Cyberwarfare, Its Modern Manifestations in North Korea, and Its Implications in Global Relations of the 21st Century*, 2017.

[91] Rod Thornton. *Asymmetric Warfare*, 62.

[92] Ibid, 62.

on rival states, vastly more damaging than those utilized by Serbia in 1999. With disinformation campaigns, trained cyber experts, and the world's increasing reliance on global networks, these powers have many vulnerable targets to exploit and will continue to do so under the threshold of warfare.

As mentioned previously, information warfare is not the lone platform of asymmetric means. Though broad in scope, terrorism represents another. This includes attacks leveraged by terrorist organization, though terrorism may also result from state-waged violence through the use of weapons of mass destruction, biological weapons, attacks on critical infrastructures that society depends on, or from attacks on people and institutions of the federal government[93]. The threat of terrorism continues to loom large over the western world especially as military accumulation forces non-state actors to utilize irregular tactics. Therefore, this platform must be addressed as fervently as information warfare in an effort to stall its global rise.

Asymmetric Threat Case Study: Cyber Attacks

Cyber operations and their role in conflict represent a dramatic shift in society over the past few decades. Under the veil of anonymity and the threshold for conventional conflict, cyberattacks are an emerging asymmetric threat being utilized to create great destruction. Academia hosts several definitions for the concept of **cyberattacks**, though specifically for this paper they refer to "*...hostile acts using computer or related networks to disrupt or destroy an adversary's cyber systems or functions.*"[94]. Whereas cyberattacks refer to isolated incidents, **cyberwarfare** expands upon this concept as *"...massively coordinated digital assaults on one government by another or by large groups of citizens, as when cyber attacks are orchestrated by state-sponsored hackers against another nation's cyber*

[93] Ashton B. Carter, William J. Perry, and David Aidekman. "Countering Asymmetric Threats". *Belfer Center*, n.d., 1–10.

[94] Ray Song. *The Hermit Threat*, 2.

infrastructure."[95]. Examining these concepts, there are generally three targets of cyberwarfare:

1. information itself;
2. information processes that disseminate and analyze material of the state;
3. the infrastructure of information systems that store, transmit and process said material[96].

The utilization of cyber methods against these targets offer actors operational flexibility, convenience, and undue authority. Computer attacks can be launched remotely or anonymously so as to avoid direct consequence, while their non-physical existence offers less-able nation-states to be equally disruptive as their more-powerful counterparts[97]. Whereas traditional warfare required a level of capability to launch an attack, cyber methods have created a sphere of conflict where power can be utilized by a wide array of political instigators for damaging purposes[98]. From this, defending national security systems proves difficult, especially considering how many potential threats exist: terrorist organizations, disgruntled individuals, or even hostile nation states can overpower cyber systems manned by limited numbers.

In recent decades, Russia has utilized cyber attacks as a means of promoting their political agenda abroad. In some instances, these tactics combined with conventional conflict in the form of hybrid warfare. In 2007, following a dispute between the Estonian and Russian national governments, pro-Kremlin forces froze Estonian networks[99]. Not officially state-run, these attacks were orchestrated by non-state actors and asymmetric in quality[100]. The following year amidst the Russo-Georgian War, Russian

---

[95] Ibid., 3.

[96] "Information Warfare: Cyber Warfare Is the Future Warfare". *Global Information Assurance Certification Paper*, 2004.

[97] Ray Song. *The Hermit Threat*, 2.

[98] Ibid., 2.

[99] Ibid., 6.

[100] Ibid., 6.

criminal gangs attacked multiple Georgian government targets, marking the first time that a known cyber attack had coincided with shooting in war[101]. This utilization of asymmetric means alongside conventional strategy explicitly demonstrates hybrid warfare.

North Korea is an additional proponent of cyber attacks. Lacking strategic advantages of large enlistment numbers, foreign investments, and advanced technical equipment, North Korea uses asymmetric strategies to offset warfare disparities against more powerful opponents[102]. This has made cyber attacks a strong strategy for North Korea: cyber attacks can be conducted from abroad, require limited assets, and relies on little manpower to wreak considerable havoc abroad. Further, North Korea leverages their detachment from global cyber networks to manipulate cyber attacks as a viable strategy[103].

Recognizing their reliance on cyber attacks, the North Korean national government has made considerable efforts to funnel their brightest students into computer hacking and cyberwarfare operations[104]. Government officials select promising students in mathematics to learn computer-based warfare. These students are then trained in specialized organizations before entering computer hacking forces, the most prestigious known as Bureau 121[105]. Forces like these have been successful in enabling North Korea to engage in asymmetric combat from a distance, in soliciting funds for national use, and in incapacitating enemies of their ideology[106].

In February of 2016, $101 million dollars was taken from a New York Federal Reserve account that belonged to a Bangladesh Central Bank[107]. A single spelling error on a withdrawal request raised the alarm that prevented the

---

[101] Ibid., 6.

[102] Ibid., 8.

[103] Ibid., 8.

[104] Ibid., 9.

[105] Ray Song. *The Hermit Threat*, 9.

[106] Ibid., 9.

[107] Ibid., 10.

initial request of $1 billion from being authorized[108]. This attack, discovered to have occurred in banks in over ten other nations, was eventually signaled to have come from North Korea. However, due to a lack of physical evidence, the funds were never recovered and are potentially in circulation in North Korea markets[109]. This attack demonstrates the sheer capabilities of cyber attacks and the flexibility in their use. Rogue nation-states or non-state actors wield the capability to freeze networks, shut down entire governments, or steal significant sums of money, all without direct conflict, under the threshold of warfare, and without global repercussions.

Responses to Asymmetric and Hybrid Threats

Modern conflict's shift to asymmetric and hybrid tactics represents one of the most pressing matters in global security. Following the arrival of these tactics on the international stage, defense doctrines and recommendations were released by national and supra-national governing bodies to outline methods of prevention. These responses were preliminary in nature and are continually evaluated to properly address evolving threats. For example, increasing Russian hybrid activity has alarmed nations in Europe and NATO into further hybrid warfare prevention[110]. As these issues continue to disrupt global processes, effective responses become increasingly crucial for international security and must comprehensively address and alleviate threats posed by asymmetric tactics.

In addressing responses to asymmetric and hybrid threats, this paper will outline current European procedure. Though response strategies to these threats will vary depending on the nature of conflict to specific regions, European alliances, specifically NATO, have formulated comparatively advanced response systems that will be discussed as models for other global regions to utilize. These responses may not apply uniformly, especially considering NATO's status as a supra-national organization.

---

[108] Ibid., 10.

[109] Ibid., 11.

[110] Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats", 2–3.

Nonetheless, the principles that they rely on are crucial to combating asymmetric threats on a global level.

NATO's Response Strategy

At the 2008 Bucharest Summit, NATO presented their Comprehensive Approach Action Plan, a framework for the mobilization of military and civilian resources to resist hybrid challenges[111]. This represented a crucial first step in acknowledging the threat of asymmetric and hybrid tactics, which to that point had not entered the public sphere. In December of 2015, this progress continued: NATO adopted a strategy of confronting hybrid threats by increased partnership with the European Union (EU). This partnership included information sharing between member states, warning signs of hybrid threats at the alliance's border, and encouraging members to recognize potential vulnerabilities within their own system to Russian interference[112].

In recent years, joint-defense efforts have been expanded by both EU and NATO officials. The two alliances have coordinated response strategies and established centers dedicated to the analysis and development of hybrid defense, among them the European Center of Excellence for Countering Hybrid Threats[113]. This coordination relays joint declarations and recommendations to member states, calls on individual national governments to identify internal weaknesses, and encourages members to contribute to a greater security threshold in Europe[114]. Despite these promising advancements, it remains true that NATO defense strategies are not being optimized and they face institutional challenges to success.

Though NATO and the EU have pledged cooperation in their war on asymmetry, their efforts remain stalled by a lack of funding, a lack of membership

---

111 Ray Song. *The Hermit Threat*, 3.

112 Ibid., 3.

113 Ibid., 4.

114 Ibid., 3.

commitment, and information blocking[115]. Specifically, between the two organizations there exists no tool to share classified, high-level information crucial to alliance defense policy[116]. In situations of pressing hybrid challenges, this lack of information sharing across organizations ensures a less effective response. Attempts to promote information sharing within the organizations has proved challenging. For example, despite Russian cyber and disinformation attacks on the U.S. 2016 election, the nation shared little information with fellow NATO members[117]. Fundamentally, this hesitance makes sense: even with allies, nations are skeptical of discussing internal vulnerabilities. Nonetheless, this approach to information sharing has stunted the alliance's ability to appropriately respond to hybrid threats and create uniform responses to urgent issues[118].

Further, despite centers positioned to address asymmetric and hybrid threats, NATO's identification policy is unclear. In modern conflict, hybrid forces are commonly fused with conventional warfare and oftentimes exist without underlying conflict. Despite this common occurrence, NATO's internal framework addressing these conflict levels has no concrete response[119]. In addition, response strategies are stalled by NATO members' varying perceptions of threat regarding asymmetric tactics. Nation-states susceptible to Russian influence in Eastern Europe may call for increased protections against information warfare, while nation-states overwhelmed by migration from the Middle East in Southern Europe may wish to adjust focus to criminal activity. NATO must find a way to blend their response strategies to fit this range of issues, or else remain fractured and pulled along by their member's diverse interests. Ultimately, it proves difficult to organize an alliance on a single issue in the face of many.

---

115 Ibid., 4.

116 Ibid., 4.

117 Ibid., 4.

118 Ibid., 4.

119 Ibid., 4.

Recommendations to Asymmetric and Hybrid Threats

While malicious state and non-state actors continue to engage in asymmetric and hybrid tactics, other global actors must not be complicit in their progress and must recognize necessary procedures to be enacted. Proactively, this recognition must translate to policy and definite changes. Therefore, this paper will identify several recommendations to effectively challenge asymmetric tactics in modern society. As European responses to hybrid warfare were outlined above, a NATO-specific recommendation will be discussed. However, as recommendations are crucial to regions that do not already have functioning response systems to hybrid threats, generalized recommendation strategies will be additionally addressed.

NATO principally relies on their stated articles to govern and direct the alliance. These articles, meant to provide guidance in times of crises, are not being effectively enforced in unifying a defense strategy. NATO Article 4 states that parties (nation-states) will consult together when, in the opinion of any member, the political independence or security of a member is threatened[120]. As previously mentioned, certain NATO members have not been transparent in their struggles with hybrid threats, particularly when it exposes vulnerabilities in a nation's infrastructure or defense capabilities. Nonetheless, the alliance must invoke article 4 to enable these difficult consultations and to properly address areas in alliance security where foreign actors may be meddling. To respond effectively, individual nations should develop internal thresholds that identify asymmetric threats[121]. When crossed, this should serve as an alarm to bring the issue to the awareness of other NATO members. Then, NATO should facilitate consultations that organize effective responses to hybrid operations. In doing so, a NATO-wide response team to assist member-states struggling with conflict would be incredibly constructive for the alliance going forward[122].

---

[120] NATO. "The North Atlantic Treaty". NATO. North Atlantic Treaty Organization, April 1, 2009. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[121] Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats", 5.

[122] Ibid., 5.

Elsewhere in the world, especially in regions plagued by terroristic activity or struggling with other governmental-infrastructure, responses to hybrid and asymmetric threats are crucial in securing national defense. These recommendations are not nation or alliance-specific, but rather they represent actions that would be beneficial outside the scope of an international organization or any individual nation-state.

For an effective national response to asymmetric threats, response mechanisms must be institutionalized. There is no universal solution to asymmetric threats; even among related means, such as chemical and biological warfare, responses differ greatly and can complicate defense strategies[123]. Therefore, responses must be institutionalized by the national military and governing bodies: in doing so, doctrine, strategy, structure of armed forces, and training must be addressed in policy and procedure to ensure a timely and effective response to hybrid attacks[124]. Further, understanding that variable asymmetric means warrant varying responses, an integrated and institutionalized defense effort should incorporate two primary efforts: protection and threat management[125]. In other words, though each unique type of asymmetric attack calls for its own individualized response, a national system must be organized with responses categorized by defensive protections versus proactive threat management. Defensively, this would establish procedures in the scenario of an incoming or on-going asymmetric attack, whereas coordinating threat management systems would attempt to prevent any attacks from materializing[126]. These efforts should be coordinated with allied states and national partners to standardize responses globally.

Specific to the African subcontinent, several additional recommendations will be made to secure nations from impending hybrid and asymmetric threats. Some of these threats are contingent on region-specific qualities, however the recommendations are applicable to a global audience.

---

[123] Bruce W. Bennett, "Responding to Asymmetric Threats", Essay. In *New Challenges, New Tools for Defense Decisionmaking*, RAND Corporation, n.d.

[124] Ibid., 50.

[125] Ibid., 50.

[126] Ibid., 50.

First, nations should revisit and revise their threat-response mechanisms[127]. Threats often assume a transnational capacity, exposing weaknesses in the state. Therefore, existing institutions and defense approaches need to constantly adapt to emerging threats as they appear[128]. In states that are particularly fragmented or with less centralized governments, this revision and policymaking process should include the involvement of local or religious leaders who would be most knowledgeable of the threats their community faces[129]. Next, the coordination of efforts and existing strategies is imperative for a successful defense system. This revisits the issue of government fragmentation or decentralization: it is possible that within government bodies of a state, information sharing and communication procedures are ineffective. To improve response systems, this must be fixed: intelligence and information sharing should be streamlined to be efficient and effective in the face of emergency threats[130]. As part of this information process, warning networks and response mechanisms should be established and optimized. However, these mechanisms will only alert the acting government of a potential threat. Following, there must be some state capacity to respond to or prevent said hybrid attack from progressing. This may be in the form of increased national intelligence organizations, increased staff of intelligence operatives and state-employees, stronger cyber infrastructure, or increased military capability to deter armed threats[131].

As part of the necessity for state capacity, it is recommended that nations improve their infrastructure as a means of defense[132]. The lack of a self-sufficient economy or reliable infrastructure leaves states vulnerable to crises or attacks. For example, an attack of biological warfare might be more effective and spread more thoroughly in a state with inadequate health

---

[127] Kwesi Aning. "Confronting Hybrid Threats in Africa: Improving Multidimensional Responses". Essay. In *Future of African Peace Operations*, edited by Mustapha Abdallah, 20–37. The Nordic Africa Institute, 2016.

[128] Ibid., 30.

[129] Ibid., 31.

[130] Kwesi Aning. "Confronting Hybrid Threats in Africa: Improving Multidimensional Responses". Essay. In *Future of African Peace Operations*, edited by Mustapha Abdallah, 20–37. The Nordic Africa Institute, 2016, 31.

[131] Ibid., 32.

[132] Ibid., 32.

care[133]. As a final recommendation, both for states defending against asymmetric threats and those that utilize them in conflict, the ability to resolve conflict without intervention, warfare methods, or illegal channels is important to global peace. International diplomacy, economic relations, and strategic policymaking must be more accessible and effective. For non-state actors and nations to abandon asymmetric means, there must be legal channels for their political agendas to be processed. This should exist through international organizations, alliances, and councils meant to support weaker states.

Conclusion

Asymmetric and hybrid threats represent the present and future of global warfare. The irregular nature of these threats allows them to adapt to opposing powers in conflict, making them especially effective on the international stage. As nation-states compete to accumulate arms and deter conventional attacks, less capable actors will continue to revert to asymmetric means to exercise their political aspirations. As such, nation-states and supra-national organizations such as NATO must establish and refine response systems to defend against these tactics. Utilizing the recommendations above, states should institutionalize their responses, streamline information-sharing procedures, and develop stable infrastructure to allow for increased state capacity. Most importantly, diplomatic means and resolutions must be developed beyond intervention or asymmetric means. The global security realm must not be complacent in their battle against asymmetric war and warfare's constant development. Otherwise, as states develop the capacity to defend against current methods of cyberattacks or terrorism, other means of warfare will arise to take their place.

[133] Ibid., 32.