Journal of Military and Strategic Studies

VOLUME 21, ISSUE 1

Syria – A Hybrid War Case Study

Meredith Jones and Sascha Dov Bachmann

> Over time, this conflict has exhibited all possible guises of war: civil war, proxy war, siege warfare, cyber-warfare, and war against terror. All forms of past and present warfare seem to converge in this one conflict. A war against children, against hospitals, against cities, against first-aid workers, against memory, against justice – maybe these are more accurate titles for this war.[1]

Introduction

The continual destruction of Syria and the ongoing political stalemate has led to the complete devastation of a once beautiful country. The Syrian conflict is one that has become increasingly complex due to the large range of contending parties that include both State and non-State actors. Not only has the Syrian crisis become one the most well-documented conflicts in history, but it has also been considered the worst conflict to arise out of the so-called *Arab Spring* of 2011. Further, it has been recently labelled as one of the most sophisticated battlefields in the world,[2] simply because Syria has been

[1] Vincent Bernard, "Editorial: Conflict In Syria: Finding Hope Amid the Ruins," *International Review of the Red Cross* 99, 3(2017): p. 865.

[2] Yimin Zhou, "A Double-Edged Sword: Russia's Hybrid Warfare in Syria," *Asian Journal of Middle East and Islamic Studies* 13, 2 (2019): pp. 246, 247. (2017)

ISSN : 1488-559X

the testbed for previously untested battlefields, operational domains, and advanced weaponry. The significant media coverage of the crisis in Syria continues to illustrate the horrors that have become the everyday norm. With an estimated 470,000 people killed and 11 million displaced, the crisis has had a disastrous effect on the Syrian population of 20 million.[3] Notably, however, the extent of this conflict has travelled far beyond the borders of Syria, with the millions of displaced persons being the most apparent consequence. Despite a new decade, a long-lasting resolution remains unlikely, leaving Syria's future in the hands of opposing powers and a divided international community.

The purpose of this paper is to apply the concept of hybrid warfare to the Syrian conflict. It is the position of this paper, that Syria is a hybrid war employing all strategies contained within the wider hybrid warfare classification, such as irregular warfare, asymmetric warfare, and compound warfare. The paper first reflects on the concept of hybrid warfare, before attempting to unpack the complexities of the Syrian conflict. The second part then engages in critical analysis of how each of the hybrid warfare strategies is illustrated within this all-encompassing war through the use of various strategies and battlespaces. Ultimately, this paper aims to add valuable academic consideration to the growing body of literature surrounding the Syrian conflict, to highlight that unless consideration is given to Syria as a hybrid war, encompassing several operational strategies and numerous conflicts all contained in a single territory, there will be no successful outcome for this enduring resolution.

What is a Hybrid War?

> Hybrid warfare might warrant its recognition as a separate form of warfare, or a category of full spectrum operations. Hybrid warfare is prompt and ready to attract elements from four existing methods and categories of warfare: terrorism, counter-insurgency, asymmetric warfare, and compound warfare, where regular and irregular forces are used

[3] Bernard, "Editorial: Conflict In Syria," p. 865; Megan Specia, "How Syria's Death Toll Is Lost in the Fog of War," *The New York Times*, 13 April 2018, www.nytimes.com/2018/04/13/world/middleeast/syria-death-toll.html.

simultaneously against an opponent. This takes place while being employed by state actors or non-state actors.[4]

Hybrid warfare as a rather new concept of warfare has its origins in US military thinking and developed over the last 15 years.[5] The first mention of hybrid warfare as we understand it today emerged from Generals James N. Mattis and Frank G. Hoffman in 2005. Simultaneously a new form of Russian mixed-method warfare has evolved as Russian Hybrid Warfare and has become known as the so-called *Gerasimov doctrine*, credited to General Valery Garasimov, despite doubts over General Gerasimov's actual intent to make his thoughts on new war and its elements the basis of a new military doctrine.[6]

Some argue that hybrid warfare simply means warfare occurring across more than one dimension, which to some also include, the political, economic, and civil spheres.[7] One aspect is quite clear however, hybrid warfare blurs the line between conventional and unconventional warfare and it can blur the line between times of peace and war. Although hybrid war is not a new concept, advances in technology have allowed hybrid strategies to be executed in a new domain of warfare, mainly in regards to the cyber dimension.[8]

It can be argued, that hybrid warfare displays elements from existing categories of warfare, including irregular warfare (terrorism and counter-insurgency), asymmetric warfare, and compound warfare.[9] Added to these could be the element of legal ambiguity as a consequence or objective of hybrid warfare reminiscent of the emerging

[4] Sascha Dov Bachmann and A. B. Mosquera, "Lawfare and Hybrid Warfare: How Russia Is Using the Law as a Weapon," *Amicus Curiae* 102 (2015).
[5] Sascha Dominik (Dov) Bachmann, Andrew Dowse and Hakan Gunneriusson, "Competition Short of War – How Russia'sHybrid and Grey-Zone Warfare are a Blueprint for China's Global Power Ambitions," *Australian Journal of Defence and Security Studies* 1, 1 (2019): p. 41.
[6] Bachmann et al., "Competition Short of War," p. 53.
[7] Elizabeth Buchanan, "Hybrid Warfare: Australia's (not no) New Normal," *The Strategist,* 19 May 2019, <https://www.aspistrategist.org.au/hybrid-warfare-australia-not-so-new-normal/>
[8] Andrew Dowse and Sascha Dov Bachmann, "Explainer: What is 'Hybrid warfare' and what is meant by the 'Grey Zone'?" *The Conversation*, 17 June 2019, https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841.
[9] Andres B. Munoz Mosquera and Sascha Dov Bachmann, "Lawfare in Hybrid Wars: The 21st Century Warfare," *Journal of International Humanitarian Legal Studies* 7 (2018): pp. 63, 66.

trend of grey zone tactics.[10] A number of commentators have defined hybrid war, however, it has been well-stated by Wilkie, that hybrid warfare is a conflict, "*in which states or non-state actors exploit all modes of war simultaneously by using advanced conventional weapons, irregular tactics, terrorism, and disruptive technologies or criminality to destabilize an existing order.*"[11] In furthering this argument, NATO in its Capstone of 2010 used hybrid threats (and warfare) as an umbrella term that "encompasses a wide variety of existing adverse circumstances and actions, such as terrorism, migration, piracy, corruption, ethnic conflict etc."[12]

As discussed by Hoffman in its original conceptualisation, hybrid warfare encompasses three elements, the relationship between terrorism and insurgency, the use of technology, and the urban battlefield. All of which are crucial features of all modern conflicts.[13] Typical hybrid military tactics are now argued to include; the wide use of non-lethal weapons; the increasing use of irregular militia groups (paramilitary forces); the increasing reliance upon the use of psychological, radio-electronic, and information warfare through cyber means; the increase of distance warfighting through the use of stealth operations; the transition towards greater use of cyber and air-space environments; and an increase in asymmetric combat actions.[14] It has also been argued that all these military strategies and use of technologies "occurs against the backdrop of the proliferation of weapons of mass destruction."[15]And, thus it can be argued that

[10] Dowse and Bachmann, "Explainer,"

[11] R. Wilkie, "Hybrid Warfare – Something Old, Not Something New," *Air & Space Power Journal* 2009, https://www.airpower.au.af.mil/airchronicles/apj/apj09/win09/wilkie.html (last accessed 1 June 2016); Mosquera and Bachmann, "Lawfare in Hybrid Wars : The 21st Century Warfare,"pp. 63, 66.

[12] Sascha-Dominik Bachmann and Håkan Gunneriusson, 'Hybrid Wars: The 21st Century's New Threats to Global Peace and Security' (2015) 43(1) *South African Journal of Military Studies*. 43, 1 (2015): pp. 77, 79. For the actual definition of Hybrid Threats, See: *BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

[13] Andrea Beccaro, "Modern Irregular Warfare: The ISIS Case Study," *Small Wars & Insurgencies* 29, 2 (2018): pp. 207, 209.

[14] Yuriy Danyk, Tamara Maliarchuk and Chad Briggs, "Hybrid War: High-tech, Information and Cyber Conflicts," *Connections: The Quarterly Journal* 16, 2 (2017): pp. 5, 12.

[15] Josef Schroefl and Stuart J. Kaufman, "Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War," *Studies in Conflict & Terrorism* 37 (2014): pp. 862, 868.

throughout the course of a hybrid war there is generally a decline in the effective application of international humanitarian law and the laws of war.[16]

It is also worthy to note Russia's own version of *hybrid warfare*, which is viewed as a strategy to accomplish political goals without traditional military methods.[17] It has been observed that Russia's hybrid warfare is more focused on special operation forces, economic warfare, sabotage, and espionage, often mixing combatants and non-combatants, for the overall purpose of achieving a political goal.[18] As stated by General Gerasimov, "the role of nonmilitary means of achieving political and strategic goals have grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[19] Whilst this does not starkly contradict the above discussion, there is a slight difference in the overall objective.

To that end, we now introduce Syria; a conflict that continues to divide the international community and rip a state apart, whilst illustrating the damage a hybrid war can achieve across multiple military domains and catastrophic effect such tactics have on civilian populations.

Hybridity of Actors: Multiple Conflicts and Contending Parties

> Hybridity ... is characterized by the interpenetration of a wide range of non-state actors including any combination of insurgent or terrorist networks; organized crime groups; social groups such as clans, tribes or ethnic groups; and ideologically or religiously motivated organizations; all of which may be backed covertly or overtly by states and/or legitimate businesses.[20]

The Syrian conflict is one that has become increasingly complex due to the diverse range of contending parties that include internal and external State and non-

[16] Schroefl and Kaufman, "Hybrid Actors.".
[17] Zhou, "A Double-Edged Sword," : pp. 246, 249.
[18] Zhou, "A Double-Edged Sword.".
[19] Valery Gerasimov, "The Value of Science in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* 96, 1 (2013): pp. 23, 24.
[20] Schroefl and Kaufman, "Hybrid Actors," pp. 862, 867.

State parties. To make matters more complicated, it has been argued that there are both international armed conflicts (IACs) and non-international armed conflicts (NIACs) occurring within a single territory (Syria), sometimes simultaneously.[21] Here, we briefly outline the dynamics of varying conflicts occurring within Syria today by assessing the internal and external hybrid actors, and as stated above, one of the characteristics of hybrid warfare is indeed the vastness of actors involved in the conflict at any given time.

Internal Hybrid Actors

Currently, within Syria, a number of domestic actors have participated in an ongoing NIAC.[22] After civil unrest began in Deraa in 2011, a sectarian conflict between the Shi'a, Sunni, and Alawaites emerged. Simply put, the Alawaites have controlled Syria since the Assad regime first came into power in the 1970s. Nowadays the Alawaites are seen as a minority, and their rule is being challenged by the Sunni majority. This sectarian conflict was exacerbated even further with the Kurdish seeking autonomy within the Syrian territory.

A further observation presented by Balanche, the Syrian territory can be divided into three main regions: a multi-sectarian regime zone, predominantly containing Assad's supporters, Alawaites, Shia and Sunnis; the Kurdish-controlled zone; and the Sunni Arab rebel zone.[23] Furthering this observation, it has been argued that Syria's internal landscape is made up of a combination of actors and can be categorised into three groups; the Assad regime and its supporters, opposition forces, and those who

[21] Tom Gal, "Legal Classification of the Conflict(s) in Syria," 2019: pp. 29, 29.
[22] The Appeals Chamber of the International Criminal Tribunal of Former Yugoslavia (ICTY), in *Tadic* ruled that the minimum threshold for a NIAC as it applies to Article 3 common to the Geneva Conventions, is 'protracted armed violence between governmental authorities and organized armed groups or between such groups within a State': see, ICTY, *The Prosecutor v. Tadic,* Case No. IT-94-1-A, Judgment (Appeals Chamber), 15 July 1999, paras. 84-141.
[23] Fabrice Balanche, *Sectarianism in Syria's Civil War* (The Washington Institute for Near East Policy, 2018), p. xv.

have been labelled as *fence-sitters*.[24] In addition, these three groups remain volatile and there a frequent changes between each coalition and where their support lies.

When looking at the internal actors currently involved in the Syrian conflict, one can argue that they are indeed hybrid actors due to the strategies they employ regularly during times of conflict. Importantly, these actors contributing to the ongoing conflict should be distinguished from the compound warfare theory. Compound warfare (CW) was originally coined by Huber in *Compound Warfare: The Fatal Knot.* Huber explained compound warfare to be "the simultaneous use of a regular or main force and an irregular or guerrilla force against an enemy. In other words, the CW operator increases his military leverage by applying both conventional and unconventional force at the same time."[25] Huber went further to explain that compound warfare "most often occurs when all or part of a minor power's territory is occupied by an intervening major power."[26] However, the distinguishing feature between compound warfare and hybrid warfare, as argued by Hoffman, is that hybrid warfare is *multi-modal* where there the lethality of the conflict is blended with "fanatical and protected fervour of irregular warfare."[27] This multi-modal factor encompasses a range of different modes of warfare comprising conventional capabilities, irregular tactics, terrorism including indiscriminate violence and coercion.[28] To further distinguish between compound warfare and hybrid warfare, one can argue that an important part of hybrid warfare in the modern context is the cyber domain and the emphasis on using hybrid means to achieve a political objective.[29] Although aspects of compound warfare are prevalent within the Syrian context, the internal actors have regularly engaged in hybrid practices, and as such their actions should be observed as falling within the hybrid war classification.

Building on the discussion presented above, it has also been argued that within the hybrid war spectrum, the aggressor combines methods and tactics including

[24] Jeffrey Martini, Erin York and William Young, "Syria as an arena for Strategic Competition," *Rand Corporation* (2013): p. 3.
[25] Thomas M. Huber, ed., *Compound Warfare: The Fatal Knot* (University Press of the Pacific, 2004), p. 1.
[26] Huber, *Compound Warfare.*
[27] Frank G. Hoffman, *Conflict in the 21st Century: the Rise of Hybrid Wars* (Potmac Institute for Policy Studies, 2007), p. 28.
[28] Hoffman, *Conflict in the 21st Century*, p. 29.
[29] Hoffman, *Conflict in the 21st Century*.

conventional capabilities, irregular tactics, irregular formations, terrorist acts, indiscriminate violence, and criminal activity.[30] Therefore it is only appropriate to designate the Assad regime itself as a hybrid actor. After combining forces with Hezbollah and Russia, the regime has displayed a mixture of regular and irregular warfare tactics. Such military strategies also include the use of advanced technologies which has arguably been provided by Russia and Iran.[31] It is now well-established that the regime has conducted irregular operations by using non-state actors as their proxies and sought to wreak havoc on populations with the use of chemical weapons. As such the regime itself however has been the perpetrator of indiscriminate violence and use of internationally banned weaponry.

External Hybrid Actors

Beyond the internal hybrid actors, there are a vast number of other actors contributing to the mayhem in Syria. It has been readily observed that hybrid challenges and strategies are not limited to non-state actors. As part of a hybrid war doctrine/approach, states shift their conventional units to irregular formations and adopt new tactics.[32] Therefore, another factor that supports the argument that Syria should be classified as a hybrid war, is the sheer number of external actors that are now involved within the conflict, of which most are States. Some States are involved to gain political objectives, whilst others have become involved to combat the international threat posed by *Daesh/IS.* Regardless of their end game, it has been readily observed that some of the external actors involved in the conflict have employed such tactics that combine cyber, kinetic, media, terrorist and military command structures which all fall within the hybrid classification.[33]

[30] Zhou, "A Double-Edged Sword," pp. 246, 247.
[31] Zhou, "A Double-Edged Sword," p. 246. It has been observed that Russia provided the Assad regime s-300 air defense systems as a response to the ongoing intervention from the United States, and whilst this is not their most advanced surface-to-air missile system, it has been compared to the US Patriot Air and Missile Defense System.
[32] Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (2009): pp. 34, 37.
[33] Laura-Maria Herta, "Hybrid Warfare – A Form of Asymmetric Conflict," *International conference Knowledge-Based Organization* 23, 1 (2017): pp. 135, 139.

One IAC that has drawn much attention has pitted the Assad regime (Syrian Armed Forces), including its proxies, and the international coalition led by the US against each other.[34] Russia, Lebanon's Iran-backed Hezbollah, and Iran itself have been actively supporting the Assad regime against the US-led coalition. Much of this IAC and the action taken by the US-led coalition operations have consisted of targeting operations and airstrikes against infrastructure reportedly containing chemical weapons. Other targeting operations have been directed against the Syrian Armed Forces. Joint airstrikes conducted by France and the UK also hit military bases and chemical weapon storage facilities in April 2018.[35] The overall objective is a political one, which is to remove Assad from government and has been a political objective for the US since at least the 1970s.[36] Importantly, this IAC should be considered separate from the IAC occurring against *Daesh.*[37]

Then there are the external state actors who have been engaged in a war against the terrorist group *Daesh* (also known as IS, ISIL, or ISIS), using a rather ambiguous United Nations' mandate under UNSC Resolution 2249 of 2015 as authorisation and justification for their military involvement. Their presence could be seen as justification for making this conflict an IAC. Due to operational successes in eradicating terrorist strongholds, the war against *Daesh* has been labelled as successful. Thanks to this *success*, US troops were subsequently withdrawn from parts of Syria in 2019 without consideration for their Kurdish allies and NGOs. This ultimately opened the door for Turkey to invade the Kurdish-held territories in northern Syria.

Other state actors involved in the Syrian conflict in one capacity or another include Saudi Arabia, the United Kingdom, and Qatar.[38]

The number of parties involved in the Syrian conflict not only highlights the complexity of the conflict but also highlights why a resolution has not yet been found.

---

[34] Anthony Paphiti and Sascha-Dominik (Dov) Bachmann, "Syria: A legacy of Western Foreign-Policy Failure," *Middle East Policy* 25, 2 (2018): p. 136.
[35] Julian Borger and Peter Beaumont, "Syria: US, UK and France launch strikes in response to chemical attack," *The Guardian,* 14 April 2018. < https://www.theguardian.com/world/2018/apr/14/syria-air-strikes-us-uk-and-france-launch-attack-on-assad-regime>
[36] Paphiti and Bachmann, "Syria," pp. 136, 136.
[37] Gal, "Legal Classification," pp. 29, 34.
[38] Paphiti and Bachmann, "Syria." pp. 136, 136.

The overall destruction in Syria has been amplified by the fact that the parties have operated across numerous military domains, such as land, sea, air, space, and now cyber and the information domain. Many military operations are being conducted across more than one military domain at a time. Apart from the military strategies used, Syria should be characterised as a hybrid war, based on the observation that there are several conflicts taking place in one territory simultaneously, each occurring simultaneously across multiple conflict domains.

Before looking more closely at the hybrid environments and strategies, one thing can be stated about the external actors that help identify this conflict as hybrid. Each state involved has a political objective, some have participated in disseminating propaganda, and some states have sought to exploit revolutionary technology to negate military superiority. These States have as hybrid war doctrine dictates, retained basic and brutal forms of violence, exploited the virtual dimensions of warfare, whilst maintaining kinetic and conventional tactics.[39]

~ ~ ~

As stated by Hoffman:

> Hybrid wars are not new, but they are different. In this kind of warfare, forces become blurred into the same force or are applied in the same battlespace.

This type of warfare and its actors should therefore be distinguished from compound warfare. Although we have discussed this distinction above in some detail concerning intra-state actors, some further explanation is warranted. To that end, a compound war from the perspective of Hoffman is "when a significant degree of strategic coordination between separate regular forces and irregular forces in conflicts occurs."[40] Here the *regular force* is seen to be a state, and the irregular force, a *non-state actor*. The irregular force generally attacks weak areas, which ultimately compels the conventional force to disperse its security forces.[41] In contrast, hybrid wars are more complex, there is a greater fusion of the methods and modes of conflict in the battlespace, and it is this, as Hoffman argues, the compound war theory did not achieve

[39] Laura-Maria Herta, "Hybrid Warfare," pp. 135, 139.
[40] Hoffman, "Hybrid Warfare," pp. 34, 36.
[41] Hoffman, "Hybrid Warfare," pp. 36-7.

or anticipate. As such hybrid warfare combines the lethality of state conflict with "fanatical and protected fervour of irregular warfare."[42]

Hybrid Environments and Strategies

Throughout the evolution of hybrid warfare, several military components have emerged with two of particular importance for the purposes of this paper; the increase of information warfare amplified through cyber warfare, cyber warfare, and the transition towards greater use of cyber and air-space domains. It has been observed that hybrid wars will:

> …exploit access to modern military capabilities, including encrypted command systems, man-portable air-to-surface missiles, and other modern lethal systems, as well as promote protracted insurgencies that employ ambushes, improvised explosives devices (IEDs), and coercive assassinations. This could include states blending high-tech capabilities such as antisatellite weapons with terrorism and cyber warfare directed against financial targets.[43]

In building upon the discussion from previous pages, it is clear that several of both Hoffman's and Gerasimov's hybrid warfare theories and approaches respectively, are present within the Syrian context. New technologies have been utilised on an unprecedented scale, and this conflict has been an accelerator to the development of more advanced weaponry. It has also become clear that the use of cyber serves both as an enhancer of such warfare and possibly as a category on its own, namely below the threshold operations within the emerging cyberwar/ conflict paradigm. To that end, the conflict in Syria has become one where previously untested battlefields and operational domains, have been explored and exploited.

The discussion that ensues analyses the prevalence of hybrid warfare strategies in the context of urban warfare and the use of the cyber domain as a separate battlespace. Specific reference will be given to Hoffman's three elements of hybrid

[42] Hoffman, *Conflict in the 21st Century*, p. 28.
[43] Hoffman, "Hybrid Warfare," pp. 34, 37.

warfare, which include: terrorism and insurgency; the use of technology; and the urban battlefield.

Hi-tech Weaponry and Convergence of Military Domains

There was once a time where military strategy utilised a single battlespace, land or sea, and just maybe, in some situations, two. Modern warfare has not only seen a quantitative increase in the battlespaces where war operates, there has now been the convergence of multiple domains to implement a single military strategy or operation. For example, NATO has a large dependency on space-based technologies. In order to conduct precision strikes through the use of unmanned aerial vehicles (UAVs) (such as military drones), data obtained through satellites is what is predominantly relied upon, especially where ground-based operations are vulnerable to physical attacks.[44] Not only does this show a convergence of cyber and space domains/battlespaces, but also air as a battlespace. Notably, this type of convergence also falls within Hoffman's definition of *multi-modal* warfare.

When analysing the convergence of military domains and the advanced nature of the weaponry engaged in the Syrian conflict, one cannot ignore Russia's involvement. It has been observed that the Russian military has viewed its operation in Syria as a *laboratory* for testing new technologies and weapons, as well as military strategies.[45] Whilst the use of UAVs is discussed in greater detail below, it is worthy to note that Russia has focused on high precision weapons and technologies, with UAVs remaining central to all operations. Beyond the use of UAVs, Russia has used the Syrian conflict to improve its high precision arsenal, with a focus on their unguided weapons systems, advanced satellite navigation, and radio-electronic warfare capabilities.[46] Using these high precision technologies, Russia was able to establish no-fly zones, impose blockades and launch thousands of strikes against *Daesh* and rebel forces. This was also achieved

44 NATO report – Chatham house, p. 9

45 Dmitry Dina Adamsky, "The Impact of the Russian Operation in Syria on Hezbollah's Operational Art: A Hypothesis," *Studies in Conflict and Terrorism* 43, 5 (2020): pp. 414, 414-5.

46 Adamsky, "The Impact of the Russian Operation in Syria," p. 417.

with the help of private military companies. Ultimately this assisted the Assad regime and Syrian Armed Forces to reclaim cities and towns.[47]

Terrorism and Insurgency

Central to the hybrid war doctrine is the recognition of the role of both terrorism and insurgency. And, one of the largest components of the Syrian conflict has indeed, been the war against *Daesh.* The military operations directed against *Daesh* have seen international involvement which extends from Syria into Iraq. This is one part of the conflict that has been labelled as an international armed conflict (IAC), and the international community as a whole has taken comprehensive and direct military action. Beyond the international involvement in combatting *Daesh,* the impact of this insurgency has been significant. Not only has the armed conflict led to the destruction of urban environments, but it has also contributed to the destabilisation of the Syrian government and Assad regime. At its peak, *Daesh* controlled a vast part of the Syrian and Iraq territories and successfully defended these areas for a number of years. To define *Daesh* as a simple terrorist organisation, would be inaccurate. It has of course committed terrorist offences and terrorised large portions of Syria and Iraq; however, it is more than a terrorist organisation. The more accurate definition or classification is one of insurgency. *Daesh,* for a long period, had a self-sustaining financial model; it engaged in sophisticated military operations; controlled territory; and had a very vocal political voice.[48] Despite being classified as an insurgency, *Daesh* used terrorism as its central tactic, which needs little discussion as one can readily recall images of suicide and car bombings.

The involvement of *Daesh* within the Syrian conflict should be distinguished from irregular warfare. If Callwell's definition is to be taken as correct, irregular warfare is where "all campaigns other than those where both the opposing sides consist of regular troops."[49] Indeed, *Daesh* was not made up of *regular troops*, but for the locals

[47] Zhou, "A Double-Edged Sword," pp. 246, 253.
[48] Beccaro, "Modern Irregular Warfare," pp. 207, 211.
[49] Charles E. Callwell, *Small Wars: Their Principles and Practice* (University of Lebraska Press, 1996,) p. 21; Beccaro, "Modern Irregular Warfare," pp. 207, 209.

who sought to fight against *Daesh*, several of the actors involved in combatting the threat they posed, were, in fact, State actors, such as the US-led coalition.

Asymmetric Warfare and Urban Battlefields

Asymmetric warfare, plainly said, is where the conflicting parties have a disparity between their capabilities, and as noted by Geiß, perfect symmetry between conflicting sides has rarely been witnessed in times of war.[50] In contemporary conflicts, asymmetric warfare has been regularly employed within urban environments where militarily weaker parties do not often engage in conventional warfare tactics.[51] Despite the barrage of direct offensive strategies conducted by militarily strong parties, those who are weaker in capabilities are left to employ indirect offensives. These weaker parties are left to conduct "indirect offensive and defensive strategies such as guerrilla warfare, concealing themselves among supportive civilian populations in cities, towns, and villages, which provide both cover for them to launch attacks and also protection from counter-attack."[52]

It seems that in the modern era, all conflicts present themselves at the doorsteps of homes in cities and urban spaces. This has, as one would suspect, had a hugely detrimental impact on civilians, but also has changed the strategies employed by armed forces. In recent conflicts, outlawed practices such as direct attacks against civilians, the use of human shields, and hostage-taking have seen a revival where military weaker parties have sought to gain advantage over the superior force.[53]

Initially, urban battlefields allowed insurgents to hide in large and high-density environments, a strategy that has been employed in numerous conflicts. However, this strategy has been met with a drive to improve military technologies specifically designed to ensure success in urban battlefields. Technological advancements for

[50] Robin Geiß, "Asymmetric conflict structures," *International Review of the Red Cross* 88 (2006): pp. 757, 758.
[51] Michael John-Hopkins, "Regulating the conduct of urban warfare: lessons from contemporary asymmetric armed conflicts," *International Review of the Red Cross* 92 (2010: pp. 469, 470.
[52] Michael John-Hopkins, "Regulating the conduct," pp. 469, 471; Ivan Arreguın-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict* (Cambridge University Press, 2008), p. 4.
[53] Geiß, "Asymmetric," pp. 757, 758.

militaries have advanced to a level where reconnaissance, surveillance, and precision strikes now allow for militaries to move deeper into urban environments. Further, and in response to this seemingly regained symmetry, militarily superior forces have revived questionable, if not, illegal practices, and increased the number of covert operations and targeted killings.[54]

Syria is no exception, and vast amounts of urban spaces have been decimated by the conflict. Millions have lost their homes and are now displaced within Syria and abroad. We are all but too familiar with the images of cities and towns being utterly destroyed throughout the Syrian conflict. As stated by Vincent Bernard, Editor-in-Chief of the *International Review of the Red Cross,* in referring to urban 'total war' and the destruction of Syrian (and Iraqi) towns and cities:

> A scene of devastation, blanketed with grey dust, stretches into the distance in eerie silence. Walls riddled with bullets, buildings collapsing in on themselves, external walls blown away to reveal an intimate view of a bedroom or living room, streets blocked by piles of rubble.
>
> These sickening images of destruction – filmed from above by drones and shared on social media – probably best symbolize the current resurgence in urban warfare. Other images come to mind: bombed-out hospitals, children being pulled from wreckage, snipers roaming the maze of tunnels and walkways that have been blasted through the walls of now-uninhabited houses.[55]

This paints a gloomy picture of cities and towns that are now nothing more than rubble. In 2017, the *International Review of the Red Cross* published *War in Cities* with one article dedicated to the voices of Aleppo. The Syrian voices captured in this publication paint a starkly ominous picture of the impact of urban warfare. Frequent mention is made of the shelling, government areas being besieged regularly, and armed groups regularly looted.[56]

Large cities and towns of Syria have been all but destroyed throughout the conflict as a result of the hybrid and asymmetric tactics employed by all warring parties.

---

[54] Geiß, "Asymmetric."
[55] Bernard, "Editorial: Conflict In Syria," pp. 865, 865.
[56] "Voices and Perspectives, Life in a war-torn city: Residents of Aleppo tell their stories," *International Review of the Red Cross* 98, 1 (2017): pp. 15, 15-20.

Insurgents or weaker parties have sought to hide amongst civilian populations in towns and cities, leaving conventional actors to be drawn into a fight where large amounts of civilians are put at extreme risk. In some respects, this has meant that symmetry has been regained, however, where there is little ability to gauge the situation on the ground and where the civilian population has sought to evacuate, there is little to prevent the conventional force from unleashing the destructive potential of its conventional arsenal.

The Use of Technology: Cyber as a Battlefield

The concept that cyber is both an enhancer of warfare methods, and possibly a category on its own is not an unfounded statement. Many of the uses of cyber technologies do indeed fall short of what would be classified as an armed *attack* pursuant to international law. However, when one assesses where cyber technologies are utilised militarily, it becomes clear that the impact can be far-reaching. Here, we discuss how cyber technologies and *hacktivists* have exploited online systems as a method of disseminating propaganda often constituting information warfare, with a secondary discussion surrounding the use of drones as a cyber technology. In furthering the argument that such strategies are included in the hybrid warfare classification, one could also argue that such operations and use of technology can also fall within the scope of so-called *grey-zone* operations, which do not cross the threshold of war due to the ambiguity of law, of action and attribution or the overall (low) impact of such operations.[57]

Grohe concludes that the cyber operations conducted during the Syrian conflict have been "more important than one might have expected."[58] This conclusion is based upon research and data pointing to numerous actors involved in the Syrian conflict who have used cyber operations as a method of warfare. Such conduct has been evidenced by the cyber involvement of Iran, Hezbollah and the Syrian Electronic Army (SEA) in

[57] Dowse and Bachmann, "Explainer."; Bachmann, Dowse and Gunneriusson, "Competition Short of War," pp. 41, 45.
[58] Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," *Comparative Strategy* 32, 2 (2015): pp. 133, 133.

distributing propaganda, with the objective of disinformation and deterrence.[59] With Russia and the United States also engaging in cyber operations and remote warfare. Unfortunately, in the case of Syria, and as will be illustrated in the discussion below, rebel groups and anti-Assad combatants have not enjoyed the same ability to engage in cyber operations as a means of hybrid warfare. Cyber operations have become commonplace within modern conflicts, and have frequently been utilised as a means of asymmetrical warfare, with non-State actors utilising the cyber domain as a way of regaining symmetry against superior forces.[60] Despite the potential to level out the battlefield, the use of cyber methods within the Syrian conflict has in some respects increased asymmetry between warring parties due to most of the cyber operations having been conducted by those who are militarily superior, such as Russia, Iran, the SEA, Israel, and the United States.

Below the Threshold of Warfare

It is worthy to mention that not all actions that have occurred during the Syrian conflict fall within the threshold of warfare. To that end, the hybridity of the Syrian conflict extends to acts that would usually fall below this threshold, and would therefore be deemed as *hybrid threats*, a term often used simultaneously with *hybrid warfare*.[61]

According to NATO:

> Hybrid threats can be also understood as the employment of a comprehensive approach by an adversary. In this interpretation, hybrid threats are not solely military threats, but they combine effectively political economic, social, informational and military means and methods.

[59] Marcin Andrzej Piotrowski, "'Mosaic Defence:' Iran's Hyrbid Warfare in Syria 2011-2016" *The Polish Quarterly of International Affairs* 3 (2017): pp. 18, 21.
[60] Michael N. Schmitt, "Rewired warfare: rethinking the law of cyber attack," *International Review of the Red Cross* 96 (2014): pp. 189, 190.
[61] Bachmann, Dowse and Gunneriusson, "Competition Short of War," pp. 41, 42 with reference to Hoffman's original definition.

> Adversaries who pose a hybrid threat employ a comprehensive approach with the speed and agility normally with unity of command.[62]

As we have observed throughout the Syrian conflict, non-state actors such as *Daesh* have exploited social media as a form of disinformation and recruitment. State actors have also used these platforms to promote and disseminate propaganda. And, although these actions fall below the threshold of warfare, they are part of warfare in that they constitute one aspect of the larger picture and therefore, cannot be separated from one another. The actions that fall below the threshold of warfare have resulted in or at least contributed to the kinetic aspects of conflict.

The Role of Social Media

Non-kinetic aspects of hybrid warfare include *influence operations* that have the core objective to misinform world opinion,[63] which is where we introduce the role of social media in Syria's ongoing conflict. Relating to Hoffman's definition of hybrid warfare, social media falls within the use of "propaganda and media coverage."[64] Social media has undoubtedly played a large role in the Syrian conflict, with the main use being to disseminate propaganda for the Assad regime, and for the recruitment of foreign fighters to serve with ISIS. Russia has contributed substantially to propaganda dissemination, with numerous social media sites being utilised to push their rhetoric.[65] The SEA has also been a key player in disseminating propaganda for the Assad regime, and has been used as a "public relations tool" to draw attention to the official Syrian version of events, with coverage extending to the impact of Syrian opposition groups.[66] Although not currently operating due to internet restrictions, SEA gained support from the Assad regime after it felt the need to counter various cyber-attacks against

[62] Headquarters, Supreme Allied Commander, Transformation, Assessing Emerging Security Challenges In The Globalised Environment: The Countering Hybrid Threats (Cht) Experiment, Final Experiment Report (Fer) *27* (29 September *2011)*, Cited In Aurel Sari, "Hybrid Warfare, Law And The Fulda Gap" In *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, eds., Christopher Ford and Winston Williams (*Oxford: Oxford University Press*, 2019), p. 173.

[63] Mosquera and Bachmann, "Lawfare in Hybrid Wars," pp. 63, 64-5.

[64] Beccaro, "Modern Irregular Warfare,"; Hoffman, *Conflict in the 21st Century,* p. 8.

[65] Zhou, "A Double-Edged Sword," pp. 246, 252.

[66] Ahmed K. Al-Rawi, "Cyber Warriors in the Middle East: The case of the Syrian Electronic Army," *Public Relations Review* 40 (2014): pp. 420, 420.

government websites.[67] It has been argued that most of the cyber operations conducted by the SEA were directed against the social media channels of traditional media outlets and social media websites belonging to oppositional groups.[68] As argued by Al-Rawi, the SEA's operations were conducted mainly because the Assad regime found it increasingly difficult to express its views to the world when the rebellion initially began.[69] However, it has been stated that the consequences of operations conducted by organisations such as the SEA, lead to difficulty in authenticating content.[70] For example, the SEA in 2012 allegedly hacked Al Jazeera, sending false mobile texts claiming that the Prince of Qatar had been subject to an assassination attempt.[71]

The recruitment of foreign fighters through the use of cyber means including social media, and websites has also been of great concern within the Syrian context. Although it may not be a major feature of the conflict, it has certainly played a role. In 2017, it was estimated that over 700 British citizens had travelled to Syria to fight against the Assad regime, with many pledging allegiance to ISIS.[72] It was also roughly estimated that there were 3000 foreign fighters affiliated with ISIS within Syria at the beginning of 2019.[73] The recruitment of these foreign fighters is largely due to the social media campaigns run through Facebook, Twitter, and YouTube.[74] Although the use of social media to disseminate hate and extremism is not a new phenomenon, it has been a factor in the Syrian conflict.

[67] Al-Rawi, "Cyber Warriors in the Middle East."
[68] Al-Rawi, "Cyber Warriors in the Middle East," p. 423.
[69] Al-Rawi, "Cyber Warriors in the Middle East."
[70] Grohe, "The Cyber Dimensions," pp. 133, 141.
[71] Al-Rawi, "Cyber Warriors in the Middle East," pp. 420, 423.
[72] Imran Awan, "Cyber-Extremism: ISIS and the Power of Social Media," *Social Science and Public Policy* 54 (2017): p. 138.
[73] *Eighth Report of the Secretary-general on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat,* UN Doc s/2019/103 (1 February 2019).
[74] *Eighth Report of the Secretary-general on the threat posed by ISIL.*

Within the Meaning of Cyber Operations

Cyber operations and capabilities can be far-reaching and are often not confined to computer-based attacks. However, two schools of thought have emerged, each discussing the scope of *cyber operations* within a conflict situation. It is not the purpose of this discussion paper to make a determination as to which school of thought should be adopted. However, a discussion will take place around each.

The first school of thought takes a narrow interpretation that argues that cyber operations are generally constrained to computer-based attacks. To provide an example; throughout the Syrian conflict, Iran has tested their cyber-capabilities with attacks targeting armed opposition and at elements that extend to other operational domains.[75] Many of the cyber operations conducted by the Syrian regime were improved and expanded by Iran and Hezbollah, with numerous attacks being documented throughout the conflict.[76] It has also been argued that some operations have reportedly had the primary objective of obtaining operational intelligence on the battlefields in Syria.[77] As discussed earlier, many cyber operations conducted by the Assad regime and the SEA have been aimed at social media and foreign media outlets. Adding to this, in some cases operations have been directed towards universities, with the main objective of disseminating propaganda and, as retaliation against the West.[78]

The broader school of thought argues that cyber operations extend to remote warfare.[79] UAVs such as drones are at the heart of this argument, and one could also classify the use of such technologies as *cyber-enhanced* military strategies. This classification is based on the argument that UAVs are made up of computer systems that are inherently cyber-related. As argued by Danyk et al, it is the use of stealth concepts, robotization, and warfighting from a distance, such as UAVS, which also aids us in determining the hybridity within the Syrian conflict. As Schmitt stated, "cyber operations have already become an integral facet of command, control,

[75] Piotrowski, '"Mosaic Defence," pp. 18, 28.
[76] Ibid., pp. 18, 64; Grohe, "The Cyber Dimensions," pp. 133, 136.
[77] Piotrowski, '"Mosaic Defence," pp. 18, 39.
[78] Piotrowski, "Mosaic Defence."
[79] Emily Crawford, *Identifying the Enemy* (Oxford University Press, 2015), p. 126.

communications, computer, intelligence, surveillance and reconnaissance activities in the battlespace."[80]

The use of UAVs has been well-documented in Syria. State parties such as Israel, Iran, Russia, the United States, and, in some circumstances, Turkey, have all been allegedly employed UAVs for the abovementioned purposes. Notably, ISIS has even gained access to high-tech weaponry such UAVs. Iranian drones have reportedly been used for reconnaissance, artillery direction, and directing attacks.[81] Despite little affirmation as to their military operations in Syria, Israel has recently claimed to have carried out a drone strike to prevent further drone attacks by Iran.[82] Russia, has also allegedly engaged in cyber operations which have included the use of UAVs and "ground systems to conduct electromagnetic reconnaissance and jamming against satellite, cellular and radio communication systems along with GPS spoofing."[83] The extent of Russia's operations has been estimated to include more than 23,000 flights conducted by UAVs.[84] In early 2018, reports emerged that Russia has also begun jamming the signal of US drones operating in Syrian airspace.[85] The widespread use of UAVs within Syria, not only highlights the extent of remote warfare and increased dependency on cyber-enhanced military strategies, but it also illustrates the convergence of military domains in modern war. In some respects, the use of UAVs by non-state actors, especially rebel forces and ISIS, goes to show that the asymmetry between warring parties can be overcome to some degree.

[80] Schmitt, "Rewired Warfare," pp. 189, 190.
[81] Piotrowski, note 9, p. 34.
[82] "Israel says it Struck Iranian 'Killer Drone' sites in Syria," *BBC News,* 25 August 2019, <https://www.bbc.com/news/world-middle-east-49464546>
[83] Col. Liam Collins, "Russia Gives Lesson in Electronic Warfare," *Army* 68, 8 (2018): pp. 18, 19.
[84] David Oliver, "Russia's Rapid UAV Expansion," *Armada International* 43, 6 (2019): p. 8.
[85] Courtney Kube, "Russia has Figured out how to Jam U.S. Drones in Syria, officials say," *CBS News,* 10 April 2018, <https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931>; Josie Ensor, "Russia to jam signals in Syria and supply regime with more advanced anti-missile technology after place was shot down," *The Telegraph,* 24 September 2018, < https://www.telegraph.co.uk/news/2018/09/24/russia-jam-signals-syria-supply-regime-advanced-anti-missile/>

Hybrid Alliances

It can be observed that external hybrid actors as mentioned earlier, have combined forces with the Assad regime, which has in effect created a *hybrid alliance*. This observation adds an additional layer to the complexity and hybridity of Syria's conflict. In fact, there is a lot to be said regarding how the Assad regime has partnered with *terrorist* organisations such as the Iran-affiliated Lebanese Hezbollah which have been embedded within the Russian war machine to conduct several significant operations, which were also jointly contributed to by the Iranian Revolutionary Guards.[86] And, as already mentioned, there have been extensive partnerships with private military companies such as the infamous Russian Wagner Mercenary group.[87]The hybridity of the pro-Assad alliance, including state and non-state actors alike as well as terrorist groups and mercenaries, has all the hallmarks of a pre-*Guestphalian* conflict which adds additional complexity to the conflict. Consequently, questions of reattribution and responsibility arise which test the current legal paradigms of modern war and conflict of our post-World War II rule-based order.

Concluding Remarks

This article discussed the ongoing conflict in Syria as a case study for a Hybrid War in terms of its nature, the methods used, and the actors involved. The tragedy of the conflict for its victims and its regional impact in terms of its potential to politically destabilise both the Middle East and Europe is clear to see. But there are also lessons to be learned from the Syrian tragedy: from its use for power-projection by Russia, the US, Turkey, and Iran before the backdrop of great power competition to the chance to revisit our capabilities, awareness, and resilience in the face of new emerging conflict scenarios and warfare approaches. Disinformation and media manipulation have been used by all sides and should be studied by our practitioners of information warfare. The hybridity of the actors involved, and their use of both conventional and irregular warfare serves as a good example for future conflict in a contested and complex battlespace. The use of grey-zone operations such as cyber-enhanced influence-

[86] Adamsky, "The Impact of the Russian Operation in Syria," pp. 414, 414-9.
[87] Zhou, "A Double-Edged Sword," pp. 246, 253.

operations will be the new normal for us when countering the current threats posed by both terrorist actors and hostile state actors applying a hybrid mix of warfighting capabilities both at home and abroad. Such lessons will enhance our awareness and consequently shape our adaptability to counter such threats and our capacity to deter such threats.