Communication and Public Diplomacy, April 2023, Vol. 2, No. 1, pp. 160–172
ISSN 2578-4277 (Online)/ISSN 2578-4269 (Print)
Doi: 10.17265/2578-4269/2023.01.013

DAVID PUBLISHING

Addressing Challenges to the Conduct of Intelligence Operations in an Age of Ambiguity

Andrew G. Cook
Intelligence & Security Studies, University of Leicester, UK

Since Krulak's "Three Block War" theories on the complexity of modern battlespaces, therehas been a growing recognition of the nature of "Ambiguous Warfare" or "Gray Zones" in the understanding of the contemporary spectrum of conflict. However, little consideration has been given to the implications for the Intelligence Community regarding these highly complex and uncertain environments in terms of oversight and ensuring conduct remains legal, ethical and within the bounds of necessity and proportionality. The employment of Artificial Intelligence and Machine Learning along with increasing reliance on local actors and collaborative approaches with allies and partners will likely further complicate the situation. In this context, this paper will provide an analysis of this landscape in order to identify areas where future activities are likely to prove controversial and problematic. It will go on to propose a framework that would ensure they remain within the normativeboundaries demanded by policy makers and their electorates.

Keywords: Three Block War, Gray Zone, intelligence

Introduction

Within the ongoing discussions as to the nature of the contemporary spectrum of conflict it some would contend that "Hybrid Warfare" best describes activities occurring in many of the troubled areas of the world. Others would claim that this view offers little that is new. Afterbriefly exploring ideas of hybrid war and hybrid threats this paper will focus on the emerging concept of "gray zone" conflict, which would appear to be increasingly recognized as the methodology of choice within contemporary strategic competition.

To date there has been a general lack of discourse as to the challenges faced regarding the multiple challenges to the conduct of intelligence operations and activities within the highlycomplex ambiguous and uncertain environments created by these phenomena. Therefore, there is a requirement to examine what if any factors are different from other types of conflict, and how these will impact on the intelligence processes.

The aim will be to draw on contemporary literature regarding intelligence problems in morebroad and general terms and contextualize those that relate to addressing ambiguity and uncertainty that will be critical in understanding this evolving problem set.

Finally, it will propose a framework that would ensure that intelligence operations can become more effective whilst remaining within the normative boundaries demanded bypolicy makers and their electorates.

Andrew G. Cook, Master's Candidate, Intelligence & Security Studies, University of Leicester. Research fields: international relations. E-mail: Andrew_G_Cook @le.ac.uk.

Hybrid War, Hybrid Threats and the Emergence of the "Gray Zone"

Since the publication of Krulak's "Three Block War" theories on the complexity of modern battlespaces (Krulack, 1999) much consideration has been given as to the nature and the character of contemporary and future warfare. In the post-Cold War era, the strategic shockof 9/11 has led to narrowly focused CT and COIN operations in Iraq and Afghanistan and against both al-Qaeda and latterly the Islamic State. A resurgent Russia, and Chinese activities such as the "belt and Road Initiative" have signaled a return to Great Power competition with the Russians making concerted efforts seeking to neutralize and make redundant the military strengths and economic might of the west.

This has generated much new impetus on the subject of hybrid warfare and hybrid threat with many conflicting interpretations. Hoffman (2014, 2016, 2018) has contributed significantly to this academicdebate on evolving understanding of this area. Hoffman and US military thinkers originally spoke of "hybrid threats", with hybrid war being the preferred descriptor in academic circles (Similiaenu, 2018). Similiaenu himself utilising an epistemological approach describes it as a non-linear multimodal asymmetric form of conflict. (2018, p. 266). Difficulties in framing this problem set continue, and a belief that there was "not so much the problem of defining the term as how to clarify the concept so to make it useful. (Reichborn-Kjennerud & Cullen, 2016). There have also been "multiple and different meanings of the term that complicate a consensus understanding of the problem" (Cullen, 2018, p. 4). Hoffman (2018) has recently offered that hybrid war is:

> "The purposeful and tailored violent application of advanced conventional militarycapabilities with irregular tactics, with terrorism and criminal activities, or combination of regular and irregular forces, operating as part of a common design inthe same battlespace".

Arguably there is nothing novel here and many conflicts have featured all or many of the elements listed above, which present few unfamiliar challenges. There is also no questioningVan Puyvelde's view that "any threat can be hybrid as long as it is not limited to a single form and dimension of warfare" (2015) and assertion that the use of this terminology causes confusion. Glenn (2009) believes that due to its multi-faceted nature no formal doctrine is required. Chambers (2016) admits that although the concept is hardly new a definition is required in order to achieve a "shared understanding in order to employ correct responses andreduce risk".

The key issue here is that although much of the concept is not new, it has certainly gained more attention due to recent developments. Russian activities in Ukraine and elsewhere havebeen a significant driver for this arising from awareness of what is described as "Russian New Generation Warfare (RNGW)." This is often referred to as the "Gerasimov Doctrine" (AWG, 2016), although Hoffman (2016) believes rather than a formal doctrine it better describes the character of modern warfare from the Russian perspective. Giles noted that "The erosion of the distinction between war and peace, and the emergence of a gray zone" has been one of the most striking developments in the Russian approach to warfare (Giles, 2016).

As with the concept of hybrid war, the nebulous "gray zone" has proved equally challengingto define although there is consensus that it is "the element of ambiguity" that makes this different from other areas of the conflict spectrum. (Hicks et al., 2018). Hoffman (2018) once again offers a useful explanation when he defines gray zone activities as:

> "Those covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve

strategic advantage".

What Is Different About Gray Zone Conflict?

Many aspects of Hybrid War described above may not differ from those of previous conflicts, but the growing recognition of threats emerging from gray zones suggests that the dynamic has indeed changed, and it is therefore the latter that warrants the closest examination. There does appear to have been a convergence of the two concepts in current discourse. A recent speech by the head of MI6 in the UK appears to reflect this when he said "You might think that countering terrorism was challenging enough. But now we face the additional complexityof the threats posed by nation states operating in the grey spaces of the hybrid era, which is a wholly separate problem" (Younger, 2018). A similar view is held in the US where a recent military report identified that "Gray zone competition and conflict present fundamental challenges to U.S. and partner security and, consequently, should be important pacers for U.S. defense strategy" (Freier et al., 2018).

The blend of strategies and tactics used will be unique to each conflict and reflect local geographical and political variations, be shaped by the different actors involved and focus the appropriate strategies and techniques on perceived areas of weakness where asymmetric methodologies can achieve greater success. This can lead to some serious difficulty in identifying what does and does not constitute an emerging threat. High levels of deception and denial used to conceal intent and create "ambiguity, complexity, and paralysis for those actors who might try to interfere or oppose" (Freier et al., 2018). Russian actions in Ukraine and Crimea demonstrated an "integrated use of capabilities including rapid deployment, electronic warfare, information operations, special-forces capabilities and cyberspace communications, targeted at both domestic and foreign audiences" (Parameswaran, 2015). Further examples have been identified during Russian operations in Syria with a drive to create "superiority of management" through unifying non-military and military activities across the strategic, operational and tactical levels in order to accelerate the decision-making process and adapt to the increasing pace of modern operations (Harris & Clarke, 2018).

High reliance on asymmetry, both of those involved and the methodologies used may result in threats manifesting and multiplying in varied ways that may or may not relate to each otherthus making it extremely difficult to identify an overall plan or strategy. Sequencing across the entire tactical to strategic spectrum will not necessarily follow any form of doctrinal time- line, with constant modification occurring in reaction to success or failure of individual lines of effort or attempts to counter them. Adversaries will continually seek to obscure and blur the lines separating war and peace by increasing complexity within a rapidly changing operating environment, utilizing evolving technologies (TRADOC, 2017, p. 5).

By its very nature gray zone conflict is highly politicized as it straddles the blurred areas between war and peace. What is becoming apparent after a period of US hegemony in the post-Cold war era is an emergence of adversaries "who now regard themselves as being in a state of perpetual confrontation" (Younger, 2018). Galleoti also refers to this as "non-linearwar" exhibiting the employment of "political, economic, informational, humanitarian, and other non-military measures" which can set the conditions for last resort military operations (2014). In order to counter this there will be a heavy reliance on intelligence, which will be critical to support a coordinated/parallel use of diplomatic, informational and economic instruments of national power to prevent gray zone conflict from manifesting in thefirst place. Continuing to address existing threats will likely stretch the capacity to do so (Miller, 2015).

The broad nature of actions utilized indicates that the threats posed are more than military alone. Based on Hizbollah actions in southern Lebanon in 2006, Glenn (2009) suggests theinclusion of "nongovernmental and intergovernmental agencies, relevant commercial enterprises, and other pertinent parties" in addition to the military. He advocates a 'Comprehensive Approach' requiring broader involvement in addition to military activity. When announcing the new national security strategy for the US President acknowledged this requirement indicating that whilst the military have an important role, a "whole-of-government approach" encompassing trade policy and utilizing economic power isnecessary (Garamone, 2017).

Increased connectivity and the rapid transmission of messaging across the global commons has also altered the dynamic. In addition to main stream journalism, citizen commentators and the rise of the social media phenomenon all contribute to "Framing the Narrative" which can be heavily influenced and manipulated. The phenomenon of "Fake News" has also impacted on the way both domestic and foreign populations consider the information they arereceiving. This has also involved the rapidly evolving Cyber domain which has been utilizedextensively and continued to empower novel threat vectors. Within their operations in Ukraine, the Russians have utilized highly integrated methodologies to blend information warfare and cyber activities to increase complexity and the "fog of war" aimed at gaining advantage at both the tactical level and seeding uncertainty outside of the operational theatre. In order to gain clarity and counter such activities there will be a requirement to continuously evolve and adapt effective means of addressing them (Brantley & Collins, 2008).

What Are the Challenges to Intelligence Operations Posed by Grey Zone Conflict?

Whilst today's great power, near-peer competition will most likely not manifest in outright open conflict, the utilization of gray zone activities certainly appears to be the new normal and is shaping current discourse about contemporary and future conflict. This would suggest there is a need to examine the ability for intelligence operations to address the additional challenges such activities will pose. As outlined, the grey zone construct can include multiple adversarial state and non-state actors, proxy forces and other malign actors such as warlords and criminals. As Mumford (2017) indicates "Not knowing exactly *who* the enemy is presents the most fundamental of challenges to strategic formulation".

Intent and preferred outcomes may overlap but can often be separate and conflicting. One only needs to consider the example of how the situation in Syria has developed since the opposition to the Government of Bashar al-Assad began in 2011. Identifying who is doing what, and to who can be difficult, exemplified by the use of "the little green men" seen in theUkraine. Undoubtedly the most significant issue, particularly in the early stages, will be theability to identify the overall aim and desired end state of the adversaries. That said, getting after the "why" is "ultimately more critical to counter-strategies and conflict resolution" (Hoffman, 2018).

The dynamic and evolutionary nature of gray zone environments can result in situations thatchange rapidly in space and time, and the second and third order effects can be extremely difficult to identify. Given the changing character of threats, it is understandable that maintaining pace with contemporary demands will be no simple task. It is also important toconsider the many existing limitations inherent to the intelligence process that have already been recognized and commented on. These numerous issues and inconsistencies can be magnified when facing new challenges in dynamic and complex environments such as thoseencountered in gray zone conflict.

Intelligence doctrine has faced constant modifications to enable the application of efficient and applicable frameworks. This has been particularly challenging in the light of evolving threats and the pace of change driven by globalization. Betts made some useful observationsin this regard and in the light of the adversarial use of highly technical and sophisticated technology his view that the requirement for ongoing modernization and adaptation will be aconstant (Betts, 2002, p. 54). Perhaps more importantly this must be central, as without continuing progress as “whatever capabilities are achieved intelligence capabilities and efforts alone will never be sufficient”, to deal with either contemporary or emerging threats (Cilluffo et al., 2016, p. 72).

The idea of building understanding by piecing together a jigsaw or “connecting the dots” is simply insufficient to address the mysteries and wicked problems that epitomise highly complex gray zone environments. Whilst it is agreed that increasing the availability of data can improve granularity and knowledge building, it can equally make it more difficult, particularly when misinformation and deception are at play. Mysteries are evaluative and estimative in character (Pythian, 2012, p. 203) and are the every-day challenge for intelligence analysts attempting to contextualize the available intelligence and to evaluate and connect in a coherent manner. This will significantly impact on their ability to realize the actual narrative. Attempts to inject ambiguity and intentionally sow confusion to conceal ultimate adversarial intent make this task harder still. It is this level of complexity that Cullen explains makes gray zone threats wicked problems by “strategic design” (2018, p. 4) making them not only difficult to detect, but they create highly unpredictable situations which are problematic to assess until desired adversarial outcomes are in progress.

Of course, one must utilize the right tool set to address such challenging problems, which is made fundamentally difficult if there is a lack of understanding of the environment in the firstplace. Hulnick (2006) and many other have been highly critical of the weakness of linear processes such as the traditional intelligence cycle claiming that this normative model is outdated and overly simplistic. There have been numerous suggestions as to alternatives, butthe use of a modernized version such as an “intelligence web” as suggested by Gill & Pythian (2013) would certainly be far more useful to address highly complex and ambiguous environments and the wicked problems they contain. Despite a recognition that the greatest challenges may emanate from strategic adversaries, traditional “over the horizon scanning” for indicators and warnings may be insufficient. Areas where potential vulnerabilities couldoccur will need to be closely monitored to identify the nuanced changes that occur at the tactical level. Early detection of such activities that could signal the potential onset of gray zone activities will be needed to enable the swift decision-making required to counter them. Gentry (2008) offered some extremely useful insights into this when describing a seven-stepprocess directly linking decision-makers directly to the strategic planning that will be required to drive the process.

There has been a constant drive to improve and increase collection capabilities in both the technical and HUMINT domains as suggested by Williamson who indicated that “the nationmust be able to collect and fuse information from a wider variety of sources and establish systems to share intelligence across services, the government, and with partners (Williamson, 2009, p. 27). The intervening period has seen an exponential increase in space-based technologies for GEOINT and SIGINT, the expanding use of unmanned aerialsystems deployed across the globe and increasing numbers of collection systems of all types down to the lowest tactical military echelons.

Many of the operational areas where these activities are faced are likely to be geographically distant where the footprint of allied assets on the ground is likely to be minimal. Most of the collection and processing will be conducted via ‘reach’ involving the use of out-of-theatre, centralized nodes for processing and dissemination.

US commanders have certainly recognized the constraints this imposes. Providing context to activity observed by unmanned aerial systems (which will also apply to space-based systems) is significantly more difficult without HUMINT or forces on the ground (Weisberger, 2014). In addition, the combinationof readily available end-to-end encryption and use of anonymization techniques used to obscure activities will pose substantial challenges in the electronic spectrum

According to Kamal Alam of the Royal United Services Institute, a failing of the US-led coalition counter-ISIS campaign in Syria was the lack of human intelligence. (Majumdar, 2015). This reflects the high value placed on HUMINT and is commensurate with the findings of Johnson (2012) who identified the weight that US policy makers place on this collection method. In order to gain greater understanding of wicked problem challenges, identification of strategic intent would be key. However, the capability to penetrate the inner circle of countries such as Russia and China continue to be an area of concern (Harris, 2016) and capabilities at this level will have been impacted due to focus on the more pressing CT fight. Gaining insight across all levels will be equally important, and despite efforts to improve tactical level HUMINT this will also face numerous difficulties. Auster hostile environments will be hard to penetrate, particularly with a small footprint in the region. The introduction of collectors with little experience of the environment will hamper effectivenessas Johnson (2012) also mentions. The option of using allies and partners to recruit "trusted locals" will be necessary, but HUMINT by proxy can be problematic and issues of trust and will inevitably arise. The recruitment and management of covert human sources will also belegally challenging.

Deliberate attempts to increase ambiguity and uncertainty into gray zone conflict will alsoinevitably result in significant broader legal issues. Sauri (2015) highlights the concept oflawfare and that there has been an increase in legal regulation which plays a greater role inmodern conflict. Wittes (2015) contends that given that many aspects of contemporary conflict are not new, existing legislation would encompass most of its elements but acknowledges the cyber domain as a new area that may be more problematic. Difficulties encountered in attributing activities conducted in the gray zone and identifying actors involved may complicate the utilization of the correct legal authorities ensuring responses remain within the boundaries of legality, necessity and proportionality.

More specifically, maintaining effective oversight of the methods of collection and the subsequent usage of intelligence in both non-kinetic and kinetic operations will be extremelydifficult given the rapidity of usage. Similiaenu highlights the "irregular militarized organizations" (2018, p. 266) one may encounter as being particularly problematic in this regard. Further issues surround the policies of sharing intelligence with allies and partners both in terms of the methodologies used to obtain it, and how it is ultimately utilized. These challenges will almost certainly increase as the distance between originator and analyst grows, the speed of the processes increases and the rising levels of automation.

Revelations of questionable collection methods have confirmed many suspicions that "The intelligence process is vulnerable at every point to the abuse of rights" (Gill, 2009, p. 89), therefore requiring a continued increase in intelligence oversight and scrutiny. This suggeststhat further investigation and study of the legal and ethical issues addressing the complexitiesof gray zone conflict will be required to ensure that these do not inhibit or obstruct collectionand other intelligence activities. There is an obvious need to address emerging issues such as the increasing usage of Artificial Intelligence and Machine Learning which is still developing along with the Cyber domain as Wittes has mentioned.

New Problems Will Need New Approaches

There is a view that countering gray zone conflict “may not be doable with the current national security organizations and processes” (Dubick & Vincent, 2017, p. 29). The previously identified challenges they pose to intelligence operations clearly indicate that despite addressing previous shortfalls in the post-9/11 environment there continues to be numerous areas for development and improvement. The latest generation of analysts have become effective in network analysis, the targeting process and the necessary skills to prosecute operations against fleeting targets in remote locations across the globe. But with al-Qaeda on the wane and Islamic State suffering defeats on the battlefields of Iraq and Syriathe intelligence community requires a reset to respond to these emerging threats.

As mentioned earlier there have been numerous studies into the numerous limiting factors that contribute to knowledge gaps and inaccurate or misleading analysis. However, it would be useful to examine some of the lessons identified from recent operational experiences such as those in Afghanistan. The understanding gained in such highly complex environments canprovide insights into the more adaptive ways of thinking required to approach contemporary and future problems. The greatest challenges in that particular theater were “attitudinal, cultural and human” (Flynn et al., 2010, p. 9). Amongst the many recommendations made to address the shortfalls of the intelligence community was the need to adopt a more holistic, less enemy-centric approach and recognize the blurred lines between the strategic and tacticallevels. It is also identified that “the context that provides the best understanding comes from the bottom up, not from the top down (Flynn et al., 2010, p. 23). This has been reflected and iterated in subsequent British defence concepts (UK MOD, 2012, pp. 3-10).

Commenting on the insights provided by Flynn et al. (2009) it has been suggested that improvements to the Intelligence Preparation of the Environment (IPOE) process would address many of the issues raised (DeGennaro, 2018). Acknowledging the inability of intelligence organizations alone to create understanding within the ambiguity of such environments Degenarro advocated that other branches of the military should have greater involvement. This is particularly relevant given the broad range of non-military activities potentially faced. It would also facilitate access to more relevant data, therefore enabling improved knowledge generation. Creating enhanced granularity of the operating environment should lead to improved discovery of the subtle and nuanced changes indicatingthe onset and development of grey zone activity.

Through understanding of such historical studies and the resulting academic discourse Governments and military organizations do appear to have recognized and understand the need to widen the scope and to synchronize and coordinate with other levers of national power in a more coherent way. Williamson stresses the need to develop “enhanced interagency and multinational capabilities and coordination” and calls for improvements todiplomacy and statecraft in addition to improvements to military capabilities (2009, p. 30). Many of the lessons identified in Iraq and Afghanistan have created an understandingthat in order to counter these emerging threats the application of military power alone will beinsufficient (Hoffman, 2018). In the UK, recognition of the interdependency between organizations has led to the creation of a “Fusion Doctrine” aimed at harnessing capabilities required to “detect, deter and counter hybrid attacks and other threats” The value of leveraging foreign partnerships in addition to domestic ones is also recognized as being of high importance (Younger, 2018).

One thing above all that must be understood by analysts and policy makers alike is that in addition to improvements to the system, is the requirement to embrace alternative approaches. Central to this is an understanding that "more than just the ontology of threats has changed, that in fact it is in the epistemological area that the most meaningful changes have taken place" (Dunn Cavelty & Mauer, 2009, p. 123). This requires the adoption of a postmodern conceptual approach to address the management of high levels of uncertainty and ambiguity. It must be clearly embraced by both analysts and policy makers that "trying to eliminate or reduce uncertainty ... is often impossible or infeasible" (Friedman & Zeckhauser, 2012, p. 824). This will be fundamental in understanding "multiple possibilities that have meaningfully different implications for policy. (Friedman & Zeckhauser, 2012, p. 825). They also suggest that the goal of intelligence is to describe the uncertainty that surrounds a specific question, and not to eliminate or to reduce this uncertainty per se (Friedman & Zeckhauser, 2012, p. 826).

Pythian provides some valuable insights that could assist in understanding how to approach the highly complex mix of knowns and unknowns necessary to drive effective judgements when addressing gray zone activities. Given the dynamic and evolving nature, it is key to understand the relationship between ignorance, uncertainty, risk and threat (2012, p. 195). In situations where high degrees of uncertainty are involved, and judgements based on partially understood events "carry with them high degrees of uncertainty as to outcomes". Pythian (2012, p. 199) underlining the reflexive role that intelligence plays in supporting the decision-making process. Due to this reflexive rationality "an awareness of both complexity sciences and postmodernism might increase understanding of the limitations of knowledge and lead to the establishment of a political discourse of uncertainty" (Dunn Cavelty & Mauer, 2009, p. 125). This will be critical in order to counter "the vicious circle that uncertainty has created for organizations built for the creation of actionable knowledge" (Dunn Cavelty & Mauer, 2009, p. 139).

Analysts must recognize that when knowledge gaps do occur there is a responsibility to understand and manage the "consequences of the missing information" (Canton, 2008, p. 487). Embracing such concepts will lead to improved capacity for the early identification of emerging and developing threats that enable greater focus to be placed on the problem set. In the light of threats of the nature occurring in gray zone conflict critical thinking methods will contribute immensely to deal with the core challenges to reasoning in intelligence identified as "insufficiency, irrelevancy, indeterminacy and instrumentality" by Hendrickson (2008, p. 689).

The use of alternative analytical techniques can be enhanced through the utilization of evolving technology such as Artificial Intelligence/Machine Learning (AI/ML) programs which will increase speed and processing power. In order to take full advantage of this intelligence organizations will need to review structures and manpower requirements to include analysts "who understand algorithms and coding" (Horowitz, 2018). It will be important to understand how this technology will impact on both the intelligence community, its methodologies, and on the decision-making process that it supports. Adversaries will also be seeking to harness such advanced technologies themselves in order to target vulnerabilitiesand it has been recognized that "the United States and Europe are ill-equipped to respond to Russian AI-driven asymmetric warfare (ADAW) in the information space" (Polyakova, 2018).

There have been significant efforts to close this technological gap with projects such as the COMPASS program in the US which aims to identify "an adversary's intentions and provide decision makers high-fidelity intelligence on how to respond — with positive and negative trade-offs for each course of action" (DARPA, 2018). From the US military perspective, modernization is also occurring with the planned employment of the Machine-Assisted Analysis Rapid-Repository System (MARS) as discussed by the DIA Director recently (CSIS, 2018). Despite such technologically advanced systems however, Karlin suggests that uncertainty will remain a constant and U.S. policymakers will nevertheless have to make decisions about dynamic conflict based on incomplete information (Karlin, 2018).

Which raises the final and arguably most critical aspect regarding the responses and actionstaken against activity within gray zones. As with all discussions on intelligence operations,the most fundamental issue will inevitably lie with the ultimate utility of its products. Therefore, one needs to examine what new challenges the emergence of gray zone conflict will have on the policy and decision-making process. Firstly, it is key to ensure that those involved are cognizant of the impacts that these activities are having on the current and future character of competition. As previously referenced, there is now a solid body of academic and other writings on the subject, and senior military and civilian leaders are certainly becoming increasingly aware. That said, numerous studies have identified multiple examples where policy makers have consistently failed to act upon the intelligence provided to them. Marrin (2017) amongst others questions the level of influence that intelligence really has on national-level decision making, and there is certainly validity to his suggestion of the further study required in this key area. As Gentry (2018) also indicates, the actions taken by decision makers will determine the success of an intelligence operation. His suggestion that priority be given to increasing understanding of the capabilities of intelligence is particularly relevant when dealing with such levels of uncertainty.

If the issue was not complex enough, adversaries will constantly be pushing the envelope intesting the tolerances of their opposing decision makers, as Chipman (2018) contends in hisdiscussion mentioned earlier. They will also deliberately attempt to obfuscate involvement seeking to limit the ability to deter or defeat their efforts and impeding the ability for a response within a time frame to alter the outcomes. Mumford (2017) explains the dilemma this will create where "over-reaction looks pre-emptive and disproportionate if clear responsibility for an attack has not been established; but the lack of a response leaves a stateopen to death by a thousand cuts".

At any stage of the process, give the high levels of uncertainty there is always the risk that one or other of the protagonists can misread the situation leading to incorrect or inappropriatedecisions which will increase chances of adversarial success, or perhaps even escalate the situation in a direction that neither side desires. According to Pillar (2009, p. 9) the "inherent indeterminacy of complex events" can and will change depending on decisions that have yet to be made. There is also a danger that any politicization of the intelligence provided can further complicate the issues when decision makers have little understanding as to the outcomes of using the intelligence for their own political purposes. Gill & Pythian (2012) also offer significant insights into this phenomenon.

Freier sums up the essence of the conundrum that adversaries seek to achieve when outlining concepts of "Risk Confusion" & "Hyper Risk" in which he sees "gray zone hybridity and menace combine in strategic decision-making to paralyze effective counter-gray zone approaches". He adds that "risk confusion emerges when the hazards associated with action and inaction against gray zone rivals appear equally unpleasant" (Freier, 2018). These issues appear to have driven a new approach to the formulation of national strategies in the United Kingdom. This has led to the creation of the "Fusion Doctrine" previously mentioned by the Head of the Intelligence Service to create a more holistic approach to improve nationallevel decision making and "enable earlier identification of emergent shocks" (McKeran, 2019). It is of course perhaps too early to tell after less than one year in existence, but McKeran is cautious but positive with the progress achieved thus far and it will be worthy of consideration as a model for others.

Conclusion and Recommendations

There has been discord as to the validity to the concept of Hybrid war, with increasing focus placed on the emerging “gray zone”. Many of the elements of hybrid environments present few unrecognized challenges. It is the nebulous “gray zone”, rapidly generating ambiguity, uncertainty and complexity that will be the most problematic to intelligence operations. There will certainly be enormous strain placed on the intelligence community by the need to identify and monitor simultaneous, dynamic multiple activities in addition to existing responsibilities. It is concluded that in order to be better placed to address the wicked problems encountered when dealing with such highly complex environments will only be achievable through the adoption of new conceptual and methodological approaches.Therefore, the following should be considered:

A Holistic Approach — The scope must be broadened beyond the military domain and encompass and leverage all aspects of power and the information space. The UK’s Fusion Doctrine may provide a useful benchmark how this may be achieved.

Historical Perspectives — Learning from historical perspectives, particularly those involving highly complex environments and multiple adversaries such as experienced during recent operations in Afghanistan. Equally useful will be studies of conflicts where asymmetric strategies and tactics predominated.

Knowledge Creation — Improved understanding of the creation of knowledge through the adoption of improved collection and data management utilizing technical innovation.

The Management of Uncertainty — Education for intelligence practitioners stressing postmodern ideas regarding the fallibility of intelligence. The incorporation of new analytical techniques addressing the management of uncertainty and improving criticalthinking will be necessary.

Producer/Consumer Interface — Improvements to the relationships between analysts and the policy makers they support, and education about the extreme challengers faced. This should include for both constituencies a far greater understanding of the reflexive nature ofintelligence judgements in risk formulation.

Such modifications will be essential in order to deliver the appropriate responses to counter activities in the gray zone and ensure they remain within the normative boundaries demandedby policy makers and their electorates.

Finally, it needs to be remembered that our own complexity may be as challenging as thecomplexity we face.

References

Betts, R. K. (2002). Fixing Intelligence, *Foreign Affairs*, *81*(1), 43–59.

Brantley, A., and Collins, L. (2018). A bear of a problem: Russian special forces perfectingtheir cyber capabilities, *Association of the United States Army*, accessed 29 Nov. 2018, available online at: https://www.ausa.org/articles/bear-problem-russian-special-forces-perfecting-their-cyber- capabilities.

Canton, B. (2008). The active management of uncertainty, *International Journal ofIntelligence and Counter Intelligence*, *21*(3), 487–518.

Center for Strategic and International Studies (CSIS) (2018). A discussion on national security with DIA director Robert Ashley, accessed on 18 Sep., 2018, available online at: https://www.csis.org/events/discussion-national-security-dia-director-robert-ashley.

Chambers, J. (2016). Countering gray-zone hybrid threats, *Modern War Institute at WestPoint.*

Chipman, J. (2018). A new geopolitical challenge to the rules-based order, *InternationalInstitute for Strategic Studies*, accessed on 19 Nov., 2018, available online at: https://www.iiss.org/blogs/analysis/2018/11/challenge-rules-based-order.

Cillufo, F., Marks, R., and Salmoiraghi G. (2010). The use and limits of U.S. intelligence, *The Washington Quarterly*, *25*(1), 61–74.

Coughlin, C. (2018). Russia poses greater threat to Britain than Isil, says new Army chief, *The Daily Telegraph*, accessed on 24 Nov., 2018, available online at: https://www.telegraph.co.uk/news/2018/11/23/russia-poses-greater-threat-britain-isil-says-new-army-chief/.

Cullen, P. (2018). Hybrid threats as a new 'wicked problem' for early warning, *StrategicAnalysis.*

Defense Advanced Research Projects Agency (DARPA) (2018). Making Gray-ZoneActivity more Black and White, *DARPA Outreach*, accessed on 15 Oct., 2018, available online at: https://www.darpa.mil/news-events/2018-03-14.

DeGennaro, P. (2017). The gray zone and intelligence preparation of the battle space, *The Small Wars Journal Online*, accessed on 23 May, 2018, available online at: http://smallwarsjournal.com/jrnl/art/the-gray-zone-and-intelligence-preparation-of-the-battle-space.

Dubick, J., and Vincent, N. (2018). The Gray Zone in context, *Institute for the Study of War.*

Dunn Cavelty, M., and Mauer, V. (2009). Postmodern intelligence: Strategic warning in an age of reflexive intelligence, *Security Dialogue*, *40*(2), 123–144, doi: 10.1177/0967010609103071, available online at: http://journals.sagepub.com.ezproxy3.lib.le.ac.uk/doi/pdf/10.1177/0967010609103071.

Flynn, M., Pottinger, M., and Batchelor, P. (2010). Fixing Intel: A blueprint for makingintelligence relevant in Afghanistan, *Center for New American Security.*

Freier, N. (2018). The darker shade of gray: A new war unlike any other, *Center forStrategic and International Studies*, accessed on 15 Sep., 2018, available online at: https://www.csis.org/analysis/darker-shade-gray-new-war-unlike-any-other.

Freier, N., Burnett, C., Cain, W., Compton. C., Hankard, S., Hume. R., Kramlich, G., Lissner, J., Magsig, T., Mouton, D., Muztafago, M., Schultze, J., Troxell, J. and Wille, D. (2016). *Outplayed: Regaining Strategic Initiative in the Gray Zone*, Strategic Studies Institute, United States Army War College Press, accessed on 15 Sep., 2018, available online at: https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325.

Friedman, J., and Zeckhauser, R. (2012). Assessing uncertainty in intelligence, *Intelligence and National Security*, *27*(6), 824–847JA.

Galeotti, M. (2014). The 'Gerasimov Doctrine' and Russian Non-Linear War, *Moscow's Shadows* (blog), accessed on 20 Nov., 2018, available online at: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Garamone, J. (2017). Trump announces new whole-of-government national security strategy, *Defense News*, US Department of Defense, 18 December 2018, accessed 10 Apr., 2018, available online at: https://www.defense.gov/News/Article/Article/1399392/trump-announces-new-whole-of-government-national-security-strategy/.

Gentry, John A. (2008). Intelligence failure reframed, *Political Science Quarterly*, *123*(2), 247.

Giles, K. (2016). The next phase of Russian information warfare, *NATO StrategicCommunications Centre of Excellence*, accessed on 18 Nov., 2018, available online at: https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Gill, P. (2009). Security intelligence and human rights: Illuminating the "heart of darkness"?, *Intelligence and National Security*, *24*(1), 78–102.

Gill, P., and Pythian, M. (2013). *From Intelligence Cycle to Web of Intelligence*, *Understanding the Intelligence Cycle*, Chap. 2, Routledge.

Glenn, R. (2009). Thoughts on hybrid conflict, *Small Ward Journal*, accessed on 14 Oct., 2018, available online at: http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf%3Fq%3Dmag/docs- temp/188-glenn.pdf.

Harris, C., and Clarke, M. (2018). Russia in review: Russia's lessons learned in Syria, *Institute for the Study of War Blogspot*, accessed 9 Nov., 2018, available online at: http://iswresearch.blogspot.com/2018/11/russia-in-review-russias-lessons.html.

Harris, D. (2016). The consequences of eroding human intelligence collection, *The Cyber Brief*, accessed 30 Oct., 2018, available online at: https://www.thecipherbrief.com/column_article/the-consequences-of-eroding-human-intelligence-collection.

Hendrickson, N. (2008). Critical thinking in intelligence analysis, *International Journal ofIntelligence and Counter Intelligence*, *21*(4), 679-693, doi: 10.1080/08850600802254749.

Hicks, K., Schaus, J., and Matlaga, M. (2018). Zone defense: Countering competition in thespace between war and peace, *Report 2018 Global Security Forum Experts Workshop Center for Strategic & International Studies*, accessed on 27 Nov., 2018, available online at: https://csis-prod.s3.amazonaws.com/s3fs-public/event/181126_Gray_Zone_Defense.pdf.

Hoffman, F. (2007). Conflict in the 21st Century: The rise of hybrid wars, *PotomacInstitute for Policy Studies.*

Hoffman, F. (2009). Hybrid warfare and challenges, *Joint Forces Quarterly*, (52), 34–39, accessed on 14 Oct., 2018, available online at: http://smallwarsjournal.com/documents/jfqhoffman.pdf.

Hoffman, F. (2014). On not so new warfare: Political warfare vs hybrid threats, *War on the Rocks Online*, accessed on 14 Oct., 2018, available online at: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Hoffman, F. (2016). The contemporary spectrum of conflict: Protracted, gray zone,ambiguous, and hybrid modes of war, *2016 Index of US Military Strength*, pp. 25–36.

Hoffman, F. (2018). Examining complex forms of conflict: Gray zone and hybrid challenges, *PRISM*, *7*(4).

Horowitz, M. (2018). Artificial intelligence, international competition, and the balance of power, *Texas National Security Review*, *1*(3), accessed 20 Nov., 2018, available online at: https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of- power/.

Hulnick, A. (2006). What's wrong with the Intelligence Cycle, *Intelligence and National Security*, *21*(6), 959–979.

Jackson, P. (2010). On uncertainty and the limits of intelligence, Loch K. Johnson (Ed.), *The Oxford Handbook of National Intelligence*, Oxford University Press, pp. 453–471, doi: https://doi.org/10.1093/oxfordhb/9780195375886.003.0028.

Johnson, L. (2010). Evaluating "Humint": The role of foreign agents in U.S. security, *Comparative Strategy*, *29*(4), 308–332, doi: 10.1080/01495933.2010.509635.

Karlin, M. (2018). The implications of artificial intelligence for national security strategy, The Brookings Institute, accessed on 20 Nov., 2018, available online at: https://www.brookings.edu/research/the-implications-of-artificial-intelligence-for-national-security-strategy/.

Kramer, A. (2019). Russian general pitches "information operations" as a form of war, *New York Times*, accessed on 2 Mar., 2019, available online at: https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

Krulak, C. (1999). The strategic corporal: Leadership in the Three Block War, *Marine Corps Gazette*, *83*(1).

Lowenthal, M. (2010). The policymaker-intelligence relationship, in: *The Oxford Handbook of National Security Intelligence*, doi: 10.1093/oxfordhb/9780195375886.003.0027.

Majumdar (2015). How Russia could win the battle for Syria, *The National Interest*, accessed on 30 Oct., 2018,available online at: https://nationalinterest.org/print/blog/how-russia-could-win-the-battle-syria-14031.

Marrin, S. (2017). Why strategic intelligence analysis has limited influence on Americanforeign policy, *Intelligence and National Security*, *32*(6), 725–742.

McKeran, W. (2019). Fusion doctrine: One year on, Royal United Services Institute, accessed on 8 Mar., 2019, available online at: https://rusi.org/commentary/fusion-doctrine-one-year.

Miller, M. (2015). Hybrid warfare: Preparing for future conflict, Air War College, AirUniversity, Maxwell AFB, AL, accessed on 18 Oct., 2018, available online at: http://www.dtic.mil/dtic/tr/fulltext/u2/a618902.pdf.

Mumford, A. (2017). The new era of the proliferated proxy war, *The Strategy Bridge*, accessed on 10 Sep., 2018, available online at: https://thestrategybridge.org/the-bridge/2017/11/16/the-new-era-of-the-proliferated-proxy-war.

Ollivant, D. (2016). The rise of the hybrid warriors: From Ukraine to the Middle East, *War on the Rocks*, accessed on 16 Oct., 2018, available online at: https://warontherocks.com/2016/03/the-rise-of-the-hybrid-warriors-from-ukraine-to-the-middle-east/.

Paul, C. (2016). Confessions of a hybrid warfare skeptic, *Small Wars Journal*, accessed on 14 Oct., 2018, available online at: http://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic.

Parameswaran, P. (2015). Are we prepared for "hybrid warfare"?, *The Diplomat*, accessed on 18 Oct., 2018, available online at: https://thediplomat.com/2015/02/are-we-prepared-for-hybrid-warfare/.

Pillar, P. (2010). The perils of politicization, in: *The Oxford Handbook of National Security Intelligence*, doi: 10.1093/oxfordhb/9780195375886.003.0029.

Phythian, M. (2012). Policing uncertainty: Intelligence, security and risk, *Intelligenceand National Security*, *27*(2), 187–205.

Polyakova, A. (2018). Weapons of the weak: Russia and AI-driven asymmetric warfare, The Brookings Institute, accessed on 18 Nov., 2018, available online at: https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare.

Reichborn-Kjennerud, E., and Cullen, P. (2016). What is hybrid warfare?, Norwegian Institute of International Affairs Policy Brief, accessed on 14 Oct., 2018, available online at: https://brage.bibsys.no/xmlui/bitstream/handle /11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf?sequence=3&isAllowed=y.

Sari, A. (2015). Legal aspects of hybrid warfare, *Lawfare Blog Post*, accessed on 14 Oct., 2018, available online at: https://www.lawfareblog.com/legal-aspects-hybrid-warfare.

Schneider, B. (2013). Could U.S. have stopped Syria's chemical attack?, *CNN*, 11 Sep., 2013, accessed on 8 Apr., 2018, available online at: https://www.cnn.com/2013/09/11/opinion/schneier-intelligence-limitation.

SIGAR (2018). Stabilization: Lessons from the U.S. Experience in Afghanistan, Special Inspector General for Afghanistan Reconstruction (SIGAR), accessed on 18 Oct., 2018, available online at: https://www.sigar.mil/pdf/lessonslearned/SIGAR-18-48-LL.pdf.

Simileanu, V. (2018). Hybrid war: Conceptual approach, *Relatii Internationale Plus*, *1*(13), 263–273.

United Kingdom Ministry of Defence (2012). Joint Concept note 2/12 future landoperating concept, The Development, Concepts and Doctrine Centre.

United States Army Asymmetric Warfare Group (2016). *Russian New Generation Warfare Handbook*, Public Intelligence Net, accessed on 16 Oct., 2018, available online at: https://publicintelligence.net/awg-russian-new-warfare-handbook/.

United States Army Training & Doctrine Command (TRADOC) (2017). Multi-domain battle: Evolution of combined arms for the 21st century, 2025-2040 (draft).

Van Dam, C. (2019). Defense Intelligence Agency director focuses on leadership, public service at 2019 INSA Achievement Awards, Defense Intelligence Agency, accessed on 2 Mar., 2019, available online at: http://www.dia.mil/News/Articles/Article-View/Article/1772876/defense-intelligence-agency-director-focuses-on-leadership-public-service-at-20/.

Van Puyvelde, D. (2015). Hybrid warfare — Does it even exist?, *NATO Review*, accessed on 14 Oct., 2018, available online at: https://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm.

Weisberger, M. (2014). A look inside a secret US Air Force Intelligence Center, *Defense One*, accessed on 20 Nov., 2014, available online at: https://www.defenseone.com/technology/2014/11/look-inside-secret-us-air-force-intelligence-center/99347.

Williamson, S. (2009). From fourth generation warfare to hybrid war, US Army WarCollege, accessed on 14 Oct., 2018, available online at: http://www.dtic.mil/dtic/tr/fulltext/u2/a498391.pdf.

Wittes, B. (2015). What is hybrid conflict?, *Lawfare Blog*, accessed on 14 Oct., 2018, available online at: https://lawfareblog.com/what-hybrid-conflict.

Younger, A. (2018). MI6 "C" speech on fourth generation espionage, UK Government Website, accessed on 3 Dec., 2018, available online at: https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage.