UNDERSTANDING GRAY ZONE WARFARE FROM MULTIPLE PERSPECTIVES

Tahir Mahmood Azad
King's College London

Muhammad Waqas Haider
Lancaster University

Muhammad Sadiq
King's College London

This study examines the dynamics of gray zone warfare by analyzing its conceptualization in the literature and through its practice in several recent examples. Ever-increasing changes in the characteristics of contemporary warfare have complicated the security environment of the 21st century. Modern warfare inclines toward non-kinetic dimensions based on the principles of hybridity, soft power, and ambiguity. This changing nature of warfare has been defined and categorized in diverse ways, leading to numerous perspectives revealing more confusion than clarity. The terms "hybrid warfare," "gray zone warfare," "unrestricted warfare," and "ambiguous warfare" have received unprecedented attention in recent years. A key contemporary challenge is to differentiate between war and peace because gray zone warfare occupies the space in between both these situations. Many contemporary conflicts are neither black nor white; instead, they fall in the middle of the two: the gray zone. These factors underscore the significance of evaluating and understanding the concept of gray zone warfare. The United States considers Russia, China, and Iran as revisionist states that employ gray zone warfare in various domains to challenge the United States-led world order. South Asia is also a *manifested playground of gray zone warfare. The research further distinguishes between gray zone warfare and hybrid warfare and proposes strategies for countering this threat.*

Keywords: War and Peace, Gray Zone Warfare, Information Operations, Revisionist States, Grey Zone, Russia, China, Ukraine 2014, United States, South Asia.

Entender la guerra en zona gris desde múltiples perspectivas

Esta investigación examina la dinámica de la guerra en la zona gris mediante la evaluación de estudios de casos de la época contemporánea. Las guerras y las guerras siguen evolucionando debido a los avances en el campo de la ciencia y la tecnología. Los cambios cada vez mayores en las características de la guerra contemporánea han complicado el entorno de seguridad en el siglo XXI. La guerra moderna se inclina hacia dimensiones no cinéticas basadas en los principios de hibridez, poder blando y ambigüedad. Esta naturaleza cambiante de la guerra se ha definido y categorizado en diversidad, y existen numerosas perspectivas en todo el mundo. Los términos "Guerra híbrida," "Guerra en la zona gris," "Guerra sin restricciones" y "Guerra ambigua" han recibido una atención sin precedentes en los últimos años. El mayor desafío de los tiempos contemporáneos es diferenciar entre guerra y paz porque la guerra de zona gris ocupa el espacio entre ambas situaciones. Estos conflictos no son blancos ni negros, sino que caen en el medio de los dos, que es la zona gris. Estos factores subrayan la importancia de evaluar y comprender el concepto de guerra de zona gris. Estados Unidos considera a Rusia, China e Irán como estados revisionistas que emplean la guerra de zona gris en varios dominios para desafiar el orden mundial liderado por Estados Unidos. El sur de Asia también es un campo de juego manifiesto de la guerra de la zona gris. La investigación distingue además entre la guerra de zona gris y la guerra híbrida y propone estrategias para contrarrestar esta amenaza.

Palabras clave: Guerra y Paz, Guerra de Zona Gris, Operaciones de Información, Estados Revisionistas, Rusia, China, Estados Unidos, Sur de Asia.

从多个视角理解灰区战

本研究通过评价当代案例研究，对灰区战的动态进行了分析。战争因科学技术领域的进步而不断发展。当代战争特点的不断变化，使*21*世纪的安全环境复杂化。现代战争向基于混合、软实力和模糊性原则的非动力维度倾斜。这种不断变化的战争性质已存在多种定义和分类，并且世界各地存在许多观点。近年来，“混合战”、“灰区战”、“超限战”、“模糊战”等术语受到了前所未有的关注。当代最大的挑战是区分战争与和平，因为灰区战位于这两种情况之间。这些冲突并不是非黑即白，而是位于两者之间，即灰区。这些因素强调了评价和理解灰区战概念的重要性。美国将俄罗斯、中国和伊朗视为修正主义国家，后者在不同领域利用灰区战挑战美国主导的世界秩序。南亚也是灰区战的一个明显地区。本研究进一步区分了灰区战与混合战，并提出了应对这种威胁的策略。

关键词：灰区战，信息操作，修正主义国家，战争与和平，俄罗斯，中国，美国，南亚。

Wars and warfare continue to evolve due to advancements in the fields of science and technology. Prussian military philosopher Carl von Clausewitz claimed that “War is more than a true chameleon that slightly adapts its characteristics to the given case” (Howard and Paret 1976, 89). Clausewitz further postulated that the interactions of the trinity (people, governments, and military forces) alter and exploit the three essential constituents of war: hatred and violence, chance, and probability and political deliberations (Howard and Paret 1976, 79). These constituents are not novel and have been essential ingredients in recorded war history. The culmination of the Second World War had a considerable impact on reshaping the pattern of conflicts and systems of governance. The emergence of non-state actors (NSAs) further reshaped power dynamics by wielding extensive influence in national and international arenas during the second half of the 20th century. Geo-economics and economic interdependence became additional significant factors in altering the dynamics of interstate relations and the international system. Geo-economics brought systematic changes in the international system which significantly reduced the use of kinetic means and hard military power, at least in the Western world. These dynamics alternatively reshaped the nature and characteristics of 21st-century warfare toward non-kinetic dimensions based on the principles of hybridity, soft power, and ambiguity. Factors such as rapid technological advancements, geopolitics draped in geo-economics, ever-increasing fissures in societies, and the diminishing boundaries of nation-states have massively impacted social interactions, political structures, and global economies. These, in turn, have had a seismic impact on contemporary conflict and warfare.

Terms such as "Hybrid Warfare," "Gray Zone Warfare," "Unrestricted Warfare," and "Ambiguous Warfare" have received unprecedented attention in recent years. Hoffman (2016, 25) argued that the biggest challenge of our times is to identify war—as we do not know what war is and what it is not. Research on the emergence of new and generational warfare has likewise gained momentum over the past few years, yet Hoffman's position remains solid because the boundaries between war and peace have been increasingly blurred. There has been a massive rise in covert, irregular, and ambiguous conflicts over the past three decades, coupled with a significant reduction in overt interstate conflicts. The Arab Spring and color revolutions are the classic manifestations of the changing nature of wars and warfare. The Russian annexation of Crimea in 2014 further enhanced Western interest in the evolving concepts of gray zone/hybrid warfare employed by Russia in Georgia in 2008 and Ukraine in 2014.

The term "gray zone" first appeared in the 2010 *Quadrennial Defense Review* (QDR). It broadly depicts multi-dimensional activities aimed to alter adversary behavior while remaining below the threshold of conventional military employment (Hoffman 2016, 26). Assertive Chinese actions in the South China Sea and its involvement in clandestine activities to tailor the international political and economic landscape to its own ends are also manifestations of gray zone warfare. Strategies discussed later in this article, such as "little green men," cyber exploitation, and disinformation, are the common themes in the gray zone. And in recent years, Russia expanded its use of gray zone warfare against Ukraine to a massive level involving covert and sabotage operations to prepare the ground favorably for a full-scale invasion. Though it launched a war against Ukraine in February 2022, Russia continues gray zone warfare to support its physical invasion.

Much controversy and debate surround how to understand gray zone warfare today in terms of the limits of its definition, its relation to—or differences with—cognate concepts often used interchangeably and in relation to the diverse ways in which it has been practiced in recent decades (and how that practice continues to evolve). In this article, we first explore and unpack the most widely used definitions of gray zone warfare to reveal its conceptual and pragmatic nuances and differences from similar concepts. We then examine briefly a few recent examples where gray zone warfare was employed, to flesh out and extend our understanding of a concept and a practice that, by its very nature, continues to be fraught with confusion and ambiguity.

Multiple Perspectives on Gray Zone Warfare

Many critics argue that gray zone warfare is just a tautological expression of terms such as hybrid warfare, fifth-generation warfare, proxy warfare, unconventional warfare, and irregular warfare (see, e.g., Matisek 2017, 4). Such arguments, we submit, are not based on sound evidence. Our central contention is that gray zone warfare is not just a catchy phrase, but rather a distinct domain of warfare. The doctrine of the armed forces of the United States defines warfare as "the mechanism, method, or modality of armed conflict against the enemy" (The Joint Staff 2013). The gray zone is that domain where the distinction between war and peace becomes impossible to draw with certainty due to the ambiguity of the tactics employed. On the continuum of war and peaceful relations, if peaceful diplomatic relations are placed at one end and total war on the other end, then the space in between both extremes is "the gray zone" (August 2016, 15). The U.S. government and the broader strategic studies community have recently paid much attention to the concept of "gray zone" conflicts (Brands 2016, 1). However, at present, no universally agreed-upon definition exists. This not only adds to the conceptual confusion and ambiguity surrounding gray zone warfare; it also obfuscates identifying gray zone threats in practice and the already difficult task of countering them. These factors show a requirement to be more explicit about what is meant by the phrase "gray zone warfare." In what follows, we contribute to discussions surrounding this objective with the hope of further refining a working understanding of gray zone warfare conceptually. We also offer brief examples of gray zone warfare in practice and end by drawing attention to a few potential avenues for countering it.

Brands (2016, 1) defines gray zone warfare as "activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war." Brands highlights the *coercive* nature of gray zone warfare, but it remains below the spectrum of a conventional military encounter, and red lines are not violated. The aim remains to achieve desired objectives without the overt use of military forces to avoid the risks posed by direct confrontation.

Brands is not the only commentator to underscore the coercive nature of gray zone warfare. U.S. Defense Department officials similarly argue that the gray zone lies at the lower end of the spectrum where full-blown war is not in progress, but coercive military strategies are underway to change the *status quo* (Roberts 2015, 75). Hoffman (2016, 25) is critical of the American strategic culture as it lacks an appreciation of history and pays little attention to the diversity of adversaries and the forms conflict can adopt. The importance of altering the *status quo* in his account of gray zone warfare is similar to that found in Wirtz (2017, 107) who writes that states and NSAs employ three types of strategies for changing the *status quo*. These include proxy warfare, the *fait accompli*, and the exploitation of ambiguous deterrence situations—also known as "salami tactics." These short-of-war strategies may be employed individually or in combination by a diverse range of state actors and NSAs. The reason for employing such strategies may include the risks associated with conclusive tactics, like an open conflict, and also fewer chances of response from the defender owing to the limited nature of provocation actions. Hoffman (2016, 26) goes on to note that, in gray zone conflicts, "adversaries employ an integrated suite of national and subnational instruments of power in an ambiguous war to gain specified strategic objectives without crossing the threshold of overt conflict." He also advocates the use of proxy forces, as highlighted by Wirtz (2017). Both the above definitions underline the *use of proxies and multiple instruments in ambiguous scenarios* to achieve the desired objective as the essence of gray zone warfare.

In a seminal monograph, Mazarr (2015, 58) describes the various characteristics of gray zone warfare in detail. They include cohesive and integrated campaigns to pursue political objectives, to stay below the red lines of escalation to a conventional conflict, and to achieve steady movement toward an objective instead of decisive campaigns for immediate results. Mazzar further argues that many states employ gray zone strategies as a distinct and particular form of warfare, but at the same time many weak states employ such forms of conflict because they do not have any other choice. A range of instruments and strategies can be adopted by the actors employing gray zone warfare. These include low-end tactics to high-end tactics in economic, military, informational, political, and other diverse domains. The aggressor has a choice to exploit any domain that suits the achievement of their desired objectives. These instruments are not definite means and may be employed individually or can be blended to suit the scenario. Here, the central idea of the gray zone is to confront the opponent with *conundrums* where one particular strategy in the cycle may have limited impact but countering that strategy may lead to crisis or escalation (Mazarr 2015, 61). Mazarr also highlights that the defender stays in a state of response dilemma while the aggressor modifies strategies gradually to bring the defender into a position of no-win, at least in theory.

The U.S. Special Operations Command defines gray zone warfare strategies as

> Competitive interaction among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, the opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks. (Bratton 2020, 42)

This comprehensive definition encapsulates the actors involved, the strategies adopted, and the ambiguity associated with such tactics. It also contributes more focus to the blurred lines between war and peace. The tactics give leverage to the aggressor to achieve an objective without triggering a significant response from the defender, while the defender either remains in a dilemma due to the risk of escalation or accepts the new *status quo* without responding to gray zone strategies.

Adding both context and a focus on the actors involved in gray zone warfare, Hayes (2018, 61) discusses the concept in terms of revisionist powers such as Russia, China, and Iran that employ military tactics in an integrated manner through economic, informational, political, and technological advancements to pursue their goals while remaining below the threshold of triggering a significant response from the United States. Hayes' (2018) definition is comparable to that given by Mazarr (2015). The view from the perspective of revisionist states is also common in the definitions formulated by Wirtz (2017), and the U.S. Department of Defense (Roberts 2015). Furthermore, Hayes (2018) and Mazarr (2015) argue that China, Russia, and Iran are the revisionist powers that possess the intent and capability to employ gray zone warfare against the United States. Votel and others (2016, 102) write that "the gray zone is characterised by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war." This also shares similar components to the definitions given by Hayes and Mazarr.

Narrowing down the definition to the South Asian context, General Zubair Mahmood Hayat (ex-Chairman of the Joint Chiefs of Staff Committee Pakistan) defines "The gray zone hybrid conflict [a]s a tailored mix of subversion, terrorism, irregular warfare tactics, economic warfare, information warfare, social engineering, societal disruption, conventional application especially the special operations and finally the criminal behaviour" (Hayat 2018, 7). This adds nuance to the concept by drawing attention to the manifold powerful strategies that can be adopted by an actor employing hybrid/gray zone warfare. It nevertheless lacks clarity concerning the actors and red lines of such conflicts. However, the elements Hayat highlighted are similar to the definitions of most Western scholars. An Indian scholar, Ahluwalia (2019, 2), notes that "The gray zone conflict involves activities directed towards the accomplishment of ends by using all methods short of a declaration of war." Ahluwalia further argues that gray zone conflicts lie between peace and war and each country defines its red lines for such conflicts. While consistent with the general view of what gray zone warfare consists of, this definition nevertheless lacks clarity as short-of-war tactics are one of the instruments of the gray zone, but not the whole gray zone.

Definitional Nuances

Analyzing this range of definitions reveals that the informational, economic, military, and political domains are the major playing fields for gray zone warfare while staying below the threshold of conventional war is its fundamental principle. As we show shortly, tactics such as cyber warfare, proxy wars, and *fait accompli* are widely employed by actors resorting to gray zone warfare. The present study adopts the definition of gray zone warfare given by the U.S. Special Operations Commands:

> Gray zone challenges are defined as competitive interaction among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks. (Bratton 2020, 42)

This definition is, for our purposes, the most precise and comprehensive while also underlining linkages between a diverse range of actors and activities.

Instruments of Gray Zone Warfare

The literature on gray zone warfare suggests that most of the strategies employed in contemporary conflicts fall into the category of gray zone warfare, but there is no consensus on this argument due to the use of several terminologies. However, the employment of "little green men," salami tactics, information operations, cyber warfare, proxy wars, special operations, and *fait accompli* are the common threads in most of the studies conducted on gray zone warfare (see, e.g., Hayat 2018; Hayes 2018; Hoffman 2016; Jackson 2019; Wirtz 2017). Aggressors may employ any one instrument or multiple instruments simultaneously to achieve their desired objectives while the defender is placed in an uncomfortable position if they respond to such actions due to fear of escalation. The instruments of gray zone warfare are discrete or exclusive, but they share specific characteristics such as hybrid means, a threat to war/military conventions, and ambiguity. Gray zone instruments are currently undergoing further conceptualization and need more attention as they can be employed to change the *status quo*. So what is precisely meant by the concepts mentioned above? Below we provide some details.

Little Green Men

The concept of "little green men" is one of the widely agreed-upon instruments of gray zone warfare. Scholars such as Jackson (2017, 43) call them "intermediaries," "agents," or the "fifth column." Bensahel (2017, 5) defines little green men in the 2014 Russian context as "soldiers and other agents without any uniforms, insignia, or other identifiable markings that enabled Russia to deny any involvement." States or NSAs employ agents who cannot be easily distinguished and cannot be associated with the party controlling them, thus creating ambiguity and confusion. The underlying logic behind using such agents is to avoid a significant response from a defender. A conventional military may, of course, very likely trigger a similar retaliation from the defender. Ambiguity about the controlling party makes it likely that the defender will be much more cautious in initiating a response against unidentifiable agents. Aggressors who employ intermediaries may conceal their liability by disguising any identification of authority, raising the question of control and hiding the intent of the agents (Jackson 2017, 44). The defender faces the dilemma of finding answers to the same questions—a challenging task—and may not be able to initiate a response without finding answers to the above factors with reasonable accuracy, precisely because of the prevailing ambiguity.

Fait Accompli

Historically, the term *fait accompli* has been used to describe an initiative that forces the opponent or defender to initiate some actions in response to the aggressor's initiative (Young 2015, 338). *Fait accompli* strategies involve the tactics to mount a sudden, decisive blow to a defender, forcing the defender into the dilemma of whether or not to concede or pursue a dangerous escalation (Mazarr 2015, 36–37). *Fait accompli* strategies strive for smaller objectives over which the defender will not choose to escalate. A sudden invasion of a country to occupy a large piece of land before anybody can respond is a classic manifestation. A smart aggressor may employ a set of small *fait accompli* to gain broader objectives gradually because individually such tactics will not yield to *casus belli* (just cause for going to war). Little green men or intermediaries play a decisive role in presenting the *fait accompli* to the defender. *Fait accompli* is regarded as the riskiest strategy in gray zone warfare because it brings a sudden change in the *status quo*. As Wirtz (2017, 108) argues, "by forcing the onus of escalation onto the power seeking to preserve the status quo, it places that power in a strategically inferior position." The major power trying to preserve the *status quo*, for instance, may not respond to the *fait accompli* presented by the revisionist power as it could shift the burden of responsibility onto the major power.

Salami Tactics

Actions aimed to exploit ambiguities in deterrence conditions are frequently denoted as salami tactics. Wirtz (2017, 109) argues that "unlike the prompt destruction of the opponent's deterrent strategy created by the fait accompli, salami tactics involve the slow-motion erosion of an opponent's deterrent by gradually making it irrelevant in an unfolding situation." The aggressor or party trying to change the *status quo* employs strategies that remain below the red lines and do not trigger a deterrent response by the defender (or the party trying to maintain the *status quo*). The *status quo* changes gradually through salami tactics because the defender lacks the military and political justification to respond to incidents of a minor nature. However, salami tactics have associated risks in defining the red lines beyond which a deterrent response by the defender would likely be triggered. An aggressor may underestimate the response or a proactive defender may respond even at lower thresholds to preserve the *status quo*. The classic example of the failure of salami tactics is the incident where the Turkish Air Force shot down a Russian fighter jet in 2015 for violating Turkish airspace after ten warnings to change course over the course of five minutes: the Russians considered it below the threshold while Turkish authorities gave repeated warnings and finally acted upon the situation to preserve the *status quo* (Nissenbaum, Peker and Marson 2015).

Proxy Warfare and the Use of Criminal Organizations and Networks

Proxy warfare is also a principal instrument of gray zone warfare which helps to change the *status quo* while staying ambiguous. The aggressors (state actors and NSAs) exploit the existing political, economic, and ethnic fault lines of society by supporting the elements that share similar interests (Wirtz 2017, 109). Proxy warfare creates ambiguity around the sources and objectives of the change which, in turn, dents the deterrence mechanisms of the defender. A proxy also complicates deterrence strategies because the defender needs to revise their own deterrence mechanisms against ambiguous actors and the unknown forces who initiated the change in the *status quo.* Gray zone aggressors may also employ criminal organizations and networks to accomplish a wide range of objectives: to shape public opinion, to create ambiguity, and for the provision of food and weapons supplies through smuggling mafias (Chambers 2016, 20). Criminal groups can also help rapid destabilization by conducting various activities such as target killings, mass shootings, and looting. Gray zone aggressors may also hire such organizations and networks to “supply proxies, disrupt adversary operations, distract adversary police forces, and intimidate or coerce target populations” (Chambers 2016, 20). Criminal networks offer a unique advantage because of their understanding of the local system and their ability to identify and exploit the loopholes in the system.

Cyber Warfare

Cyberspace is another critical enabler of gray zone warfare that aims to intensify the fog and uncertainty by inducing confusion and interrupting essential services. Cyberspace provides numerous opportunities for the disruption of both state actors and NSAs, especially for revisionist actors. Various actors use cyberspace to link or hire like-minded people, brainwash believers, activate dispersed resistance, and fight without any limitations of time and space (Freier et al. 2016, 21). Cyber warfare is a vital choice of actors operating in the gray zone because it offers the advantage of non-attribution and conceals actions in the fog of confusion. Russia employed cyber warfare against Estonia in 2007 by adopting the denial of services strategy due to tensions between both countries. The fact that

Estonia is a member of NATO and can invoke Article 5 of its charter in case of an armed attack deterred Russia from overt use of force. Russia thus resorted to gray zone warfare which helped achieve its objectives while ensuring deniability through ambiguity.

Cyber warfare is, and will remain, an effective instrument of gray zone warfare in the foreseeable future (Fitton 2016, 110). In contemporary times, cyber operations have been employed for a diverse range of activities, including shutting down nuclear facilities through computer viruses and spying on governments through various means (Rid 2012, 13). The idiom "on the internet no one knows you are a dog" clearly fits in the cyber warfare scenarios where a diverse range of gray zone actors want to achieve strategic goals without reaching the conflict threshold to avoid triggering Article 5 of the NATO charter (Fitton 2016, 114). The employment of cyber warfare may never kill an individual directly, but there is a possibility that cyber-attacks on industrial or communal infrastructure may lead to deaths in future.

Information Operations

Ronfeldt and others (1999) noted two decades ago that information is not just a force multiplier; it is a force modifier. It is argued that gray zone warfare is "frequently shrouded in misinformation and deception, and [is] often conducted in ways that are meant to make proper attribution of the responsible party difficult to nail down" (The Economist 2018). Information operations are, therefore, and unsurprisingly, a significant element of gray zone warfare, and contemporary conflicts are frequently waged in the information domain (Chekinov and Bogdanov 2013). Many types of information operations are employed by states and NSAs to modify the behavior of contending, friendly, and neutral target entities. Information operations are people-centric, aiming to influence people through various strategies, and are employed to build narratives that are favorable to accomplish one's own goals. The internet and social media play a crucial role in the dissemination of propaganda and misinformation. Information dominance or denial applies leverage to an aggressor by inducing delay and uncertainty in the defender's political and military decision-making process. Although propaganda and misinformation are centuries-old techniques, technological revolutions have increased the speed and the implications in manifold ways. Information is the primary raw material of the evolving international society of modern times (Ehrhart 2017, 264). The information revolution has empowered states and NSAs to embark on local and transnational operations to modify essential elements of the *status quo*. The internet and social media provide such vast amounts of information and misinformation that it becomes impossible for individuals to absorb (or indeed identify) all the information needed to draw unbiased conclusions. Recent issues concerning misinformation and conspiracies regarding COVID-19 can be understood as representative in this respect. Both China and the United States, for instance, struggled to dominate the information landscape by blaming each other for the outbreak of the novel coronavirus in 2020.

Gray Zone and Hybrid Warfare

Competing ideas, perspectives, and expressions are used by various scholars to explain the phrases "gray zone warfare" and "hybrid warfare." One common misperception is that these two terms are different names for the same concept—which is not the case. These terms cannot be used interchangeably (Fitton 2016, 111) without loss. The main difference between them concerns the use of kinetic means, which are limited to hybrid warfare, whereas gray zone warfare is limited to non-kinetic means. The invasion of Ukraine by Russia in 2014 can nevertheless be used to challenge this kind of separation because both kinetic and non-kinetic means were employed during the conflict even though this conflict has been termed as a gray zone conflict. However, this practical example should perhaps be taken to indicate that both kinds of warfare can be used together under certain circumstances, or for certain objectives, rather than as a sign that the two are synonymous or fully interchangeable concepts.

The next significant difference concerns the classification based on the actors involved in the conflict. A few academics and practitioners argue that only states can employ gray zone warfare while both state actors and NSAs can employ hybrid warfare. This kind of view does not stand up to scrutiny well because a diverse range of actors can employ both types of warfare and any classification based on such assumptions may make the concepts (and practices) more ambiguous. State actors frequently employ NSAs (proxies) while operating in the gray zone for managing ambiguity and denying attribution—the fundamental tenets of gray zone warfare.

Chambers (2016, 43) argues that "hybrid threats and the gray zone are issues that have existed in warfare for centuries. However, their recent emergence in the discussion of conflict; among strategists, scholars, and policy makers highlights their renewed importance." Interestingly, there is slight or no consensus at all among the military, academics, policy makers, and strategists as to what constitutes "gray zone warfare" or "hybrid warfare" or how to define these phrases. Arquilla (2018) concludes that hybrid warfare is a more broad and all-encompassing term for modern warfare, while the concept of gray zone warfare is complicated and does not cover such a wide range of contemporary conflicts. The conflicts that pose a threat to the United States-led world order can be best described as gray zone conflicts in this view. For example, the Tamil Tigers insurgency in Sri Lanka cannot be described as a gray zone conflict because it was not a threat to the United States-led world order (Matisek 2017, 5). This definition lacks plausibility, though, as many other countries face similar threats, and the gray zone concerns changing the *status quo*—which is not limited to the international order. It can, of course, refer to the *status quo* prevailing between two countries over disputed territory.

Mazarr (2015, 46–47) notes that hybrid warfare employs many military tools that make hybrid conflicts more violent in comparison to gray zone conflicts (which are less violent and fit into a broader form of conflict). This argument attracts attention because it falls in line with the fundamental principle of gray zone warfare which implies not crossing the red lines to avoid escalation to violent conflict. Actors employing hybrid warfare aim to exploit the existing vulnerabilities of a defender by attacking the integration flaws in policy, organization, and doctrine. By contrast, actors using gray zone warfare aim to achieve strategic objectives by employing various information operations and other short-of-war tactics without crossing the established threshold of an open war (Chambers 2016, 9–13). This article contends that hybrid warfare and gray zone warfare are distinct forms of warfare with only a few important commonalities. Therefore, these two terminologies should not be used interchangeably to avoid confusion and encourage greater precision and deeper understanding.

Critique of Gray Zone Warfare

Gray zone warfare may appear to be simple at first glance, but by now the discussion should reveal that it is complicated and full of contrasting themes. The concept of gray zone warfare has been stretched to limits beyond the breaking point (Brands 2016) because proponents of the concept have amalgamated a varied range of ideas and used it as an umbrella term for modern conflicts. This critique is valid to a reasonable extent because gray zone warfare is used to explain many modern conflicts that differ greatly in characteristics. Many other terms such as hybrid warfare, unrestricted warfare, ambiguous warfare, and new generation warfare are also extensively used to explain contemporary conflicts. Pomerantsev (2015) labels the Russian actions in Ukraine in 2014, the Chinese involvement in the South China Sea, and some actions of the Islamic State and Boko Haram under the same category of gray zone warfare. Nevertheless, the Russian actions in Ukraine are in stark contrast to Chinese actions in the South China Sea. Also, the Islamic State's violent strategies in the Middle East lie on the other end of the spectrum in comparison to Chinese gray zone strategies in the South China Sea. Labeling everything short of conventional war, or that which lies between peace and war, as gray zone warfare may therefore undermine the analytical usage of the concept.

In the final part of his article, Arquilla (2018) argues that gray zone warfare is an intellectual construct that confuses instead of clarifying. Critics also question the validity of the idea that gray zone warfare is a novel concept by claiming that there is nothing new about the concept and people have been using such strategies for a long time (Arquilla 2018, 121; Brands 2016, 4). While gray zone tactics may indeed be centuries old, innovation and developments in technology have certainly helped gray zone actors to improvise and attack in novel ways in the contemporary era. We contend that gray zone strategies may be helpful for short- and medium-term objectives but may be problematic for pursuing long-term objectives. While Mazarr (2015) notes that gray zone warfare is gradualist—the desired results are achieved over a long period of time by incremental efforts—maintaining ambiguity for a long time may be problematic. From the above discussion, we find significant reasons to maintain that gray zone warfare is a distinct concept and that the term should not be used interchangeably with hybrid warfare without an important loss of nuance. Now we turn to a brief discussion of how gray zone warfare has been employed in differing scenarios, with the aim to further the conceptual understanding developed so far.

Examples of Gray Zone Warfare

Freier and others (2016, 19–20) argue that three types of powers exist in the world: *status quo* (actors who value the current order and actively work to secure it), revisionist (actors who value a rule-based order but not necessarily in its current form and who resist the U.S.-led *status quo*), and rejectionist (actors who discard the existing international order altogether). The United States and its allies are examples of *status quo* powers, while Russia, China, and Iran are examples of revisionist powers. On this view, the United States considers Russia, China, and Iran as revisionist states that employ gray zone warfare in various domains to challenge the U.S.-led world order. These states employ various instruments, such as influence and intimidation, to achieve war-like objectives while using means and methods that fall short of a full-scale, open war (Pierce, Douds, and Marra 2015, 52). These countries use strategies that remain below the threshold of the U.S. red lines to avoid triggering a decisive response or provocation. The following section highlights several contemporary gray zone strategies adopted by Russia, China, Iran, India, and Pakistan to deepen our understanding of how various instruments of gray zone warfare are employed in practice.

Russian Actions in Ukraine

The Russian invasion of Ukraine in 2014 is considered a classical manifestation of gray zone warfare by most leading Western scholars, military thinkers, and analysts (Hoffman 2016, 26–27). Russia aimed to conceal the attribution of its actions in Ukraine to create a response dilemma for the West. Hoffman (2016, 27) claims that "the war in eastern Ukraine is not just a proxy war; it is a combination of advanced military assets with irregular forces, propaganda, and coercion of the civilian population." Hoffman's arguments underscore that Russia employed a diverse range of gray zone strategies in Ukraine in 2014 to achieve its strategic objectives. Indeed, the concept of "little green men" emerged from the Russian engagements in Ukraine. Russian employment of "little green men" offered two distinct advantages; first, Russia was able to internationally deny that it had no linkage with the events in Ukraine. Second, it gave a strategic advantage to Russia as there was massive confusion on the ground about who was commanding and controlling the masked and unaffiliated soldiers. Ukraine was in a state of the classic response dilemma as Russia was able to maintain ambiguity regarding attribution. The government in Kyiv and the Ukrainian population were unable to ascertain with a reasonable degree of certainty the identity(ies) of enemy forces and who was supporting those forces until it was too late (Chambers 2016, 19; Najzer 2018, 172).

Information Operations emerged as the second most significant facet of the 2014 Russian invasion of Ukraine. Scholars, analysts, and practitioners around the world extensively focused on Russian information operations. Control or influence over information plays an imperative role in gray zone warfare. In this case, Russia proved a smart actor in gray zone warfare and intelligently employed the media before and after its 2014 operations while Ukraine and its Western allies were caught off guard and were unable to respond effectively. The media played a significant role in stirring up discomfort among local populations in the West; this put much pressure on governments which further undermined the response strategy (Giles 2016, 31–32). In the end, the United States and its Western allies were only able to condemn Russia for spreading misinformation and manipulating facts. Russia's use of its UN veto saved it from any strict sanctions as the United States and the EU were able to impose only a few economic sanctions which proved to be insignificant. It is argued that the information operations were successful due to the advanced planning of Russia to use such operations (Najzer 2018, 173). There is evidence that Russia also employed criminal networks in Ukraine as a part of its gray zone strategies (Chambers 2016, 14). Russia blended various instruments of national power and adopted gray zone warfare to attain its strategic goal of annexing Crimea by destabilizing Ukraine. The Russian calculation of the thresholds was highly successful as they did not cross a red line that could have triggered a response by global powers, especially NATO.

Chinese Actions in the South China Sea

China likewise pursues its objectives via gray zone warfare to avoid escalation to full-scale wars—its assertive behavior in the South China Sea is a glaring example of how gray zone warfare is used to challenge the *status quo*. It relies heavily on military and paramilitary intimidation and the non-violent employment of military force (Freier et al. 2016, 37) and pursues its objectives in the gray zone by mixing political, military, and commercial instruments. Strategies such as forceful commercial expansion, non-violent coercion through armed forces, the threatening use of law enforcement and maritime paramilitary, and employment of cyber warfare and information operations (Thayer 2011, 33) are common. As a part of its gray zone tactics, China employs fishers in the South China Sea to claim the disputed areas and also to disrupt U.S. naval presence (Kazianis 2014).

Jackson (2017, 43–44) argues that "China's coast guard or its maritime militia—the latter is affiliated with the central government but is not a war-making instrument of the state—may engage in confrontational actions in the East or the South China Sea." The use of civilian agencies for maintaining military-like control offers the advantage of deniability of military action in the region. Chinese actions in the South China Sea can be regarded as *fait accompli* because these actions helped China to claim those areas without triggering any response from the United States or regional competitors. China also conducts numerous aggressive activities in the cyber domain of the gray zone and Chinese hackers interfere in numerous dominions ranging from spying to the stealing of intellectual properties across the world. In 2020, the United States raised alarms regarding Chinese hackers' attempts to steal research data regarding the COVID-19 vaccine (Corera 2020).

Iranian Actions

Iran is a revisionist state—one of the main preconditions of a gray zone actor—that wants to change the *status quo* and reject the U.S.-led world. It employs a diverse range of gray zone strategies, including subversion and proxy warfare, to undermine the existing international order and shift the balance of power in the Middle Eastern region. As Arquilla (2018, 119) reminds us, "The Islamist regime in Tehran oversees an arc of strategic involvement in wars ranging from Syria to the southern Arabian Peninsula; supports the vibrant, violent Hezbollah organization; and cultivates covert nodes, cells, and networks throughout the world." Iran uses multiple instruments of gray zone warfare on multiple fronts which is alarming for the United States as these actions undermine the U.S. stakes in the Gulf region. Ground realities reveal that Iran is proactively involved in many regional conflicts and supports many proxies while propagating the policy of denial at the international level.

Gray Zone Warfare in South Asia

The South Asian region has witnessed a wide range of multiple conflicts involving many actors and factors. The enduring rivalry between India and Pakistan is a key example where both states engage in different kinds of warfare strategies from sabotage to full-scale conventional wars with nuclear overhang. Bratton (2020, 41) notes that India and Pakistan regularly use coercive measures in the gray zone to achieve their objectives while trying to avoid the chances of escalation. Under the shadow of nuclear deterrence, their territorial disputes attract the application of gray zone strategies on both sides. Each has endeavored to avoid crossing red lines and both pursue their national interests through various instruments of gray zone warfare such as terrorist attacks, the use of spies, proxies, and *fait accompli*, which are not easily attributable due to ambiguity. Bratton (2020, 43) contends that "these are countries that have engaged in cross border shelling and minor raids and accuse the other of aiding insurgent and terrorist groups to attack the other, all the while under the threat of nuclear war."

Evidently, gray zone warfare is attractive for Pakistan because the military capacity of India is quantitatively and qualitatively superior. Pakistan desires to change the *status quo* of the disputed region of Jammu and Kashmir, which may not be possible without the application of gray zone tactics. India employs gray zone warfare to maintain superiority in the region and to pursue its strategic objective of rising as a global power, applying proxies and *fait accompli* against smaller states—Pakistan, Sri Lanka, Afghanistan, Nepal, and Bangladesh. Indian policymakers consider Pakistan the epicenter of terrorism and the so-called Indian "surgical strikes" against terrorists inside Pakistan are likewise regarded as an instrument of gray zone warfare because the red lines leading to almost certain escalation are not crossed. However, interestingly this assumption of red lines proved faulty when India conducted surgical strikes after the Pulwama attack in 2019, and Pakistan responded forcefully. Both states teetered on the brink of a nuclear war, indicating a failure of the prevailing deterrence mechanisms. The India–Pakistan case is a genuine demonstration of gray zone warfare, but calculations of where exactly the red lines lie, as well as accurately calculating potential responses, are risky.

Countering Gray Zone Threats

Countering gray zone threats is a daunting task for any state. The lack of comprehension and authenticated information of a gray zone aggressor's intent makes it challenging to detect, characterize, and counter the gray zone threats. Chambers (2016, 4) argues that "describing the current state of warfare is not just important to academic and military strategists, it is also essential to helping policy makers and civilian leaders understand the changing nature of warfare." It is critical to note that no two antagonists and no two conflicts can be regarded as similar. Russian gray zone tactics against a Baltic state will vary to a great extent from the tactics employed by China in the South China Sea. Similarly, the tactics employed by China in the South China Sea are in stark contrast to those employed by Hezbollah against Israel or by the Islamic State against many states. The tactics and techniques employed in each conflict consider various dynamics to match the circumstances on the ground. There cannot be a single strategy to counter gray zone warfare, so the defender needs to adapt according to the prevailing situation. As Chambers (2016, 15) notes, paraphrasing James Dubik's words, "We need to fight the war we have got, not the one we want." Countering gray zone conflicts involves a continuous struggle as the defender needs to adjust strategies as per the changing dynamics of the conflict.

Robert O. Work, former U.S. Deputy Secretary of Defence, stated that the gray zone is composed of agents, deception, infiltration, paramilitaries, and persistent denial and the United States is least prepared to counter this type of warfare (cited in Jackson 2017, 40). This admission is alarming. If the most advanced nation in the world is not prepared to counter gray zone threats, then questions arise concerning how developing states can mitigate such threats. Freier et al. (2016, 13) write in their report that, "whether emerging via purpose or implication, gray zone challenges increasingly exact warlike consequences on the United States and its partners." If this is so, a better, more nuanced understanding of gray zone warfare is most definitely needed alongside a range of adequate countermeasures. While the latter are inherently difficult to compile, due to the varied contexts and diverse strategies of this kind of warfare, some innovations have recently been considered.

The fundamental requirement for countering gray zone warfare is to identify and understand the nature of conflicts. The examples discussed briefly above highlight this. In the case of Ukraine in 2014, it was too late when the government in Kyiv and its Western allies were able to identify the actual adversary. To understand the dynamics of a gray zone conflict, the defender needs to deconstruct the ambiguity created by the aggressor, potentially enabling the defender to identify the actors involved. Defining the thresholds is one of the riskiest and most complicated tasks in gray zone warfare because a slight miscalculation may lead to a catastrophe. The threshold is arbitrarily established and heavily relies on the situational context and prevailing geo-strategic environment (Chambers 2016, 12). The defender must define and change the thresholds smartly, and nothing can be neglected on the pretext of insignificance.

Recently, several strategies, doctrines, programs, and software have been developed to counter gray zone threats. The U.S. Army and Marine Corps developed a joint operational strategy to counter the emerging gray zone threats through multi-domain battles. The central idea is based on the assumption that future aggressors are likely to confront the United States in multiple domains which necessitate joint force planning to counter 21st-century conflicts (Hayes 2018, 60). Senior military leaders from the Army and Marine Corps agree upon the augmented role of Special Forces operations in evolving conflicts. The Strategic Technology Office of Defense Advanced Research Projects Agency (DARPA) has also launched a computer software-based program Collection and Monitoring via Planning for Active Situational Scenarios (COMPASS), which aims to assist in better realizing and countering an adversary's gray-zone strategies (Staff Writers 2018). This program utilizes artificial intelligence, simulations, computer modeling, and game theory to assess a gray zone scenario and extrapolate the potential outcomes of its own projected actions and the adversary's probable reactions.

Conclusion

Contemporary conflicts are neither black nor white. Rather, many of them stand in the middle: the gray zone—the domain where the distinction between war and peace becomes impossible to see clearly due to the ambiguity of the tactics employed. In this article, we reviewed and unpacked a diverse range of definitions that, taken together, identify the major playing fields of gray zone warfare in the informational, economic, military, and political domains. By extension, staying below the threshold of conventional war is the fundamental principle of gray zone warfare. Strategies and tactics such as cyber warfare, proxy wars, salami tactics, information operations, and *fait accompli* are extensively employed by actors resorting to gray zone warfare and can be employed by state actors as well as NSAs to create ambiguity about the conflict, the parties involved, who is responsible, and what their real intentions are. Revisionist states generally employ gray zone tactics to alter the *status quo* or challenge the existing U.S.-led international world order. We discussed briefly several examples that illustrate the wide and diverse range of strategies and conflicts that can comprise gray zone warfare. These include Russia's actions in Ukraine in 2014 and the annexation of Crimea, China's assertive attitude in the South China Sea, and Iran's covert involvement in various regional conflicts through proxies. Before invading Ukraine militarily in February 2022, Russia employed both hybrid and gray zone warfare tactics primarily in those Ukrainian regions where Russia believed it had support. India and Pakistan also continue to use gray zone strategies to pursue their respective interests. There is no unique recipe for countering gray zone strategies, although a comprehensive understanding and an integrated response appear to be necessary prerequisites. Undoubtedly, the concept of gray zone warfare is wrapped in a controversy that provides space to conduct significantly more research in this emerging area.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

About the Authors

Tahir Mahmood Azad is a Visiting Research Fellow at the Centre for Science and Security Studies (CSSS) in the Department of War Studies at King's College London and joined the CSSS in 2019. Previously, Azad held fellowships at the Sandia National Laboratories, New Mexico, United States; the SPAIS/Global Insecurities Centre, University of Bristol; the Center for International Trade & Security (CITS), University of Georgia, United States; Centre on Conflict, Development, and Peacebuilding (CCDP), Graduate Institute Geneva, Switzerland; the Institute for Security and Development Policy (ISDP) Stockholm, Sweden, and the Peace Research Institute Frankfurt (PRIF), Germany.

Muhammad Waqas Haider holds an MA in Conflict Resolution and Peace Studies from the University of Lancaster, United Kingdom as a Chevening Scholar. He has special interests in the changing nature of warfare, contemporary issues of peace and conflict, and deterrence. He explored Hybrid Warfare in his MPhil Thesis at the National Defence University, Islamabad, Pakistan, and conducted research on Gray Zone Warfare and deterrence at the University of Lancaster.

Muhammad Sadiq is a Visiting Research Fellow at the Centre for Science and Security Studies (CSSS) in the Department of War Studies at King's College London and joined CSSS in 2021. Sadiq holds a PhD from the School of Politics and International Relations (SPIR), Quaid-i-Azam University (QAU) Islamabad, Pakistan. Sadiq received his MSc and MPhil from the Department of Defence and Strategic Studies (DSS), QAU Islamabad, Pakistan, and is associated with the DSS Department at QAU as a faculty member since 2007.

ORCID iDs

Tahir Mahmood Azad https://orcid.org/0000-0003-3826-2009
Muhammad Waqas Haider https://orcid.org/0000-0001-7076-168X

References

Ahluwalia, Poshuk. 2019. "Gray Zone Conflicts and Informationisation in the Indian Context: Challenges, Capabilities and Way Ahead." https://www.claws.in/publication/gray-zone-conflicts-and-informationisation-in-the-indian-context-challenges-capabilities-and-way-ahead/ (accessed April 30, 2022).

Arquilla, John. 2018. "Perils of the Gray Zone." *Prism* 7 (3): 118–129. https://cco.ndu.edu/News/Article/1507653/perils-of-the-gray-zone-paradigms-lost-paradoxes-regained/ (accessed April 30, 2022).

August, Mark B. 2016. "The Red Zone: Russian Conflict Management in the Gray Zone." 10140836 M.S., San Diego State University. https://digitallibrary.sdsu.edu/islandora/object/sdsu%3A1611 (accessed April 30, 2022).

Bensahel, Nora. 2017. "Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex." Foreign Policy Research Institute. https://www.fpri.org/article/2017/02/darker-shades-gray-gray-zone-conflicts-will-become-frequent-complex/ (accessed April 30, 2022).

Brands, Hal. 2016. "Paradoxes of the Gray Zone." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2737593 (accessed April 30, 2022).

Bratton, Patrick C. 2020. "The Not So Gray Zone in South Asia." *Comparative Strategy* 39 (1): 41–61. https://doi.org/10.1080/01495933.2020.1702346.

Chambers, John. 2016. *Countering Gray-Zone Hybrid Threats: An Analysis of Russia's New Generation Warfare and Implications for the US Army.* US Military Academy-Modern War Institute West Point. https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf (accessed April 30, 2022).

Chekinov, Sergey G., and Sergey A. Bogdanov. 2013. "The Nature and Content of a New-Generation War." *Military Thought* 4: 12–23.

Corera, Gordon. 2020. "Coronavirus: US Accuses China of Hacking Coronavirus Research." *BBC News,* May 14. https://www.bbc.com/news/world-us-canada-52656656 (accessed April 30. 2022).

The Economist. 2018. "Shades of Gray; Hybrid Warfare." The Economist, January 27.

Ehrhart, Hans-Georg. 2017. "Postmodern Warfare and the Blurred Boundaries between War and Peace." *Defense & Security Analysis* 33 (3): 263–275. https://doi.org/10.1080/14751798.2017.1351156.

Fitton, Oliver. 2016. "Cyber Operations and Gray Zones: Challenges for NATO." *Connections* 15 (2): 109–119. https://www.jstor.org/stable/26326443 (accessed April 30, 2022).

Freier, Nathan, Charles R. Burnett, William CainJr., Christopher D. Compton, Sean M. Hankard, Robert S. Hume, Gary KramlichII, J. Matthew Lissner, Tobin A. Magsig, and Daniel E. Mouton. 2016. *Outplayed: Regaining Strategic Initiative in the Gray Zone.* Army War College Carlisle Barracks, PA, United States.

Giles, Keir. 2016. "Russia's 'New' Tools for Confronting the West." *Chatam House,* March 21. https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power (accessed April 30, 2022).

Hayat, Zubair M. 2018. "Inaugural Address." Compound (Hybrid and Gray Zone) Threats to Pakistan, Islamabad.

Hayes, James E.III. 2018. "Beyond the Gray Zone: Special Operations in Multidomain Battle." *Joint Force Quarterly* 91 (4): 60–66. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-91/jfq-91_60-66_Hayes.pdf?ver=2018-11-06-094122-477 (accessed April 30, 2022).

Hoffman, Frank G. 2016. "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War." *The Heritage Foundation,* 25–36. https://www.heritage.org/sites/default/files/2019-10/2016_IndexOfUSMilitaryStrength_The%20Contemporary%20Spectrum%20of%20Conflict_Protracted%20Gray%20Zone%20Ambiguous%20and%20Hybrid%20Modes%20of%20War.pdf (accessed April 30, 2022).

Howard, Michael, and Peter Paret. 1976. *On War,* Vol. 117. Princeton, NJ: Princeton University Press.

Jackson, Van. 2017. "Tactics of Strategic Competition: Gray Zones, Redlines, And Conflicts Before War." *Naval War College Review* 70 (3): 39–62. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1069&context=nwc-review (accessed April 30, 2022).

Jackson, Nicole. 2019. "Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO." *Journal of Military and Strategic Studies* 19 (4): 104–125. https://jmss.org/article/view/68870 (accessed April 30, 2022).

The Joint Staff. 2013. Joint Publication 1, Doctrine for the Armed Forces of the United States. edited by Department of Defense.

Kazianis, Harry J. 2014. "China's 50,000 Secret Weapons in the South China Sea." *The National Interest*, July 30. https://nationalinterest.org/feature/china%E2%80%99s-50000-secret-weapons-the-south-china-sea-10973 (accessed April 30, 2022).

Matisek, Jahara W. 2017. "Shades of Gray Deterrence: Issues of Fighting in the Gray Zone." *Journal of Strategic Security* 10 (3): 1–26. www.jstor.org/stable/26466832 (accessed April 30, 2022).

Mazarr, Michael J. 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* U.S. Army War College, Carlisle.

Najzer, Brin. 2018. "Clarifying Hybrid Warfare: Investigation and Elucidation of the Phenomenon of Low-Level Coercion and Conflict in the Gray Zone." Unpublished Doctoral Dissertation, Department of International Relations, University of Aberdeen.

Nissenbaum, Dion, Emre Peker, and James Marson. 2015. "Turkey Shoots Down Russian Military Jet." *The Wall Street Journal*, November 24. https://www.wsj.com/articles/turkey-shoots-down-jet-near-syria-border-1448356509 (accessed April 30, 2022).

Pierce, William G., Douglas G. Douds, and Michael A. Marra. 2015. "Understanding Coercive Gradualism." *Parameters* 45 (3): 51–61. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2742&context=parameters (accessed April 30, 2022).

Pomerantsev, P. 2015. Fighting While Friending: The Gray War Advantage of ISIS, Russia, and China.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Roberts, Brad. 2015. *The Case for US Nuclear Weapons in the 21st Century.* Stanford, CA: Stanford University Press.

Ronfeldt, David, John Arquilla, Graham Fuller, and Melissa Fuller. 1999. *The Zapatista "Social Netwar" in Mexico.* Santa Monica, CA: Rand Corporation. https://www.rand.org/pubs/monograph_reports/MR994.html (accessed April 30, 2022).

Staff Writers. 2018. "Making Gray-Zone Activity More Black and White." *DARPA*, March 14. https://www.darpa.mil/news-events/2018-03-14 (accessed April 30, 2022).

Thayer, Carlyle A. 2011. "China's New Wave Of Aggressive Assertiveness in the South China Sea." *International Journal of China Studies* 2 (3): 555–583. https://www.files.ethz.ch/isn/130696/Thayer%20CSIS%20South%20China%20Sea.pdf (accessed April 30, 2022).

Votel, Joseph L., Charles T. Cleveland, Charles T. Connett, and Will Irwin. 2016. "Unconventional Warfare in the Gray Zone." *Joint Forces Quarterly* 80 (1): 101–109. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/article/643108/unconventional-warfare-in-the-gray-zone/ (accessed April 30, 2022).

Wirtz, James J. 2017. "Life in the 'Gray Zone': Observations for Contemporary Strategists." *Defense & Security Analysis* 33 (2): 106–114. https://doi.org/10.1080/14751798.2017.1310702.

Young, Oran R. 2015. *Politics of Force: Bargaining during International Crises.* New Haven, CT: Princeton University Press.