REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* **05-05-2019**	2. REPORT TYPE **FINAL**	3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

DETERRING MARITIME GRAY ZONE AGGRESSION ETHICALLY WITH EMERGING TECHNOLOGIES

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ BERTRAM CHUN HOU ANG

Paper Advisor (if Any): **DR JAMES KRASKA**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Ethics and Emerging Military Technologies
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Ethics and Emerging Military Technologies Graduate Certificate Program. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College, the Department of the Navy or the Republic of Singapore Navy.

14. ABSTRACT

Gray zone strategies have become more widespread in the maritime domain as states see an opportunity to advance their interests while staying below the threshold of a conventional military response. By exploiting the ambiguity, asymmetry, and incrementalism that characterize gray zone activities, gray zone coercers are able to bypass traditional deterrence measures and effect substantial strategic change over time at minimal cost. In particular, gray zone provocateurs are able to capitalize on the fear of escalation to engender paralysis and negate effective responses to their coercive activities. Emerging technologies can be harnessed to strengthen deterrence by denial measures against maritime gray zone aggression by imposing significant expected costs at the point of aggression, thereby shifting the burden of escalation back to the aggressor. However, defenders must leverage these technologies while adhering to normative ethical and legal principles. Only then can they avoid undermining international laws and norms underpinning the rules-based order, which would prove counterproductive for their legitimacy in the long term.

15. SUBJECT TERMS
GRAY ZONE WARFARE, NON-LETHAL TECHNOLOGIES, DRONES, ARTIFICIAL INTELLIGENCE, DETERRENCE

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON **DR THOMAS CREELY**
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED		44	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

DETERRING MARITIME GRAY ZONE AGGRESSION ETHICALLY WITH EMERGING TECHNOLOGIES

by

Bertram Chun Hou Ang

MAJ, Republic of Singapore Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Ethics and Emerging Military Technologies Graduate Certificate Program.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Republic of Singapore Navy, the Naval War College or the United States Department of the Navy.

Signature: _______________

05 MAY 2019

ABSTRACT

Gray zone strategies have become more widespread in the maritime domain as states see an opportunity to advance their interests while staying below the threshold of a conventional military response. By exploiting the ambiguity, asymmetry, and incrementalism that characterize gray zone activities, gray zone coercers are able to bypass traditional deterrence measures and effect substantial strategic change over time at minimal cost. In particular, gray zone provocateurs are able to capitalize on the fear of escalation to engender paralysis and negate effective responses to their coercive activities. Emerging technologies can be harnessed to strengthen deterrence by denial measures against maritime gray zone aggression by imposing significant expected costs at the point of aggression, thereby shifting the burden of escalation back to the aggressor. However, defenders must leverage these technologies while adhering to normative ethical and legal principles. Only then can they avoid undermining international laws and norms underpinning the rules-based order, which would prove counterproductive for their legitimacy in the long term.

Table of Contents

ACKNOWLEDGEMENTS

I would like to thank Dr. James Kraska for graciously agreeing to be my thesis supervisor, and for sharing his legal expertise and insights throughout the entire writing process. I am also grateful to Dr. Tim Schultz and Dr. Tom Creely for their guidance and wisdom throughout the entire Ethics and Emerging Military Technologies graduate certificate program, and for their willingness to open up such a great opportunity to international students at the Naval War College. It has truly been my honor and privilege to participate in this rewarding program. I would also like to express my thanks to Ms. Isabel Lopes for her commitment to the program and to every individual in it – her expertise and encouragement were truly invaluable to the writing process. Last but certainly not least, I would like to thank my wife Li Sha for her ceaseless love and support for me throughout our time in Newport.

Soli Deo Gloria.

I. INTRODUCTION

Much ink has been spilled in writing about the growing prevalence of gray zone coercion in modern statecraft, which is illustrated by recent Russian actions in the Crimea and Chinese behavior in the South China Sea. Gray zone activities have become more ubiquitous in the maritime domain as countries see an opportunity to make significant strategic gains at sea while minimizing potential losses in blood, treasure, and reputation. States defending against gray zone aggressors have thus far struggled with responding to the latter's subtle, yet obviously antagonistic approach, often becoming paralyzed into inaction for fear of unwanted escalation.

Operating below the threshold of conventional conflict is not new. Indeed, the concept of achieving strategic gains without having to expend conventional military force has early origins. Subduing the enemy without fighting was after all declared as the pinnacle of skill by the renowned Chinese strategist Sun Tzu as early as 500 B.C.[1] In the intervening period since, gray zone methods have been acknowledged as "political warfare," "covert operations," and "active measures."[2] Notwithstanding its archaic origins, the study of gray zone coercion remains pertinent and is indeed even more relevant today. The use of such stratagems by states will likely grow as a tried and tested means of achieving strategic gains in an international order that shuns the exercise of overt violence. As a Center for Strategic and International Studies (CSIS) report observes, would-be gray zone coercers exploit the gray zone characteristics of ambiguity, asymmetry, and incrementalism to minimize the costs of attaining their revisionist objectives.[3]

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 77.
[2] U.S. Department of State, *Report on Gray Zone Conflict*, ISAB Study (3 January 2017), 1. https://www.state.gov/t/avc/isab/266650.htm.
[3] Michael Green et al, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (Washington DC: Center for Strategic & International Studies, 2017), 29-34.

Moreover, the employment of new technologies has also increased the efficacy of such means below the threshold of war.[4] As gray zone campaigns become increasingly prevalent and dangerous, states seeking to defend their maritime interests and uphold the laws and norms underpinning the international rules-based order must expand their capacity to respond.

Scholars have sought to address the gray zone conundrum by offering various counter-strategies. Michael Green and his colleagues at CSIS have identified key lessons for the U.S. and its partners in countering gray zone aggression. They argue that the U.S. and its partners must tailor their deterrence approaches to the type of gray zone challenge they face, clarify commitments to existing alliances, and increase their risk tolerance for escalation.[5] Specific to Chinese actions in the South China Sea, the scholars Hal Brands and Zack Cooper conclude that the U.S. needs to implement containment or offset strategies in response to China's gray zone offensive. Here, Brands and Cooper contend that the U.S. should seek to contain the most egregious Chinese activities while offsetting less aggressive behavior by imposing long-term costs on China in other domains.[6] In addition, naval experts James Holmes and Toshi Yoshihara maintain that the U.S. must sustain a long-term posture of vigilance, reduce ambiguity by underscoring its non-neutrality in disputes concerning key maritime interests, and expand its playbook in the South China Sea beyond the maritime domain, among other suggestions.[7]

Although many of these proposals are strategically sound, they tend to focus on broader ways rather than specific means to achieve objectives in the gray zone. Here, while technology cannot be viewed as a panacea for strategic problems, it can certainly expand the range of

[4] Michael J. Mazarr, foreword to *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Washington, DC: U.S. Army War College Press, 2015), ix.
[5] Green et al, *Countering Coercion in Maritime Asia*, 283.
[6] Hal Brands and Zack Cooper, "Getting Serious About Strategy in the South China Sea," *Naval War College Review* 71, no.1 (Winter 2018): 28.
[7] James Holmes and Toshi Yoshihara, "Deterring China in the 'Gray Zone': Lesson of the South China Sea for U.S. Alliances," *Orbis* 61, no.3 (2017): 338, https://www.sciencedirect.com/science/article/pii/S003043871730042X.

options available to gray zone defenders. In this regard, a gap in the literature exists with regard to emerging technologies and their potential role in strengthening traditional deterrence frameworks that are often circumvented by gray zone strategies. Emerging technologies will become increasingly relevant as they continue to advance and mature. We have already begun observing incidents involving unmanned vehicles occurring in disputed areas in East Asia, validating concerns that we are now swimming in uncharted ethical, legal, and operational waters. The increasing prevalence of such interactions is a strong indication that deeper dialogue on the role of emerging technologies in the gray zone is well overdue, especially for those seeking inspired methods to erode the efficacy of gray zone aggression and discourage their application. The discourse here seeks to build on the theoretical solutions offered by various commentators and scholars by exploring how emerging technologies can be creatively and practically employed to deter gray zone aggression in disputed maritime areas.

Emerging technologies can indeed be harnessed to strengthen a deterrence by denial approach against maritime gray zone aggression by helping defenders raise the expected costs for gray zone coercers at the point of aggression, thereby shifting the burden of escalation back to the latter. At the same time, while these technologies are valuable in deterring gray zone aggression and defending international rules and frameworks, ethically questionable applications of such technologies risk tainting the international order they are meant to preserve. Perceived abuse of emerging technologies would likely have far-reaching negative implications for the rule of law and the establishment of norms in the governance of inter-state relations. Hence, even as gray zone defenders pursue new means to strengthen existing deterrence frameworks, they must be careful to ensure the principled use of these technologies.

This essay will first define the gray zone and outline why and how gray zone approaches are applied in the maritime domain. Next, it will discuss the applicability of existing deterrence concepts to the gray zone. The subsequent discussion on the role of emerging technologies will evaluate their utility for gray zone deterrence through the lens of ambiguity, asymmetry, and incrementalism, while evaluating ethical and legal considerations that could undermine the legitimacy of gray zone defenders. Based on these deliberations, the essay will conclude by proposing the suitability of these technologies.

II. INSIDE THE GRAY ZONE

"*All warfare is based on deception.*"

Sun Tzu, *The Art of War*

Gray zone strategies can be defined as efforts that seek to attain specific strategic aims without resorting to the use of direct force. Even though gray zone approaches seek to avoid violence, they are still recognized as hostile and coercive.[8] Gray zone coercion therefore does not appear to fit within the conventional dichotomy of war and peace. Indeed, a report from the Center for New American Security (CNAS) defines the gray zone as a "state of security competition between peace and war."[9] As Hudson Institute fellow Nadia Schadlow elegantly elucidates, this expanse between conventional notions of war and peace is not barren, but one "churning with political, economic, and security competitions."[10] The possibilities within the gray zone, while certainly not boundless, are therefore confined only by the threshold of conventional force.

In this regard, gray zone coercion should not be conflated with hybrid warfare, which is a more expansive concept. Hybrid warfare has been described by Frank Hoffman, a leading scholar on the subject, as a "tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain…political objectives."[11] The key difference between hybrid warfare and gray zone strategies is the exclusion of conventional

[8] Hal Brands, "Paradoxes of the Gray Zone," *FPRI E-Note*, Foreign Policy Research Institute, February 5 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone.

[9] Amy Chang et al, *Shades of Gray: Technology, Strategic Competition, and Stability in Maritime Asia* (Washington, DC: Center for New American Security, 2015), 3.

[10] Nadia Schadlow, "Peace and War: The Space Between," War on the Rocks, August 18 2014, https://warontherocks.com/2014/08/peace-and-war-the-space-between.

[11] Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs Hybrid Threats," War on the Rocks, 28 July 2014, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats.

weapons from the toolbox of the latter. Hybrid warfare therefore lies closer to the conventional end on the spectrum of conflict than gray zone approaches, given its embrace of traditional means of warfare and violence that gray zone provocateurs deliberately avoid.

A gray zone practitioner's approach in the murky landscape of the gray zone is intentionally calibrated to remain below red-lines in order to avoid escalation, while remaining sufficiently aggressive so as to impose its will on its target. To achieve their aims, gray zone perpetrators are likely to utilize a vast array of means across various domains to achieve broader political objectives, while hovering just below traditional escalatory thresholds. These include the employment of proxies, covert operations, and paramilitaries in the physical domains of air, land, sea, and space, the realm of cyberspace, and dominance in the legal and informational spheres of influence.[12] By exploiting a gradual long-term approach employing these varied means, a gray zone aggressor can subtly gain influence over an extended period of time at the expense of its target.

Some gray zone practitioners utilize such non-traditional means to avoid confrontation because they perceive their adversaries as having an advantage at higher levels of escalation. Weaker states are compelled to use gray zone tactics in an effort to complicate and even bypass conventional deterrent measures while degrading their credibility.[13] This approach allows a weak gray zone aggressor to present a *fait accompli* to its target, before the latter is able to adapt and create appropriate mechanisms to respond. For instance, China has successfully reclaimed and militarized islands in the South China Sea through a series of *faits accomplis*, even in the face of sustained objections from regional disputants and others in the international community.

[12] Green et al., "Countering Coercion," 21.

[13] Michael B. Petersen, "The Chinese Maritime Gray Zone: Definitions, Dangers, and the Complications of Rights Protection Operations," in *China's Maritime Gray Zone Operations*, ed. Andrew S. Erickson and Ryan D. Martinson (Annapolis, MD: Naval Institute Press, 2019), 19.

In other cases, gray zone approaches appear to be the domain of revisionist states and rising powers seeking to alter the existing status quo in the international environment. While these state actors recognize the utility of an international order, they are resentful of the status quo and seek to reshape specific elements without resorting to violence.[14] Besides the possibility of incurring substantial losses, these states are also anxious about potential reputational costs even as they seek to achieve their ambitious goal of reforming elements of an entrenched system. The use of force in particular could result in international opprobrium, or worse, significant reprisals led or endorsed by other powers. Gray zone actors are therefore eager to avoid escalation, given the heightened risk of a broader conflict against other stakeholders in the international system.

A. GRAY ZONE CHARACTERISTICS – AMBIGUITY, ASYMMETRY, AND INCREMENTALISM

A successful gray zone state practitioner is able to entrench its position of advantage by capitalizing on the key characteristics of gray zone strategies – ambiguity, asymmetry, and incrementalism.[15] First, as its name suggests, the gray zone is shrouded in ambiguity, particularly a lack of clarity concerning the appropriate international policy and legal mechanisms that should be observed.[16] Indeed, the chief characteristic of gray zone campaigns is ambiguity concerning "ultimate objectives, the participants, [and] whether international treaties and norms have been violated."[17] The employment of non-conventional means serve to obfuscate and

[14] Mazarr, *Mastering the Gray Zone*, 11.

[15] Green et al, "Countering Coercion," 29-34.

[16] Philip Kapusta, "The Gray Zone," *Special Warfare* 28, no.4 (October-December 2015), 20, ProQuest Central (1750033789).

[17] David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone'," War on the Rocks, May 19 2015, https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone.

hinder an appropriate and proportionate reaction, thereby reducing the likelihood of a coherent response to the original provocation. For instance, the use of maritime militia embarked on fishing vessels allows gray zone state actors to accrue gains from the militia's aggressive activities while disclaiming responsibility for their illicit actions. Moreover, the lack of intelligence and information concerning gray zone activities allows their perpetrators to deny involvement, foster further uncertainty, and impede an appropriate response.

Second, aggressor states are able to exploit asymmetric capabilities and interests to attain their objectives in the gray zone.[18] For instance, a state can choose to target specific aspects of the status quo that are worth relatively less to its expected adversary. By exploiting differences in the perceived "value of the object," it is able to reduce the likelihood of a response and the corresponding possibility of escalation to full-fledged conflict.[19] Separately, an aggressor can also seek to challenge its adversaries within certain domains where it has an asymmetric capability advantage despite being conventionally inferior. Hence, a weak state turned gray zone aggressor is able to gain the strategic initiative by rendering its adversary's conventional advantage irrelevant. In this regard, the use of coast guard and maritime militia vessels for gray zone operations effectively neutralizes stronger navies concerned about the legal and operational ramifications of a military response. By negating the conventional dominance of its adversary and diminishing the prospect of an effective response, a gray zone provocateur is able to improve its chances of success.

Third, gray zone coercers seek to achieve incremental gains over time, given their challenge of accomplishing ambitious aims without provoking a sizeable backlash. Such

[18] Green et al, "Countering Coercion," 30-31.
[19] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 92.

strategic gradualism involves the progressive attainment of limited objectives, which individually do not suffice to provoke conflict, but when accumulated over time allows gray zone aggressors to achieve significant strategic gains. These incremental strategies are effective because a gray zone target is often unable to recognize the broader implications of such cumulative actions, thereby delaying a potential response. This usually results in either an ineffective reaction or eventual inaction. In effect, strategic gradualism challenges the Clausewitzian dictum that the value of the object governs the sacrifices that must be made in terms of magnitude and duration, simply by impeding a defensive response.[20] Hence, strategic gradualism allows an aggressor to achieve substantial gains at disproportionately little cost to itself.

B. THE MARITIME GRAY ZONE

In their in-depth analysis of Chinese maritime activities as a clear example of gray zone aggression, Michael Green and his colleagues at the CSIS find that Beijing's actions can be classified into four categories. These maritime gray zone incidents coalesce around China's challenge to existing norms, its abuse of these norms via lawfare, its exploitation of *faits accomplis* to establish physical control, and its establishment of control over disputed areas by explicitly violating red-lines.[21] While these categories may appear distinct, each can be mapped to the common hallmarks of gray zone strategies – ambiguity, asymmetry, and incrementalism.

In some respects, the unique features of the maritime domain and the inherent shortfalls of existing regimes governing its use make it more susceptible to gray zone activity. First, the

[20] Clausewitz, *On War*, 92.

[21] Green et al., "Countering Coercion," 266.

international maritime regime is itself sufficiently ambiguous so as to provoke dispute. While there is a set of established international laws and norms governing the maritime order through frameworks such as the United Nations Conventions on the Law of the Sea (UNCLOS), these frameworks do not necessarily offer concrete guidance on the application of these rules to specific contexts.[22] In this regard, UNCLOS was ultimately attained only through a “grand bargain” that sought to attain a “balance of interests” through compromise.[23] Hence, ambiguities were intentionally structured within the framework of UNCLOS for the purpose of bridging the divide between coastal states seeking to consolidate their authority over maritime space, and other states concerned with protecting the freedoms of navigation and overflight.[24] Second, the intricacies of the international maritime legal order often exacerbate the complexity of maritime claims and generate multifaceted disputes over sovereign possessions, maritime rights and other uses of the sea.[25] For instance, questions of sovereignty over land territory do not fall under the ambit of UNCLOS, with relevant provisions in the framework on coastal state jurisdiction assuming such sovereignty.[26] Thus, the inherent ambiguity of the maritime domain effectively allows gray zone practitioners to contest and exploit perceived lacunas in international laws, rules, and norms for their own ends.

Besides ambiguity, the gray zone characteristics of asymmetry and incrementalism are also applicable to the maritime domain. Here, a veritable buffet of coercive options exists for

[22] Petersen, “Chinese Maritime Gray Zone,” 21.

[23] James Kraska, “The Law of the Sea Convention: A National Security Success – Global Strategic Mobility Through the Rule of Law,” *The George Washington International Law Review* 39, no.3 (2007): 544.

[24] Sam Bateman, “UNCLOS and Its Limitations as the Foundation for a Regional Maritime Security Regime,” *The Korean Journal of Defense Analysis* 19, no. 3 (2007): 31.

[25] Petersen, “Chinese Maritime Gray Zone,” 21.

[26] Robert Beckman, “The UN Convention on the Law of the Sea and the Maritime Disputes in the South China Sea,” *The American Journal of International Law* 107, no.1 (Jan 2013): 142.

maritime gray zone actors to "nibble" away at the status quo, including what has frequently been referred to as "cabbage" and "salami-slicing" techniques.[27]

"Cabbage" tactics have allowed gray zone actors to capitalize on their asymmetric advantage in non-military capabilities to establish control over disputed maritime areas via *faits accomplis*. For instance, in what Chinese scholars have termed a "war without gun smoke," Beijing deploys a mix of maritime assets from the coast guard, maritime militias, civilian fishing fleets, and even state-owned oil and gas corporations to encircle disputed maritime areas.[28] Retired Chinese Major General Zhang Zhaozhong described such tactics as "surrounding a contested area with so many boats… that the island is thus wrapped layer by layer like a cabbage."[29] By surrounding contested zones or islands with multiple layers of vessels, China has been able to assert its sovereignty claims while restricting access to other disputants. Beijing effectively compels its opponents to recognize de facto Chinese sovereignty, even as traditional instruments of hard power stand ready to reinforce Chinese actions when necessary.[30] Furthermore, any deployment of military assets in response to such implicit aggression risks accusations of disproportionate retaliation and the negative optics of naval vessels facing off against civilian fishing vessels in the outer layer of the "cabbage." Hence, "cabbage" tactics have enabled gray zone coercers like China to achieve strategic gains at little or no cost.

Similarly, gray zone practitioners employ salami-slicing tactics to incrementally violate established red-lines while mitigating the risk of escalation. By initiating a "low-level incident,"

[27] Brands, "Paradoxes of the Gray Zone".
[28] Andrew S. Erickson and Ryan D. Martinson, "Introduction. "War Without Gunsmoke," in Erickson and Martinson, *China's Maritime Gray Zone Operations*, 2.
[29] Scott Cheney-Peters, "A Feast of Cabbage and Salami: Part I – The Vocabulary of Asian Maritime Disputes," Center for International Maritime Security, October 29 2014, http://cimsec.org/feast-cabbage-salami-part-vocabulary-asian-maritime-disputes/13441.
[30] James R. Holmes, "The Return of China's Small-Stick Diplomacy in South China Sea," *The Diplomat*, 9 January 2014, https://thediplomat.com/2014/01/the-return-of-chinas-small-stick-diplomacy-in-south-china-sea.

potential responses are probed and analyzed in what has been described as a method of "erosion."[31] The incident at hand can be disavowed in the event of resistance, or expanded accordingly to set a new precedent if there is none. Here, the lack of "qualitative division between a minor transgression and a major affront" allows a gray zone practitioner to leverage an incremental strategy to increase the level of provocation gradually without provoking a clear response.[32] Eventually, through the accumulation of many such incidents, or salami-slicing, a gray zone aggressor is able to achieve a drastic alteration in the status quo over time despite violating multiple red-lines in the process.

Given the difficulties in rolling back gains that have accrued over time through maritime gray zone coercion, defenders must seek to strengthen deterrent measures that will shift the burden of escalation back to the aggressors. Establishing credible deterrent measures would increase the expected costs of gray zone aggression and alter the risk calculus of gray zone coercers, thereby compelling them to reconsider commencing their illicit activities.

[31] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 67.

[32] Ibid, 68.

III. GRAY ZONE DETERRENCE

As the renowned deterrence strategist Thomas Schelling explains, deterrence works through "latent violence that can influence…choice," with the "threat of pain [used] to structure someone's motives."[33] Deterrence seeks to persuade an adversary not to initiate a course of action because of the fear that the expected costs associated with the action will exceed the potential gains that can be accrued. In this regard, deterrence attempts to maintain the status quo by influencing the intentions of others who may seek to change it. One should therefore view deterrence as the practice of "interstate signaling" through which states engage in negotiation over opposing aims.[34] Indeed, the eminent statesman Henry Kissinger notes that deterrence is the product of "power, the will to use it, and the assessment of these by the potential aggressor."[35] Deterrence is therefore most effective when a potential aggressor perceives that the defender has the capability and resolve to act against it.

Writing in reference to the maritime domain, Holmes and Yoshihara offer several broad principles of deterrence that allow states to maximize their capability and resolve in the gray zone, while ensuring that aggressors recognize the credibility of the potential responses. They suggest that gray zone deterrers must accept the nature of gray zone conflict as an extended confrontation requiring sustained attention as well as credible red lines to identify and respond to gray zone strategies. In this regard, states must utilize every instrument of statecraft available to them and adopt a multi-domain response to gray zone strategies. Notably, Holmes and Yoshihara

[33] Schelling, *Arms and Influence*, 3.
[34] Green et al., "Countering Coercion," 34.
[35] Henry A. Kissinger, *The Necessity for Choice: Prospects of American Foreign Policy* (New York, NY: Harper, 1961), 12.

contend that deterrers must retain their legitimacy even as they undertake robust peacetime operations and strengthen conventional deterrent measures.[36]

Such conventional deterrent measures typically take two forms – denial and punishment. Deterrence by denial renders aggression unprofitable by reducing the likelihood that the aggressor is able to achieve its key objective.[37] Specifically, a defender makes it more challenging for an aggressor to acquire the disputed object by emplacing "defensive attributes" that have a strong potential to inflict heavy costs on their adversaries and make the object in question "indigestible."[38] A conventional example in the maritime domain would be anti-access/area-denial capabilities such as anti-ship cruise missiles. The expectation of higher costs that such measures impose on would-be aggressors influences their cost-benefit analysis and reduces their incentive to initiate coercive activities. Such deterrence relies on generating sufficient fear of costs that will be imposed *during* the act of aggression.[39] The efficacy of this form of deterrence is therefore dependent on credible *defensive* capabilities that generate the expectation of high costs.

In contrast, deterrence by punishment threatens reprisal and subsequent escalation *after* the initial act of aggression, rather than imposing direct costs at the time and place of the coercive action. The effectiveness of deterrence by punishment is therefore predicated on the credibility of the defender's threat, including its *offensive* capabilities and commitment to the disputed object. Furthermore, the defender's red-lines must be clear as any perceived ambiguity would only serve to weaken the deterrent effect.[40] Here, a hypothetical example in the context of

[36] Holmes and Yoshihara, "Deterring China in the Gray Zone," 337-8.
[37] Glenn H. Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1961), 15.
[38] Ibid.
[39] A. Wess Mitchell, "The Case for Deterrence by Denial," *The American Interest*, 12 August 2015, https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial.
[40] Ibid.

the maritime gray zone would be the threat of conventional strikes against China in retaliation for its *de facto* annexation and militarization of the Spratly Islands.

A. CHALLENGES OF GRAY ZONE DETERRENCE

In general, deterrence by denial is considered by most to be a more viable option in responding to gray zone strategies because it imposes costs that are directly linked to the specific act of aggression, thereby leaving little room for further misinterpretation and ambiguity.[41] Conversely, critics of deterrence by punishment contend that a punitive approach requires wide-ranging responses that would be unpalatable to defenders given the higher risk of escalation. Thus, pursuing deterrence by punishment may be counterproductive, given the questionable credibility of the defender's responses.

Indeed, the challenges of deterrence by punishment illustrate how a gray zone approach exploits the asymmetry of interests between the aggressor and the defender, calling into question the commitment of the latter to the disputed object. Essentially, deterrence by punishment forces the defender to incur significant costs associated with retaliation that it may not be willing to sustain. In particular, reprisals could quickly evolve into compellence. Instead of dissuading further gray zone aggression, a gray zone defender could inadvertently find itself pursuing the more onerous objective of coercing its gray zone adversary into backing down completely from its quest to change the status quo.[42] As Schelling opines, compellence is far more difficult than deterrence.[43] The defender may simply be unwilling to enter an indeterminate and prolonged

[41] Mitchell, "The Case for Deterrence by Denial."
[42] Ibid.
[43] Schelling, *Arms and Influence*, 100.

conflict with a high probability of escalation, especially if its valuation of the object in question does not warrant the magnitude of effort required to defend it.[44]

Moreover, limited-war techniques embodied by gray zone warfare are precisely designed to avoid punitive measures, thereby undermining the efficacy of deterrence by punishment. By bypassing well-defined red-lines, gray zone practitioners circumvent response frameworks typically designed around conventional responses, thereby averting reprisal. Consequently, defenders fearing inadvertent escalation are left in a quandary when faced with such unorthodox provocations. An aggressor's ability to circumvent conventional deterrent frameworks therefore empowers it to take action, while shifting the full weight of the "burden of escalation" to the defender. Schelling would describe the act of shifting the "burden of escalation" as the aggressor shaping circumstances in such a way that it is the defender "who is embarrassed by having the 'last clear chance' to avert disaster."[45]

Taking on the "burden of escalation" exacerbates a defender's difficulties, given that it is already forced to respond under significant time pressure to provocations that typically do not align with preplanned responses. The lack of a clear *casus belli* justifying a conventional response compels the gray zone defender to either respond disproportionately and assume full responsibility for any resulting escalation, adopt inadequate half-measures as a compromise to lower the risk of escalation, or simply avoid acting to preclude the possibility of escalation entirely. Indeed, the burden of escalation often proves sufficiently weighty to engender strategic and tactical paralysis. The resulting walk-over for the gray zone practitioner is a strategic masterstroke worthy of Sun Tzu himself.

[44] Clausewitz, *On War*, 92.

[45] Schelling, *Arms and Influence*, 101.

What then can be done to stop the seemingly inexorable advance of gray zone aggression? Here, a turn to ultra-modern means could perhaps hold the key to countering this age-old conundrum. While technology should not be viewed as a panacea for strategic problems, it can certainly expand the range of options available to gray zone defenders. In this regard, emerging technologies can be tailored to play a role in strengthening deterrence against gray zone aggression and in shifting the burden of escalation back to gray zone coercers. The following discourse illustrates examples of how specific technologies can be ethically employed in alleviating ambiguity, addressing asymmetry, and inhibiting incrementalism. This is by no means an exhaustive list of solutions to the gray zone challenge, but one meant to inspire further discussion on creative countermeasures to gray zone aggression.

IV. EMERGING TECHNOLOGIES IN THE GRAY ZONE

Emerging technologies can play a role in strengthening deterrence against gray zone aggression. Technologies such as artificial intelligence (AI), unmanned platforms, and non-lethal weapons can be employed against gray zone tactics by bolstering deterrence by denial measures designed to increase expected costs at the point of aggression. Unfortunately, there has been minimal discussion on the use of emerging technologies as a defensive response to maritime gray zone strategies. The shortfall in academic discourse also includes ethical considerations that have implications for gray zone defenders seeking to apply these technologies in a manner consistent with the underlying principles and norms forming the basis of the rules-based order.

At present, much of the existing literature emphasizes the application of these emerging technologies as offensive rather than defensive tools. For instance, a report from the Center for Strategic and Budgetary Assessments considers the possibility of leveraging electromagnetic warfare (EMW) to establish "escalation dominance" over gray zone activities. The report proposes EMW as a tool to counter Russian or Chinese gray zone aggression, noting that Russian and Chinese long-range sensors and weapons grant them an asymmetric advantage by enabling precise attacks on their adversaries in the vicinity of their objectives.[46] It suggests that EMW can improve the ability of U.S. weapons to conduct small and "less-escalatory" offensive operations, while denying Russia and China the ability to strike U.S. forces.[47] While the findings are noteworthy, the report's focus on denying and responding to high-end conventional strikes conflates the concepts of gray zone and hybrid warfare, which as explained, are separate and

[46] Bryan Clark et al, *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance*, CSBA Report (Washington, DC: CSBA, 2017), 17-22.
[47] Ibid, 67.

distinct. Furthermore, the report's emphasis seems to be the use of EMW as a tool for compellence rather than as an instrument of deterrence.

Another CNAS study describes how emerging technologies can potentially be used in conjunction with gray zone strategies to gain an advantage in geopolitical competition, by capitalizing on the uncertainty concerning the adoption of such technologies. Specifically, new technological capabilities become a concern when they are offensively used to alter existing "patterns of interaction" that contribute to predictability and stability in interstate relationships.[48] For instance, the study's authors cite how unmanned drones enabled the United States to conduct "sovereignty-violating" precision strikes in Pakistan without risking the lives of American pilots.[49] By changing the risk calculus among all involved stakeholders in an unprecedented manner, the employment of these technologies could escalate existing tensions and contribute to inadvertent conflict.[50] To the authors' credit, they explicitly reject the Pollyannish view of preventing the proliferation of such technologies. Rather, they acknowledge the need to establish norms and develop dialogue on the employment of such technologies in the maritime domain in order to encourage consistent behavior and minimize the risk of unwanted escalation.[51]

While the report presents valid concerns that offensive uses of emerging technologies could escalate tensions and generate conflict, it neglects consideration of their potential defensive applications. Indeed, emerging technologies can address the gray zone challenges of ambiguity, asymmetry, and incrementalism that have posed such seemingly intractable problems to gray zone defenders. A deterrence by denial approach incorporating emerging technologies can diminish the appeal of gray zone coercion by raising the expected costs and reducing the

[48] Chang et al, *Shades of Gray*, 7.
[49] Ibid, 8.
[50] Ibid, 9-10.
[51] Ibid, 6.

potential payoff for a gray zone perpetrator. Moreover, it is feasible for gray zone defenders to judiciously employ emerging technologies while upholding ethical and legal principles that bolster their legitimacy.

A. ALLEVIATING AMBIGUITY

Emerging technologies can be used to shed light on the gray zone by enhancing indicators and warning (I&W) initiatives and bolstering intelligence, surveillance and reconnaissance (ISR) efforts that facilitate the crafting of credible deterrent measures. As noted earlier, the ambiguity pervading gray zone activities is a key stumbling block that impedes appropriate responses to gray zone aggression. Here, defenders' deficiencies include insufficient forewarning, indication, and evidence of gray zone activities. When faced with coercive strategies, defenders are therefore often strategically and operationally surprised, which results in either a reactionary and poorly considered response, or strategic and operational paralysis.

Indicators and Warning

The application of emerging technologies in the domain of I&W would primarily focus on providing overall strategic assessments of adversarial plans and intentions in the gray zone. Here, AI can play a role in sense-making vast amounts of information and predicting potential courses of coercion. With the support of AI, gray zone defenders can prepare suitable counter-measures and deploy appropriate assets well ahead of time to deter potential adversaries and impede their ability to achieve their objectives.

AI is able to display intentionality, intelligence, and adaptivity by serving as a close imitation of human intellect and capacity.[52] The U.S. Department of Defense (DoD) defines AI as "the ability of machines to perform tasks that normally require human intelligence…whether digitally or as the smart software behind autonomous physical systems."[53] When AI is applied together with machine learning and data analytics, it can be used to integrate information, analyze data, and improve human decision-making. Besides these functions, the predictive potential of AI is also well-recognized. A study of 152 AI business ventures by Harvard Business Review found that 38% of these projects involved the use of machine-learning algorithms to conduct "cognitive insight," where AI is essentially used to sift through vast amounts of data, identify patterns, and conduct a predictive analysis of consumer preferences.[54]

While the use of AI in forecasting adversarial plans sounds fantastical, its application in this domain is advancing rapidly. The tremendous promise of AI in this field has led some to contend that AI is fundamentally a "prediction technology," whose ability to use existing data to generate new information makes it valuable in multiple fields.[55] Machine learning allows algorithms to learn from historical datasets to predict the likelihood of outcomes and uncover patterns in the data that are not easily observable. A report by the U.S. Government Accountability Office notes that AI can conceivably be used to "build a predictive model of cyber-attacks," and can even be employed to forecast the likely location of crimes to "improve

[52] Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world," Brookings, 24 April 2018, https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world.
[53] U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy* (Washington, DC: Office of the Secretary of Defense, 2019), 5.
[54] Thomas H. Davenport and Rajeev Ronanki, "Artificial Intelligence for the Real World," *Harvard Business Review*, January-February 2018, https://hbr.org/2018/01/artificial-intelligence-for-the-real-world.
[55] Ajay Agrawal et al., *Prediction Machines: The Simple Economics of Artificial Intelligence*, (Boston, MA: Harvard Business Review Press, 2018), 24.

allocation of law enforcement resources."[56] The DoD and Google had previously undertaken a joint effort under the ambit of Project Maven that would have utilized AI to comb through data, recognize patterns, and alert analysts of suspicious or anomalous activity.[57] While Google has since pulled out of the joint venture, the project is still being actively pursued by the DoD. There are other similar AI endeavors, including the Defense Advanced Research Projects Agency's (DARPA) effort to develop software that can gauge an adversary's response to various provocations, determine its intentions, and provide feedback to commanders that can better inform their response on the ground.[58]

Here, inputs to a baseline "gray zone dataset" could include the number and type of assets previously deployed by the aggressor, the diplomatic, informational, political, economic, and military circumstances precipitating aggression, the precise locations of prior gray zone activities in the wider theater of interest and the media environment both prior to and after the act of coercion. Indeed, large amounts of open source information residing in opinion surveys, social media, and imagery can also be analyzed with the aid of AI that could reveal significant insights into adversarial behavior. For instance, a National Security Innovations study found that there was a strong correlation between spikes of certain linguistic indicators in official Russian and Chinese discourse and the conduct of gray zone activities by both countries.[59] In sum, a greater number of inputs would contribute to a more robust dataset, which in turn can warn defenders of

[56] U.S. Government Accountability Office, *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications.* (Washington, DC: GAO, March 2018): 60; Ibid, 7.

[57] Christian Davenport, "Future Wars May Depend as much on Algorithms as on Ammunition, report says: Pentagon boosts spending on artificial intelligence, big data and powerful computers," *Washington Post*, 3 December 2017. ProQuest (1971618030).

[58] Todd South, "DARPA to use artificial intelligence to help commanders in 'gray zone' conflicts," *Army Times*, 27 March 2018, https://www.armytimes.com/news/your-army/2018/03/27/darpa-to-use-artificial-intelligence-to-help-commanders-in-gray-zone-conflicts.

[59] National Security Innovations, "Panel Discussion on the Gray Zone," Strategic Multi-Layer Assessment Report, 27 April 2017, 8. http://nsiteam.com/social/wp-content/uploads/2017/06/U_Final_SMA_SOCOM-Gray-Zone-Panel-Discussion-v2.pdf.

impending gray zone activity. Essentially, the predictive capacity of AI can be harnessed to address critical deficiencies in the situational awareness of gray zone defenders. By establishing a baseline set of potential gray zone behaviors from prior instances of coercion, trends and patterns can be identified to forecast future aggression.

Foreknowledge of adversarial intentions and actions will help gray zone defenders avoid strategic and tactical surprise by giving them the initiative. Indication of the likely composition, capabilities, and location of the vessels deployed by a gray zone coercer would be extremely helpful given the limited assets gray zone defenders possess in policing the vast maritime domain. Gray zone defenders can thus marshal their limited resources to match their adversaries with credible forces and capabilities that would deter the latter's initiation of coercive gray zone activities. In this regard, calibrated maritime capabilities can be deployed prior to a predicted gray zone operation, serving as an effective deterrent presence and discouraging the commencement of coercive activities. Even if the gray zone actor decides to proceed, it would be at a disadvantage given the additional time the gray zone defender would have had to determine appropriate rules of engagement and coordinate a holistic response that increases the costs and lowers the benefits to the aggressor. In sum, the overall response of gray zone defenders would be vastly enhanced, enabling them to avoid strategic and operational paralysis. Moreover, defenders would be empowered to shift the burden of escalation back to the would-be gray zone coercer by altering its cost-benefit calculus, thus discouraging the initiation of coercive gray zone activities.

Some would suggest that relying on AI algorithms to furnish highly accurate predictions of adversarial behavior is at best a questionable endeavor. In particular, there are valid concerns that insufficiently robust data could give rise to unreliable output, given the reliance of machine learning algorithms on the quantity and quality of input data. Moreover, the internal processes of predictive algorithms can be rather impenetrable because of their immense complexity, especially with regard to how data is evaluated and the derivation of eventual output. These fundamental uncertainties could prove to be significant stumbling blocks for military planners and civilian policymakers struggling to trust and act on these algorithmic forecasts.

Indeed, one should exercise due caution when considering the output of predictive analysis. Predictive algorithms are not meant to replace the judgment of human analysts, who should ideally view AI-based forecasts as another factor in their decision-making, albeit an increasingly important one. These algorithms require continuous refinement in order to bolster their predictive accuracy, which necessitates additional observations and feedback from real-world application. Hence, some initial trial and error is to be expected before the algorithm's accuracy can be improved through feedback. With regard to the issue of transparency, attempts are being made to design algorithms that can identify the specific factors they rely on to make predictions. For instance, DARPA is seeking to create new machine learning techniques that will allow human users to understand the rationale for their algorithmic output, including comprehensible explanations in prose.[60] Advances in this area can open up the black-box of machine-learning algorithms, present underlying processes for human consideration, and assuage the concerns of planners and policymakers leveraging AI-based forecasts in decision-making.

In addition, there are other benefits to the use of machine learning models that go beyond simply attempting to forecast gray zone activities with flawless accuracy. Specifically, these models can also determine unexpected correlations between seemingly disparate factors and aid

[60] David Gunning, "Explainable Artificial Intelligence," Defense Advanced Research Projects Agency, https://www.darpa.mil/program/explainable-artificial-intelligence.

in weighting specific factors contributing to gray zone behavior.[61] Underlying patterns of adversarial conduct would therefore still be unearthed even if predictive accuracy is ultimately limited. These insights are inherently invaluable in contributing to a deeper understanding of the intentions and actions of a gray zone adversary, which would also inform and improve the responses of gray zone defenders.

Intelligence, Surveillance, and Reconnaissance

At the same time, a gray zone defender should still seek to enhance the accuracy of its predictive analysis by seeking to gather more data on adversarial behavior both in and out of the gray zone. This objective can be achieved via the establishment of a strong operational intelligence, surveillance, and reconnaissance (ISR) capability. Beyond ensuring a steady stream of data to drive predictive analysis and contribute to their further refinement, pervasive ISR would greatly assist in providing a clearer tactical picture and reduce the uncertainty of the gray zone.

However, existing ISR solutions face significant limitations. Operational sustainability and human fatigue often dictate the boundaries of human-driven ISR. The limited men and materiel available will simply not suffice to attain sustained vigilance over the vastness of the maritime domain. Moreover, despite the ability of space-based ISR to provide global coverage, the actual operational utility of existing systems is constrained by their capacity and "associated orbit requirements."[62] Simply put, given the growing emphasis on conventional threats

[61] Agrawal et al., *Prediction Machines*, 37.
[62] Chairman, U.S. Joint Chiefs of Staff, *Space Operations*, Joint Publication (JP) 3-14 (Washington, DC: CJCS, 10 April 2018), II-4.

associated with great-power competition, the tracking of non-military gray zone assets using these limited assets is likely to be deprioritized.

In this regard, unmanned systems can be employed to provide sustained operational ISR and establish superior maritime domain awareness. Indeed, the ability for drones to conduct pervasive and low-cost ISR is a significant advantage that gray zone defenders can leverage to maintain a persistent presence in a disputed area without sustaining significant manpower and maintenance costs. A Defense Science Board study commissioned by the DoD found that ISR capabilities were among four categories of physical effects or capabilities most useful for constrained military operations in the gray zone. Given their unattributable and "reversible" effects, the report noted that the use of unmanned underwater vehicles for surveilling harbors and the employment of unmanned aerial platforms for beyond-horizon surveillance would be of most utility in operating against gray zone coercers.[63] Unmanned vehicles can therefore play an important role in contributing to the situational awareness of gray zone defenders while minimizing the risk of unwanted escalation.

At the same time, ensuring that a gray zone aggressor understands that it is potentially under unremitting surveillance by unmanned systems would likely shape its behavior and serve as a crucial deterrent measure. Much like the concept of Jeremy Bentham's fabled Panopticon, the very possibility of being under surveillance induces "a state of conscious and permanent visibility" in a gray zone aggressor that would likely give it pause, regardless of whether it is indeed under observation.[64] In this regard, the intrinsic power of the unmanned "gaze" can shape

[63] U.S. Department of Defense, *Capabilities for Constrained Military Operations* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, December 2016), 27.

[64] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York, NY: Pantheon Books, 1977), 201.

behavior in the gray zone by compelling a would-be gray zone coercer concerned with its international reputation to reconsider initiating illicit activities.

B. ADDRESSING ASYMMETRY

Beyond performing ISR functions, unmanned vessels can also be used to conduct operations such as freedom of navigation maneuvers within disputed maritime zones, which are more likely to carry a greater risk of escalation given the unpredictable and dynamic interactions that may occur. In this regard, the technology enabling unmanned vessels to conduct transoceanic cruises has matured significantly, as demonstrated by the successful autonomous navigation of the U.S. Navy's Sea Hunter unmanned surface vessel from San Diego to Pearl Harbor.[65] The use of unmanned systems is advantageous when there is asymmetric commitment to the object in question, specifically when the gray zone defender is unwilling to incur significant operational risk vis-à-vis the aggressor. Deploying unmanned patrols minimizes risk by reducing the potential for loss of life and limb, while simultaneously allowing defenders to maintain a credible presence.

A near-miss incident between the USS *Decatur* and the Chinese Luyang-class destroyer *Lanzhou* in the South China Sea illustrates a gray zone defender's typical conundrum. In this instance, the *Decatur* and the *Lanzhou* were engaged in a potentially lethal game of chicken during the former's freedom of navigation operation in September 2018. The *Lanzhou* approached to within 45 yards of the *Decatur's* bow, forcing the *Decatur* to take evasive maneuvers to avoid certain collision. While the captain of the *Decatur* rightly took the necessary

[65] Gina Harkins, "A Navy Ship Sailed to Hawaii and Back with No One on Board," Military.com, 15 February 2019, https://www.military.com/defensetech/2019/02/15/navy-ship-sailed-hawaii-and-back-no-one-board.html.

actions to avoid endangering the lives of his crew, the interaction between both ships highlights the asymmetric interests between the U.S. and China. Indeed, the *Lanzhou*'s actions underscore Beijing's strong commitment to its maritime claims, while the *Decatur*'s evasive maneuvers can be interpreted as Washington's relatively lower valuation of its objectives in the South China Sea. The apparent interest disparity will not only have a bearing on future exchanges, but would likely erode the U.S.' credibility and undermine the value of its regional alliances.

The dynamics of the situation would have been completely altered had the *Decatur* been an unmanned surface vessel instead of a manned destroyer. The use of an unmanned vessel would arguably have tilted the balance of risk in favor of the U.S. as no American lives would have been at stake. In such circumstances, the Chinese captain may have "blinked" first, with the altered balance between risk and reward likely compelling the Chinese captain to avert disaster by swerving first. In all likelihood, the *Lanzhou* would have avoided initiating such dangerous maneuvers in the first place to avoid the embarrassment of having to back down in the face of an unwavering unmanned adversary. In this regard, unmanned surface vessels can increase the credibility of freedom of navigation patrols by increasing the potential costs of coercion and shifting the burden of escalation to the aggressor.

Despite the potential for unmanned vehicles to mitigate the challenge of asymmetric interests, there are legitimate fears that their deployment could provide greater impetus for the use of force at the tactical level. A 2015 CNAS wargame that involved the hypothetical use of drones in scenarios ranging from low-intensity conflicts to conventional war found that their employment *lowered* the threshold for the use of force.[66] Here, the absence of an internationally

[66] Alexandra Sander, "Game of Drones: Wargame Report," Center for a New American Security, 29 June 2016, http://drones.cnas.org/reports/game-of-drones.

recognized regime governing unmanned interactions, coupled with ambiguous circumstances in the gray zone, could potentially lead to severe consequences.

Real-world events highlight the altered risk calculus involved in such interactions and the increased potential for the use of force. In one such incident, a Chinese warship shadowing the USNS *Bowditch* in the South China Sea brazenly intercepted and absconded with the *Bowditch's* unmanned underwater vehicle (UUV) in 2016. In a separate incident, China deployed a drone that purportedly intruded into Japan's air defense identification zone near Okinawa in September 2013. While Japan launched manned aircraft to shadow the drone, the drone's unmanned status stymied Japanese pilots who were unable to issue the usual air warnings. The unique circumstances subsequently triggered the introduction of new procedures by the Japanese Defense Ministry to shoot down foreign drones intruding into its airspace.[67] This mid-air interaction not only highlights the lack of clarity concerning the employment of unmanned systems in disputed areas, but also illustrates how unmanned systems influence the risk thresholds of gray zone belligerents in novel ways that could increase the likelihood of escalation.

Notwithstanding these concerns, respondents in a CNAS survey actually considered the destruction of drones *less* escalatory vis-à-vis the shooting down of manned aircraft in comparable settings.[68] Here, the scholar Paul Scharre suggests that the emerging pattern of drone interaction indicates that drones "occupy a new rung on the escalation ladder," as the fact that no lives are at stake significantly diminishes the magnitude of losses.[69] Hence, one can draw the

[67] Ankit Panda, "Japan to Shoot Down Foreign Drones," *The Diplomat*, 22 October 2013, https://thediplomat.com/2013/10/japan-to-shoot-down-foreign-drones.

[68] Paul Scharre, "The Coming Drone Wars: A Headache in the Making for American Foreign Policy," The National Interest, 25 July 2017, https://www.cnas.org/publications/commentary/the-coming-drone-wars-a-headache-in-the-making-for-american-foreign-policy.

[69] Ibid.

fascinating conclusion that while the use of drones alters the *tactical* decisions of gray zone belligerents and leads to a lower threshold for violence, their employment minimizes negative *strategic* implications and reduces the risk of broader escalation because of smaller overall stakes. Unmanned systems could therefore prove to be invaluable assets that allow gray zone defenders to assume greater tactical risks and gain deterrent credibility while mitigating the possibility of broader escalation and conflict.

Moreover, despite greater impetus for the use of force, one can contend that it is the fundamental lack of clear red-lines supported by credible defensive measures that underpins the willingness of gray zone coercers to adopt an aggressive posture in the first place. For instance, the successful capture of the *Bowditch*'s UUV can conceivably be attributed to the UUV's lack of adequate defensive mechanisms. At a broader strategic level, the paucity of non-escalatory defensive means has arguably hampered the ability of gray zone defenders to deter and disrupt incremental gray zone strategies. Thus, even as gray zone defenders leverage technological solutions described above to alleviate ambiguity and address the challenge of asymmetric interests, they should also seek to capitalize on emerging technologies to check the incremental strategic gradualism practiced by their adversaries.

C. INHIBITING INCREMENTALISM

To impede gray zone incrementalism, the use of technological means must meet the daunting challenge of establishing credible defensive measures that can successfully deter aggressors without increasing the risk of escalation. Here, non-lethal weapons are a viable and credible means of deterrence. Separately, defenders could also broaden conflict domains to impose reputational costs directly linked to specific gray zone provocations while minimizing the likelihood of escalation. At the same time, the application of these technologies in the gray zone inevitably raises relevant ethical and legal challenges that must be carefully considered and addressed.

Non-lethal Weapon Technologies

Non-lethal weapons are designed and employed with the intention of incapacitating personnel or equipment while minimizing the risk of fatalities, permanent injury or damage to materiel and the environment.[70] While various non-lethal weapons have been in existence for some time and may not appear to be "emerging," their potential use in contemporary warfare underscores their revitalization as an "emerging" military technology.[71] Moreover, these technologies have also progressively advanced over time. Several examples of new-generation non-lethal weapons that have recently been developed include electromagnetic pulse devices that disable electrical systems, radio frequency vessel stoppers that emit high power microwaves to incapacitate vessels, focused acoustic devices, and active denial systems.[72]

Gray zone defenders should consider capitalizing on these technologies by mounting non-lethal weapons on both manned and unmanned platforms operating in the gray zone. Like unmanned platforms, non-lethal weapons seem to occupy a unique rung on the escalation ladder, given their ability to inflict temporary but sufficiently disruptive effects on individuals and platforms perpetrating gray zone activities. For instance, active denial systems produce millimeter waves that penetrate human skin up to 1/64th of an inch, creating an intense heating

[70] Richard M. O'Meara, *Governing Military Technologies in the 21st Century* (New York, NY: Palgrave Macmillan, 2014), 18.
[71] Pauline M. Kaurin, "And Next Please? The Future of the NLW Debate," *Case Western Reserve Journal of International Law* 47, no.1 (2015): 222.
[72] U.S. Department of Defense, Non-Lethal Weapons Program, accessed on 3 March 2019, https://jnlwp.defense.gov.

sensation that should generate sufficient discomfort to compel a premature halt to gray zone activities.[73] If the use of the active denial system proves inadequate, further measures can be taken with radio frequency vessel stoppers to disable naval platforms. Moreover, the use of non-lethal weapons in response to gray zone aggression shifts the burden of escalation to the aggressor. In this regard, gray zone coercers would arguably assume responsibility for further escalation if they choose to retaliate against the defenders' non-lethal measures. Non-lethal weapons should therefore play an increasingly important role in expanding the envelope of options for defenders.

While non-lethal weapons should appear intuitively preferable to lethal means, there are legitimate concerns regarding their employment. Some may argue that the term "non-lethal" could be considered disingenuous given that improper use or untoward circumstances could potentially result in fatal consequences.[74] Furthermore, in the context of the gray zone, these unintended fatalities could lead to inadvertent escalation, thereby undermining the original operational intent and impetus for non-lethal weapons. There are also ethical and legal considerations regarding the potential violation of international law by non-lethal weapons. For instance, some have argued that the active denial system can be seen as a tool that inflicts disproportionate harm on its targets.[75]

Although non-lethal weapons can indeed potentially cause serious injury or even death, their alternatives are precisely designed to inflict injury and death in *all* contexts when they are employed against human targets. Any weapon can be lethal under specific circumstances. The

[73] U.S. Department of Defense, "Active Denial Technology," Non-Lethal Weapons Program, 11 May 2016, https://jnlwp.defense.gov/Press-Room/Fact-Sheets/Article-View-Fact-sheets/Article/577989/active-denial-technology.

[74] Jean-Lou Chameau et al, *Emerging and Readily Available Technologies and National Security – A Framework for Addressing Ethical, Legal, and Societal Issues* (Washington, DC: National Academies Press, 2014), 106.

[75] Stephen Coleman, "Possible Ethical Problems with Military Use of Non-Lethal Weapons," *Case Western Reserve Journal of International Law* 47, no.1 (2015): 194.

nomenclature of non-lethal weapons arises from their design and intent to avert fatalities, and acknowledges a legitimate effort to distinguish their purpose from their lethal counterparts. Indeed, the aim of non-lethal weapons is to ensure that no lives are inadvertently lost.[76] Relatedly, the assertion that non-lethal weapons inflict disproportionate harm is rather excessive. In fact, an argument can be made that non-lethal weapons promote the fundamental human rights premise to minimize human suffering as much as possible.

Some might point to inconsistencies in the use of non-lethal weapons that belie their "benign intent," particularly if they are employed in conjunction with lethal weapons specifically to enhance the latter's effectiveness in military operations.[77] However, in the context of the gray zone, non-lethal weapons are meant as an *alternative* to lethal means given the greater risk of escalation accompanying the latter. The deployment of these non-lethal devices in gray zone disputes should therefore be interpreted as a deliberate effort to reduce the harm inflicted on the men and materiel of gray zone aggressors. Here, the employment of non-lethal weapons instead of lethal force clearly reduces the risk of escalation, even as they provide defenders with a credible option to counter aggressive incrementalism. As the philosopher Pauline Kaurin notes, non-lethal weapons are useful in deterring adversaries even as they constrain aggression and change the "trajectory of violence" so as to lower the risk of conflict.[78] Hence, non-lethal weapons should be operationally and ethically preferable for gray zone defenders.

At the same time, there are doubts as to whether such devices can legally be deployed against civilians. This concern is particularly relevant in the gray zone, where civilian militia

[76] John Alexander, "An Overview of the Future of Non-Lethal Weapons," in *The Future of Non-Lethal Weapons*, ed. Nick Lewer (Portland, OR: Frank Cass Publishers, 2002), 13.

[77] Neil Davison, *'Non-Lethal' Weapons* (London, UK: Palgrave Macmillan, 2009), 3.

[78] Pauline M. Kaurin, "With Fear and Trembling: A Qualified Defense of 'Non-Lethal' Weapons," *Journal of Military Ethics* 9, no.1 (2010): 110.

often operate in tandem with conventional military forces. While armed conflict is governed by international humanitarian law that clearly states civilians enjoy the right of being protected from attack "unless and for such time as they take a direct part in hostilities,"[79] gray zone confrontations are inherently designed to fall below the threshold of armed conflict. Thus, there is significant uncertainty as to whether engaging civilians with non-lethal weapons would be legally sanctioned.

Gray zone confrontations should not be conflated with armed conflict. Based on an analysis of Common Article 2 to the Geneva Conventions, the International Committee of the Red Cross (ICRC) expounds the view that a state of armed conflict exists only when there is either "resort to armed force" in the case of international armed conflict, or when there are "protracted armed confrontations" that reach a "minimum level of intensity" in the case of non-international armed conflicts.[80] Gray zone confrontations do not appear to meet the criteria to be considered armed conflicts, given the carefully calibrated actions of gray zone aggressors to avoid the use of force. The applicable legal framework within the gray zone should therefore be that of international human rights law rather than international humanitarian law. Under human rights law, force may be employed when it is necessary and reasonable under the circumstances.[81]

[79] International Committee of the Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (*Protocol I*), 8 June 1977, 1125 UNTS 3, https://www.refworld.org/docid/3ae6b36b4.html.

[80] International Committee of the Red Cross, "How is the Term 'Armed Conflict' Defined in International Humanitarian Law," ICRC Opinion Paper, March 2008, 5, https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf; "Geneva Convention Relative to the Protection of Civilian Persons in Time of War," 12 August 1949, 75 UNTS 287, article 2, International Committee of the Red Cross, https://www.refworld.org/docid/3ae6b36d2.html.

[81] *M/V "SAIGA" (No. 2) (Saint Vincent and the Grenadines* v. *Guinea), Judgment*, ITLOS Reports 1999, 61-63, https://www.itlos.org/fileadmin/itlos/documents/cases/case_no_2/published/C2-J-1_Jul_99.pdf.

With regard to the application of force, non-lethal weapons such as the active denial system and high frequency microwaves appear to share a similar purpose to riot control agents, which are meant to incapacitate their targets instead of killing them. While riot control agents are prohibited in armed conflict under international humanitarian law, they can be used in law enforcement efforts under the framework of international human rights law.[82] Since non-lethal weapons share similar intent and effects to that of riot-control agents, an argument can be made that non-lethal weapons should be similarly permissible, particularly in the context of gray zone confrontations. Hence, there should be no legal impediment to the use of non-lethal weapons against gray zone aggressors. Indeed, the use of such means by gray zone defenders seeking to protect international laws and norms against the corrosive effects of gray zone coercion can be somewhat likened to law enforcement actions.

Separately, the concept of mounting non-lethal weapons on unmanned vessels raises the perennial ethical and legal deliberations of the need for a human in the loop when deploying potentially autonomous weapons platforms. Much of the discussion thus far has centered on ethical concerns regarding the use of lethal autonomous weapons systems (LAWS). The U.S. DoD defines LAWS as platforms that "once activated, can select and engage targets without further intervention."[83] Examples of LAWS include the Republic of Korea's SGR-A1 sentry robots guarding the demilitarized zone with North Korea. Although these robots are remotely monitored by human operators, they have the capacity to automatically make decisions to conduct lethal engagements without human intervention.[84] The deployment of these autonomous

[82] Samuel Longuet, "Permitted for Law Enforcement Purposes but Prohibited in the Conduct of Hostilities: The Case of Riot Control Agents and Expanding Bullets," *International Review of the Red Cross* 98, no. 901 (2016): 250.
[83] U.S. Department of Defense, *Autonomy in Weapon Systems*, Department of Defense Directive (DODD) 3000.09 (Washington, DC: DoD, 21 November 2012), 13-14.
[84] Jean Kumagai, "A Robotic Sentry for Korea's Demilitarized Zone," *IEEE Spectrum*, 1 March 2007, https://spectrum.ieee.org/robotics/military-robots/a-robotic-sentry-for-koreas-demilitarized-zone.

platforms raises ethical concerns over the use of lethal force without human input, especially if these systems do not possess the requisite ethical agency that typically informs these decisions. There are also related challenges regarding responsibility and accountability for these life-and-death deliberations that normally reside with humans and cannot be easily encoded in or transferred to machines.

Based on these concerns, various organizations have imposed limits on the use of LAWS. For instance, the DoD has mandated that autonomous systems may be employed only for "non-lethal, non-kinetic force…against materiel targets."[85] Notably, the DoD directive uses the specific example of electronic warfare to underscore its key principle that autonomous platforms should not be used to target humans, even if the weapon used is non-lethal or non-kinetic. The question is whether unmanned vessels carrying non-lethal weapons are fundamentally comparable to LAWS and should therefore be deployed within similar operational boundaries.

Here, it can be contended that key ethical and operational concerns pertaining to the deployment of LAWS are not applicable to non-lethal systems. As discussed, a non-lethal weapon should be viewed as operationally and ethically distinct from its lethal counterpart. It is worth reiterating that non-lethal weapons are ethically preferable given that they are designed and purposed precisely to avoid inflicting fatalities and causing unnecessary or disproportionate harm. The intent of non-lethal weapons distinguishes them from their lethal counterparts, and arguably makes non-lethal means an ethically superior option for a gray zone defender. Moreover, the use of non-lethal weapons in the context of the maritime gray zone – outside the domain of armed conflict – is permitted under international human rights law. The legal, ethical,

[85] U.S. Department of Defense, *Autonomy in Weapon Systems*, 3.

and operational considerations that influence the deployment of LAWS are therefore significantly distinct from the use of non-lethal weapons.

Notwithstanding these differences, having a human in the loop is still desirable given the inherent ambiguity of gray zone interactions and the overarching consideration of avoiding further escalation. Specifically, although gray zone defenders can consider allowing unmanned vessels to maneuver autonomously, they should retain direct human control over the decision to operate non-lethal weapons. The considerations with regard to employing autonomous non-lethal systems are therefore more operational than ethical in nature. In sum, non-lethal weapons present a viable means from the ethical, legal and operational perspectives for gray zone defenders to impose costs on their adversaries and shift the burden of escalation back to their adversaries.

Broadening Conflict Domains

At the same time, gray zone defenders can broaden the dimensions of the physical dispute to the cyber-information domain, giving them additional credible options to impose costs on their gray zone adversaries while diminishing the risk of escalation. Here, AI-based facial recognition tools can be used to expose the identities of individual perpetrators of gray zone coercion, along with their respective affiliations with specific states and organizations. The deterrent effect is achieved primarily when gray zone activities and their perpetrators are named and shamed to impose reputational costs. This tactic would be especially effective when applied against revisionist states seeking an alteration to the status quo without incurring international censure for their actions. In this regard, gray zone aggression can be effectively deterred by lifting the fog of ambiguity surrounding gray zone operations and digitally unmasking their perpetrators. A real-world example here is the use of social media by individuals and nongovernmental organizations to identify non-uniformed Russian “little green men” illegally entering the Ukraine in 2015. By matching the social media accounts with known military personnel, these non-state actors were able to expose Russian duplicity by positively identifying the “little green men” as soldiers, thereby imposing reputational costs on the Russian government and undermining their credibility.[86]

However, the use of AI takes the imposition of reputational costs to the next level and significantly enhances its deterrent effect. For instance, while the United States’ 2018 National Defense Authorization Act directs the Pentagon to “immediately” report on escalatory Chinese activities in the South China Sea, this process inevitably takes time, with the delay likely diluting the reputational impact to the gray zone aggressor. [87] In contrast, the real-time identification of gray zone perpetrators allows defenders to impose direct and instantaneous reputational costs. The deterrence by denial effect is heightened by the defenders’ ability to impose costs that are unambiguously linked to the time and place of the specific gray zone activity. Here, facial recognition software augmented with machine learning algorithms can be used to trawl through openly available social media profiles and establish the individual identities of gray zone perpetrators in real-time. Essentially, algorithms are able to compare images captured in the midst of gray zone confrontations, detect human features within those images, and compare them to a database of faces that can be compiled from open source social media.

Such technology is already openly available, with technology companies such as Google, Facebook, and Amazon developing sophisticated image and video analysis algorithms that can parse the voluminous amounts of data present on social media networks to identify specific

[86] John Schaus et al., “What Works: Countering Gray Zone Coercion,” *CSIS Briefs,* 16 July 2018, https://www.csis.org/analysis/what-works-countering-gray-zone-coercion.
[87] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law 115-232, 115th Cong., 2d sess. 2018, §1262(a).

individuals. Certain deep-learning algorithms are sufficiently advanced to the extent that they are even able to match concealed visages with significant accuracy.[88] Such technologies would indeed go a long way toward helping unmask gray zone entities.

AI-powered cyber-information measures inevitably raise ethical and legal concerns with regard to its use as a tool to impose expected costs on gray zone coercers and influence their decision-making processes. Here, the status of cyber-information warfare with regard to its standing under international law is complicated by the inherent lack of physical conflict and resulting damage.[89] Exposing and broadcasting individual identities in the cyber-information domain would however certainly have a disruptive impact on the lives of the individuals involved, particularly their individual privacy. Without further clarity, the ethical implications of such actions are ambiguous and would potentially undermine the legitimacy of gray zone defenders adopting such measures. In addition, these concerns are exacerbated by facial-recognition algorithms being prone to biases inherent in the data that hinder the accurate identification of individuals.[90] This deficiency could potentially lead to the misidentification of gray zone perpetrators, consequently risking the degradation of these deterrence measures into ethically questionable "trolling" that undermines the ethical and legal legitimacy of these deterrent measures.

In considering these potential legal and ethical drawbacks, one must first seek to define the boundaries of the debate given the significant scope of the cyber-information domain. After all, cyber-information exploitation not only includes the propagation of (dis)information but also

[88] CBInsights, "AI-Driven Facial Recognition Is Coming And Brings Big Ethics And Privacy Concerns," CB Information Services Research Brief, accessed 13 March 2019, https://www.cbinsights.com/research/facial-recognition-privacy-ai.

[89] Patrick Lin et al, "Is Warfare the Right Frame for the Cyber Debate?" in *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo (Springer International Publishing, 2014), 40-44.

[90] Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy," *New York Times*, 9 February 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

includes cyberattacks that seek to damage computer systems or networks and the information residing in them. In this context, the latter falls outside the scope of this discussion given the limited nature of the proposed measures, which focus on information-centric broadcasts rather than attacks on cyber-infrastructure or data contained therein. In addition, the boundaries of the proposed measures are constrained to the exploitation of open-source information residing in social networks, without resort to nefarious means to misappropriate personal data. This qualification limits possible legal or ethical objections with regard to the exploitation of private data given that the information has been openly shared by the individuals on publicly accessible networks.

Separately, one can contend that the exploitation of openly accessible data to propagate accurate information is ethically viable regardless of the legal status of informational warfare in the cyber domain. Specifically, there should be no real ethical concerns regarding the real-time identification of gray zone perpetrators using open-source data. The exposure of gray zone perpetrators simply by open-source collection should not raise any undue concerns in the first place, unless the highlighted activities are either illegal or unethical. For instance, there are typically no undue sensitivities raised when servicemen of various countries are identified in photographs or video recordings in the midst of a conventional military exercise or maneuver, unless there are valid concerns about operational security. In this context, the illegitimate nature of maritime gray zone activities necessitates hiding behind a cloak of anonymity especially in the undertaking of dangerous or aggressive actions against gray zone defenders. Indeed, on top of the strategic and operational necessity to push back against gray zone coercion, it can be viewed as an ethical imperative to unmask gray zone perpetrators in order to disrupt illicit activities undermining the sanctity of international rules and norms meant to protect lives at sea. The example that comes to mind here is the interaction between the *Decatur* and the *Lanzhou,* which could potentially have led to the loss of life as a result of poor seamanship and dangerous maneuvers on the part of the latter.

The legal and ethical considerations of violating the right to privacy are perhaps more salient when perpetrators are erroneously identified. In this regard, the quality of the data that is used to train the algorithm is of utmost importance to avoid the pitfall of misidentification. Here, the main factor behind biased algorithms is the lack of racial and gender diversity in the data sets they are trained on, which also often reflects the homogeneity inherent in the algorithm's development team.[91] As a result, unintentional biases can be introduced at multiple points, whether in the algorithm's design to focus on specific facial features that are more prominent in certain ethnicities, or within the training dataset that could be overly representative of some races over others.[92]

In light of these potential deficiencies, the dataset used to identify gray zone perpetrators should be specific to the ethnicity and race of the adversary in question in order to reduce the risk of misidentification. The team developing the facial recognition algorithm must be familiar with the unique facial features and characteristics of the gray zone perpetrators, and adapt the algorithmic parameters accordingly. Moreover, there should be a human in the loop to make the final decision in determining if there is indeed a match in order to mitigate the risk of misidentification. A study by the National Institute of Standards and Technology in the U.S. found that human facial recognition experts were able to achieve their best results by working

[91] Clare Garvie and Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," The Atlantic, 7 April 2016, https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991.
[92] Lohr, "Facial Recognition."

with AI algorithms.[93] In this regard, these facial recognition algorithms should be employed as a collaborative tool that would not only enhance the operational effectiveness of facial recognition and identification efforts, but also mitigate valid ethical and operational concerns arising from the misidentification of individuals.

In sum, the use of AI and non-lethal technologies can be used to impose expected costs on gray zone practitioners that will alter their risk-reward calculus, thereby shifting the burden of escalation back to the aggressors and forcing them to reconsider the use of gray zone tactics to achieve their goals. While there are valid ethical, legal, and operational concerns in relation to the employment of these technologies, the discourse above has elucidated why their use is viable, with proposed measures to mitigate potential pitfalls that could hinder their deployment. The inhibition of incrementalism is indeed a conceptual cornerstone of a deterrence by denial framework designed to discourage the initiation of gray zone aggression, with emerging technologies playing a key role as important enablers.

[93] P. Jonathon Phillips et al, "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," *Proceedings of the National Academy of Sciences* 115, no.24 (June 2018): 6171.

V. CONCLUSION

Judging by the increasing prevalence of gray zone activity and their effectiveness, modern-day gray zone provocateurs are certainly poised to become Sun Tzu's most accomplished acolytes. However, buoyed by their success in making significant strategic strides, they risk forgetting that their adversaries get a vote, even if it is late in coming. Indeed, gray zone defenders are certainly not helpless. The critical requirements for the success of gray zone tactics – ambiguity, asymmetry, and incrementalism – can be addressed with the use of emerging technologies to impose expected costs where there were previously none. Most importantly, the burden of escalation can be shifted back to the aggressors in a bid to alter the latter's risk calculus and force them to reconsider their intentions and activities.

Notwithstanding the benefits emerging technologies bring, the key to parrying the probes of gray zone coercion does not lie in merely developing counter-tactics that employ more advanced means. Rather, any response to gray zone incursions must fundamentally seek to reinforce the laws and norms that underpin the international order in order to expose these stratagems and render them counter-productive.[94] Sober consideration of the ethical and legal implications of technological means used to strengthen deterrence against gray zone aggression is itself a strong signal that gray zone defenders are serious about adhering to international laws and norms. In doing so, they cement the fundamental cornerstones of the liberal international order, which is perhaps the strongest defense against gray zone aggression. Indeed, by complementing these essential efforts with emerging technologies that lift the fog of ambiguity,

[94] Michael Mazarr, "Struggle in the Gray Zone and World Order," War on the Rocks, December 22 2015, https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order.

address asymmetric interests, and inhibit incremental gray tactics, defenders can successfully deter their adversaries and give themselves, and the liberal international order, a fighting chance.

BIBLIOGRAPHY

Agrawal, Ajay, Joshua Gans and Avi Goldfarb. *Prediction Machines: The Simple Economics of Artificial Intelligence*. Boston, MA: Harvard Business Review Press, 2018.

Alexander, John. “An Overview of the Future of Non-Lethal Weapons.” In *The Future of Non-Lethal Weapons*. Edited by Nick Lewer. Portland, OR: Frank Cass Publishers, 2002.

Barno, David and Nora Bensahel. “Fighting and Winning in the ‘Gray Zone’.” War on the Rocks. May 19 2015. https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone.

Bateman, Sam. “UNCLOS and Its Limitations as the Foundation for a Regional Maritime Security Regime.” *The Korean Journal of Defense Analysis* 19, no. 3 (2007): 27-56.

Beckman, Robert. “The UN Convention on the Law of the Sea and the Maritime Disputes in the South China Sea.” *The American Journal of International Law* 107, no.1 (Jan 2013): 142-163.

Brands, Hal. “Paradoxes of the Gray Zone.” *FPRI E-Note*. Foreign Policy Research Institute. February 5, 2016. https://www.fpri.org/article/2016/02/paradoxes-gray-zone.

Brands, Hal and Zack Cooper. “Getting Serious About Strategy in the South China Sea.” *Naval War College Review* 71, no.1 (Winter 2018): 13-32.

Buchanan, Ben and Taylor Miller. *Machine Learning for Policymakers*. Belfer Center for Science and International Affairs. June 2017. https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf.

CBInsights. “AI-Driven Facial Recognition Is Coming And Brings Big Ethics And Privacy Concerns.” CB Information Services Research Brief. Accessed 13 March 2019. https://www.cbinsights.com/research/facial-recognition-privacy-ai.

Chameau, Jean-Lou, William F. Ballhaus, and Herbert S. Lin. *Emerging and Readily Available Technologies and National Security – A Framework for Addressing Ethical, Legal, and Societal Issues.* Washington, DC: National Academies Press, 2014.

Chang, Amy, Ben FitzGerald and Van Jackson. *Shades of Gray: Technology, Strategic Competition, and Stability in Maritime Asia*. Washington, DC: Center for New American Security, 2015.

Cheney-Peters, Scott. "A Feast of Cabbage and Salami: Part I – The Vocabulary of Asian Maritime Disputes." Center for International Maritime Security. 29 October 2014. http://cimsec.org/feast-cabbage-salami-part-vocabulary-asian-maritime-disputes/13441.

Clark, Bryan, Mark Gunzinger and Jesse Sloman. *Winning in the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance*. CSBA Report. Washington, DC: CSBA, 2017.

Clausewitz, Carl Von. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Coleman, Stephen. "Possible Ethical Problems with Military Use of Non-Lethal Weapons." *Case Western Reserve Journal of International Law* 47, no.1 (2015): 185-199.

Davenport, Christian. "Future Wars May Depend as much on Algorithms as on Ammunition, report says: Pentagon boosts spending on artificial intelligence, big data and powerful computers." *Washington Post*. 3 December 2017. ProQuest (1971618030).

Davenport, Thomas H. and Rajeev Ronanki. "Artificial Intelligence for the Real World." *Harvard Business Review*. January-February 2018. https://hbr.org/2018/01/artificial-intelligence-for-the-real-world.

Davison, Neil. *'Non-Lethal' Weapons*. London, UK: Palgrave Macmillan, 2009.

Erickson, Andrew S. and Ryan D. Martinson. "Introduction. "War Without Gunsmoke." In *China's Maritime Gray Zone Operations*. Edited by Andrew S. Erickson and Ryan D. Martinson. Annapolis, MD: Naval Institute Press, 2019.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York, NY: Pantheon Books, 1977.

Garvie, Clare and Jonathan Frankle. “Facial-Recognition Software Might Have a Racial Bias Problem.” The Atlantic. 7 April 2016. https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991.

“Geneva Convention Relative to the Protection of Civilian Persons in Time of War.” 12 August 1949. 75 UNTS 287. International Committee of the Red Cross. https://www.refworld.org/docid/3ae6b36d2.html.

Green, Michael, Kathleen Hicks, Zack Cooper, John Schaus and Jake Douglas. *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*. Washington, DC: Center for Strategic & International Studies, 2017.

Gunning, David. “Explainable Artificial Intelligence.” Defense Advanced Research Projects Agency. https://www.darpa.mil/program/explainable-artificial-intelligence.

Harkins, Gina. “A Navy Ship Sailed to Hawaii and Back with No One on Board.” Military.com. 15 February 2019. https://www.military.com/defensetech/2019/02/15/navy-ship-sailed-hawaii-and-back-no-one-board.html.

Henckaerts, Jean-Marie. “Study on Customary International Humanitarian Law: A contribution to the understanding and respect for the rule of law in armed conflict.” *International Review of the Red Cross* 87, no.857 (March 2005): 175-212.

Hoffman, Frank. “On Not-So-New Warfare: Political Warfare vs Hybrid Threats.” War on the Rocks. 28 July 2014. https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats.

Holmes, James R. “The Return of China’s Small-Stick Diplomacy in South China Sea.” *The Diplomat*. 9 January 2014. https://thediplomat.com/2014/01/the-return-of-chinas-small-stick-diplomacy-in-south-china-sea.

Holmes, James and Toshi Yoshihara, “Deterring China in the ‘Gray Zone’: Lesson of the South China Sea for U.S. Alliances.” *Orbis* 61, no.3 (2017): 322-339.

https://www.sciencedirect.com/science/article/pii/S003043871730042X.

International Committee of the Red Cross. “How is the Term ‘Armed Conflict’ Defined in International Humanitarian Law.” ICRC Opinion Paper. March 2008. https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf.

______*Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (*Protocol I*). 8 June 1977. 1125 UNTS 3. https://www.refworld.org/docid/3ae6b36b4.html.

Kapusta, Philip. "The Gray Zone." *Special Warfare* 28, no.4 (Oct, 2015): 18-25. ProQuest Central (1750033789).

Kaurin, Pauline M. “And Next Please? The Future of the NLW Debate.” *Case Western Reserve Journal of International Law* 47, no.1 (2015): 217-227.

______“With Fear and Trembling: A Qualified Defense of ‘Non-Lethal’ Weapons.” *Journal of Military Ethics* 9, no.1 (2010): 100-114.

Kissinger, Henry A. *The Necessity for Choice: Prospects of American Foreign Policy*. New York, NY: Harper, 1961.

Kraska, James. “The Law of the Sea Convention: A National Security Success – Global Strategic Mobility Through the Rule of Law.” *The George Washington International Law Review* 39, no.3 (2007): 543-572.

Kumagai, Jean. “A Robotic Sentry for Korea’s Demilitarized Zone.” *IEEE Spectrum*. 1 March 2007. https://spectrum.ieee.org/robotics/military-robots/a-robotic-sentry-for-koreas-demilitarized-zone.

Lin, Patrick, Fritz Allhoff and Keith Abney. “Is Warfare the Right Frame for the Cyber Debate?” In *The Ethics of Information Warfare*, edited by Luciano Floridi and Mariarosaria Taddeo. Springer International Publishing, 2014.

Lohr, Steve. “Facial Recognition Is Accurate, if You’re a White Guy.” *New York Times*. 9 February 2018. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

Longuet, Samuel. “Permitted for Law Enforcement Purposes but Prohibited in the Conduct of Hostilities: The Case of Riot Control Agents and Expanding Bullets.” *International Review of the Red Cross* 98, no. 901 (2016): 249-274.

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

______“Struggle in the Gray Zone and World Order.” War on the Rocks. December 22 2015. https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order.

Mitchell, A. Wess. “The Case for Deterrence by Denial.” *The American Interest*. 12 August 2015. https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial.

National Security Innovations. “Panel Discussion on the Gray Zone.” Strategic Multi-Layer Assessment Report. 27 April 2017. http://nsiteam.com/social/wp-content/uploads/2017/06/U_Final_SMA_SOCOM-Gray-Zone-Panel-Discussion-v2.pdf.

O’Meara, Richard M. *Governing Military Technologies in the 21st Century*. New York, NY: Palgrave Macmillan, 2014.

Panda, Ankit. “Japan to Shoot Down Foreign Drones.” *The Diplomat*. 22 October 2013. https://thediplomat.com/2013/10/japan-to-shoot-down-foreign-drones.

Petersen, Michael B. “The Chinese Maritime Gray Zone: Definitions, Dangers, and the Complications of Rights Protection Operations.” In *China’s Maritime Gray Zone Operations*. Edited by Andrew S. Erickson and Ryan D. Martinson. Annapolis, MD: Naval Institute Press, 2019.

Phillips, P. Jonathon, Amy N. Yates, Ying Hu, Carina A. Hahn, Eilid Noyes, Kelsey Jackson, Jacqueline G. Cavazos, Geraldine Jeckeln, Rajeev Rajan, Swami Sankaranarayanan, Jun-Cheng Chen, Carlos D. Castillo, Rama Chellappa, David White and Alice J. O’Toole. “Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms." *Proceedings of the National Academy of Sciences* 115, no.24 (June 2018): 6171-6176.

Sander, Alexandra. "Game of Drones: Wargame Report." Center for a New American Security. 29 June 2016. http://drones.cnas.org/reports/game-of-drones.

Schadlow, Nadia. "Peace and War: The Space Between." War on the Rocks. August 18 2014. https://warontherocks.com/2014/08/peace-and-war-the-space-between.

Scharre, Paul. "The Coming Drone Wars: A Headache in the Making for American Foreign Policy." The National Interest. 25 July 2017. https://www.cnas.org/publications/commentary/the-coming-drone-wars-a-headache-in-the-making-for-american-foreign-policy.

Schaus, John, Michael Matlaga, Kathleen H. Hicks, Heather A. Conley and Jeffrey Rathke. "What Works: Countering Gray Zone Coercion." *CSIS Briefs.* 16 July 2018. https://www.csis.org/analysis/what-works-countering-gray-zone-coercion.

Schelling, Thomas. *Arms and Influence.* New Haven, CT: Yale University Press, 1966.

Snyder, Glenn H. *Deterrence and Defense*. Princeton, NJ: Princeton University Press, 1961.

South, Todd. "DARPA to use artificial intelligence to help commanders in 'gray zone' conflicts." *Army Times*. 27 March 2018. https://www.armytimes.com/news/your-army/2018/03/27/darpa-to-use-artificial-intelligence-to-help-commanders-in-gray-zone-conflicts.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

U.S. Department of Defense. "Active Denial Technology." Non-Lethal Weapons Program. 11 May 2016. https://jnlwp.defense.gov/Press-Room/Fact-Sheets/Article-View-Fact-sheets/Article/577989/active-denial-technology.

______ *Autonomy in Weapon Systems.* Department of Defense Directive (DODD) 3000.09. Washington, DC: DoD. 21 November 2012.

______*Capabilities for Constrained Military Operations*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Defense Science Board, December 2016.

______Non-Lethal Weapons Program. Accessed on 3 March 2019. https://jnlwp.defense.gov.

______*Summary of the 2018 Department of Defense Artificial Intelligence Strategy*. Washington, DC: Office of the Secretary of Defense, 2019.

U.S. Department of State. *Report on Gray Zone Conflict*. ISAB Study. 3 January 2017. https://www.state.gov/t/avc/isab/266650.htm.

U.S. Government Accountability Office. *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications.* Washington, DC: GAO, March 2018.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Space Operations*. Joint Publication (JP) 3-14. Washington, DC: CJCS, 10 April 2018.

West, Darrell M. and John R. Allen. “How artificial intelligence is transforming the world.” Brookings. 24 April 2018. https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world.