1-1-2018

Maritime Gray Zones

Center on Irregular Warfare & Armed Groups

Center on Irregular Warfare and Armed Groups Reading List 2018-2019

Maritime Gray Zones

These articles and associated links are provided as items of general interest and are made available for the purpose of peer review and discussion, as well as to promote critical thinking. This document is primarily produced for educational purposes for courses taught by CIWAG faculty. Selection of articles should not be construed as an explicit or implicit endorsement of particular publications, or the authors' or publishers' views or interpretations. They do not necessarily represent the views of the Department of Defense, the Naval War College, or CIWAG. The links embedded within this PDF may direct you to websites not controlled by the Naval War College or the Department of Defense and should not be construed as endorsements of those websites. Any questions should be directed to ciwag@usnwc.edu.

DOCUMENT DISCLAIMERS

Unclassified Disclaimer:

Articles, references, and links are unclassified and for information purposes only, and are provided for the convenience of the reader. Such references do not necessarily represent the views of the Naval War College, Department of Defense, or CIWAG.

Document Inquiries:

For inquiries regarding this document contact the Center on Irregular Warfare and Armed Groups at the U.S. Naval War College, Newport RI. ciwag@usnwc.edu.

Maritime Gray Zones

Table of Contents

"The Cold War was a 45-year-long Gray Zone Struggle."[1] – General Joseph L. Votel

I. Core Concepts

GRAY ZONES

Lohaus, Phillip. "A New Blueprint for Competing Below the Threshold: The Joint Concept for Integrated Campaigning." War on the Rocks. May 23, 2018. https://warontherocks.com/2018/05/a-new-blueprint-for-competing-below-the-threshold-the-joint-concept-for-integrated-campaigning/.

The JCIC was designed to solve a specific problem: how to apply the power of the American military when adversarial behavior falls below the threshold that would trigger a direct response. While the global distribution of America's joint force positions it well to contribute to broader government strategies in the space "short of war," such activities have mostly been limited to the domain of special operations forces. The JCIC marks an important step toward improving the ability of the entire military to contribute to international competition outside of combat.

Dubik, James M., Nic Vincent. "America's Global Competitions: The Gray Zone in Context." Institute for the Study of War. February 2018. http://www.understandingwar.org/report/americas-global-competitions-gray-zone-context.

The actions that the leading powers must take to help resolve the competition with revisionists, the war with the revolutionaries, and chronic crises with the rogue are a key determinant of which future ultimately emerges. The United States must redirect itself, for currently it is not intellectually or organizationally in the right position and it is not leading sufficiently enough.

Kay, Larry. "Managing the Gray Zone is a Gray Matter Challenge." *Small Wars Journal*, July 27, 2016. http://smallwarsjournal.com/jrnl/art/managing-the-gray-zone-is-a-gray-matterchallenge.

Due to the unclear or "gray" nature of the problems and subsequent solutions, the U.S. is uncertain how to respond. Much of our focus thus far has been to address these problems as we have in the past in other unconventional conflicts, however, our methodologies, our cultural paradigms, and institutional habits inhibit our ability to create solutions other than those that we have used to address past problems. This

[1] General Joseph L. Votel, USA, Lieutenant General Charles T. Cleveland, USA (Ret.) and Will Irwin. "Unconventional Warfare in the Gray Zone." JFQ 80, (1st Quarter, 2016). National Defense University Press, 102. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/643108/unconventional-warfare-in-the-gray-zone/

paper promotes an alternative approach, which is to adopt a generative or systemic solution to ways in which to develop strategies to manage gray zone competitions by adapting officer career and education tracks to create a more operationally and intellectually excellent officer corps.

Freier, Nathan P., Charles R. Burnett, William J. Cain, Jr., Christopher D. Compton, Sean M. Hankard, Robert S. Hume, Gary R. Kramlich, II, J. Matthew Lissner, Tobin A. Magsig, Daniel E. Mouton, Michael S. Muztafago, James M. Schultze, John F. Troxell, and Dennis G. Wille. Outplayed: Regaining Strategic Initiative in the Gray Zone. U.S. Army War College Press, 2016. June 7, 2016. http://strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1325.

It is in this "gray zone" – the awkward and uncomfortable space between traditional conceptions of war and peace – where the United States and its defense enterprise face systemic challenges to U.S. position and authority. Gray zone competition and conflict present fundamental challenges to U.S. and partner security and, consequently, should be important pacers for U.S. defense strategy.

Echevarria II, Dr. Antulio J. *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*. U.S. Army War College Press, 2016. April 4, 2016. http://strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1318.

Recent events in Ukraine, Syria, Iraq, and the South China Sea continue to take interesting, if not surprising, turns. As a result, many security experts are calling for revolutionary measures to address what they wrongly perceive to be a new form of warfare, called "hybrid" or "gray zone" wars, but which is, in fact, an application of classic coercive strategies. These strategies, enhanced by evolving technologies, have exploited a number of weaknesses in the West's security structures. To remedy one of those weaknesses, namely, the lack of an appropriate planning framework, this monograph suggests a way to re-center the current U.S. campaign-planning paradigm to make it more relevant to contemporary uses of coercive strategies.

Brands, Hal. "Paradoxes of the Gray Zone." Foreign Policy Research Institute. February 5, 2016. http://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Contrary to what skeptics argue, then, the gray zone is not an illusion. But if the concept does pack a punch, it is also elusive and even paradoxical. Edward Luttwak has written about the paradoxical logic of strategy – the fact that it seems to embody multiple, and seemingly contradictory, truths at once. In dealing with the gray zone, this basic proposition applies in spades. The gray zone concept may seem relatively straightforward at first glance. But upon closer inspection, it is fraught with complexities, contradictions, and ironies. These characteristics do not make the concept worthless or meaningless. They do, however, make it quite slippery.

Votel, General Joseph L. USA, Lieutenant General Charles T. Cleveland, USA (Ret.) and Will Irwin. "Unconventional Warfare in the Gray Zone." *Joint Force Quarterly* no. 80 (January, 2016). National Defense University Press. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf

Unconventional warfare, whether conducted by the United States or Russia or any other state seeking to advance national interests through Gray Zone proxy warfare, has a rich history but continues to evolve to meet changing global conditions. One certainty in a world of continuing disorder, a world bereft of Cold War clarity and relative "stability," where globalization has enabled almost continuous change, is that the UW mission must continue to adapt and so must those responsible for executing it.

Mazarr, Michael J. "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/.

The real significance of gray zone campaigns is in their relation to the most fundamental challenge of the coming decades: finding a way to integrate rising, quasi-revisionist powers into the international order. Our inability to do so is the basis for gray zone conflict; progress in that direction would make such campaigns less necessary and less worrisome.

Kapusta, CAPT. Philip. "The Gray Zone" *Special Warfare* 28 no. 4 (October-December 2015): 18-25. October 2015. http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf

The ambiguity making gray zones so vexing also makes them useful to statesmen. In fact, they are crucial to the conduct of international relations in defining the importance of situations to the parties involved. That is, states and non-states can 'test the waters' with gray zone activities to determine the relative strength of domestic and international commitment to an endeavor without resorting to the more lethal violence of war. In brief, gray zone conflicts are an immensely better alternative to full-scale wars.

HYBRID WARFARE

Kremidas-Courtney, Chris. "Countering Hybrid Threats in the Maritime Environment." Center for International Maritime Security. June 11, 2018. http://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/36553.

Of course, these threats have always existed, but what makes hybrid threats different are the new vulnerabilities presented by a globalized world interconnected by instant

global communications, systems of finance, and commerce. Hybrid threats represent the weaponization of globalization.

Cullen, Patrick. "Strategic Analysis May 2018: Hybrid Threats as a New 'Wicked Problem' for Early Warning." June 4, 2018. https://www.hybridcoe.fi/publication-tags/strategic-analysis/.

Hybrid threats are designed to blur the distinction between peace and war, as well as complicate and fall below the target's detection and response thresholds. The wicked problems created by hybrid threats require new solutions for early warning.

Wither, James K. "Making Sense of Hybrid Warfare." *Connections: The Quarterly Journal* 15, no. 2 (Spring 2016): 73-87. http://search.proquest.com/docview/1784582336?accountid=322.

The term hybrid warfare has been widely analyzed by scholars, policymakers and commentators since Russia occupied Crimea in March 2014. The topic has ceased to be a subject only studied by military strategists, but has entered the wider policy domain as a significant security challenge for the West. This article seeks to place the debate about hybrid warfare in a broader analytical and historical context and summarizes discussion to date on this and related strategic concepts. The Russian approach to hybrid warfare as demonstrated by operations in Ukraine is a particular focus for discussion.

Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007. December 2007. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Because of their perceived success, hybrid challenges will not be a passing fad nor will they remain focused on low tech applications. Future opponents will be dedicated, learn rapidly and adapt quickly to more efficient modes of killing. The ongoing Long War underscores their capacity for incorporating new tactics, techniques and procedures. This diffusion will continue. We can no longer overlook our own vulnerabilities or underestimate the imaginations of our antagonists. In the world of Hybrid Wars, the price for complacency grows steep.

CYBER

Stoltenberg, Jens. "How NATO Defends Against the Dark Side of the Web." *WIRED*, June 9, 2018. https://www.wired.com/story/how-nato-defends-against-the-dark-side-of-the-web/.

For almost 70 years, NATO has been the bedrock of transatlantic security, whether on land, at sea, or in the air. The same is now true in cyberspace. A cyberattack can now

trigger Article 5 of NATO'S founding treaty, which states that an attack on one Ally is an attack on all Allies.

Barker, Pete. "Undersea Cables and the Challenges of Protecting Seabed Lines of Communication." CIMSEC. March 15, 2018. http://cimsec.org/undersea-cables-challenges-protecting-seabed-lines-communication/35889.

Strategists have neglected submarine cables. Whilst topics such as piracy and cyber attacks on ports frequently arise in discussions on maritime threats, cables have not always been as prominent. Some authors have identified the potential risks (such as this 2009 report for the UN Environment World Conservation Monitoring Centre), but these works have not always received the attention they deserve.

Howard, Travis, and José De Arimatéia Da Cruz. "A Cyber Vulnerability Assessment of the U.S. Navy in the 21st Century." CIMSEC. January 31, 2017. http://cimsec.org/cyber-vulnerability-assessment-u-s-navy-21st-century/30405.

With over 320,000 active duty personnel, 274 ships with over 20 percent of them deployed across the world at any one time, the Navy's ability to securely communicate across the globe to its forces is crucial to its mission. In this age of rapid technological growth and the ever expanding internet of things, information security is a primary consideration in the minds of senior leadership of every global organization. The Navy is no different, and success or failure impacts far more than a stock price.

Malekos Smith, Jessica. "Twilight Zone Conflicts: Employing Gray Tactics in Cyber Operations." *Small Wars Journal*, October 27, 2016. http://smallwarsjournal.com/jrnl/art/twilight-zone-conflicts-employing-gray-tactics-in-cyber-operations.

In an opening that would perhaps make Rod Serling proud: There is a fifth dimension of warfare known to man as cyberspace – it is a dimension of infinite possibilities, representing an uncertain middle ground between peace and war. An amorphous realm, wherein actors are strategically employing gray tactics via cyber operations in 'twilight zone conflicts.' And while gray tactics like information operations, sabotage and economic coercion are not new to the pages of history, the medium for leveraging such tactics is.

Thiele, Ralph D. "Game Changer – Cyber Security in the Naval Domain." *ISPSW Strategy Series: Focus on Defense and International Security*, no. 530 (January 2018). http://www.ispsw.com/wp-content/uploads/2018/01/530_Thiele.pdf.

The systems and networks naval forces must protect are complex and large in size. Ships are increasingly using systems that rely on digitization, integration, and automation.

Offensive actors understand the naval reliance on communications, ISR, and visualization technologies, and perceive them as vulnerable to disruption and exploitation. Cyber has been moving from a supportive to a rather active role within an operational force. With today's rapidly evolving threats, naval forces are well advised to develop a sense of urgency not only to develop cyber resilience capabilities that will enable them to "fight through", but also cyber warfighting capabilities as these will be particularly valuable when they can be delivered reliably and in concert with other capabilities.

Kruithof, Kristy, Judith Aldridge, David Decary Hetu, Megan Sim, Elma Dujso, and Stijn Hoorens. "Internet-Facilitated Drug Trade." RAND. August 2016. http://www.rand.org/pubs/research_reports/RR1607.html

This report analyses the size and scope of Internet-facilitated drugs trade both on the so-called clear and hidden web, paying special attention to the Netherlands, and delineates potential avenues for law enforcement for detection and intervention.

Russell, Alison Lawlor. *Cyber Blockades*. Georgetown University Press, 2014.

Cyber Blockades is the first book to examine the phenomena of blockade operations in cyberspace, large-scale attacks on infrastructure or systems that aim to prevent an entire state from sending or receiving electronic data. Cyber blockades can take place through digital, physical, and/or electromagnetic means. Blockade operations have historically been considered acts of war, thus their emergence in cyberspace has significant implications for international law and for our understanding of cyber warfare.

DIS/INFORMATION CAMPAIGNS

Gordon, Daniel. "Defending the Indefensible: A New Strategy for Stopping Information Operations." War on the Rocks. May 25, 2018. https://warontherocks.com/2018/05/defending-the-indefensible-a-new-strategy-for-stopping-information-operations/.

We can apply the Centers for Disease Control and Prevention (CDC) strategies for combating emerging epidemics to contain the spread of viral information and reduce the effectiveness of information operations. The CDC's strategies include educating the public, training responding personnel, using science and technology to understand transmission and treatment, and identifying specific areas in need of additional resources. That's right, the CDC isn't just for stopping zombie outbreaks. Its recommendations for containing emerging epidemics can help fill the gaps in, and improve effectiveness of, the response to information operations.

CYBER LAW

Schmitt, Michael N., and Liis Vihul, eds. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

The fact that international law is often dismissed as window-dressing on realpolitik is misleading. Such an approach understates the importance of international agreements in maintaining peace and security. For liberal democracies that respect the rule of law, international law undoubtedly shapes and bounds governments. Activities. At a time when the actions of unscrupulous States and violent extremist groups continue to threaten peace and security internationally, it is even more important that such actions are countered with a strong commitment to existing international law and the values that it represents.

Gerstein, Daniel M. "Define Acceptable Cyberspace Behavior." *The RAND Blog* (blog), September 27, 2015. https://www.rand.org/blog/2015/09/define-acceptable-cyberspace-behavior.html.

While a U.S.-China agreement is a welcome step, it also underscores the greater issues facing the United States, and indeed the international community, in this largely ungoverned space. It further highlights that a precondition for securing U.S. networks should be the development of an overarching cyber doctrine that defines the limits of acceptable behavior and allows the U.S. to defend its networks against current and future threats.

Schmitt, Michael N. "The Law of Cyber Targeting." *Naval War College Review* 68 no. 2(Spring, 2015). https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_07_2015.pdf.

In light of the role which cyber operations are playing in contemporary conflicts, attention must be paid to the law that governs these activities because, to borrow a sports analogy, a team that takes the field without knowing the rules is usually going to lose, even if it is the better team. International law, and particularly IHL, exerts a powerful influence on tactics, operational planning and strategic decision-making in modern warfare. The fight can be won on the battlefield but lost in the court of public and international opinion when one side appears to have acted outside the law. Given the novelty of cyber operations as a method of warfare during an armed conflict, any alleged misuse, even at the tactical level, has the potential for strategic consequences.

II. Maritime Gray Zones by Country

RUSSIA

GRAY ZONE STRATEGY

Kabanenko, Ihor. "Russian Naval Exercises in Sea of Azov: A Prelude to 'Hybrid'-Style Invasion?" *Eurasia Daily Monitor* 15, no. 78 (May 22, 2018). May 22, 2018.

https://jamestown.org/program/russian-naval-exercises-in-sea-of-azov-a-prelude-to-hybrid-style-invasion/.

On May 18, Moscow released a navigation alert for a section of the Sea of Azov, cautioning that Russian naval training exercises would make the area dangerous for maritime passage from 0500 to 1700 UTC, on May 21–23. The zone, which occupies 2,000 square kilometers, has been closed to shipping traffic. Though the announcement quickly drew the attention of Ukrainian news outlets, the Russian state media has so far kept silent.

Aliyev, Nurlan. "Russian Military Presence in Caspian Sea: Protection of National Interests or Military Muscle Flexing?" *Jamestown Foundation*, November 2, 2017. https://jamestown.org/program/russian-military-presence-in-caspian-sea-protection-of-national-interests-or-military-muscle-flexing/

The Kremlin's strategic vision regarding the protection of Russian national interests in the Caspian and barring outside powers from accessing the region has thus encouraged Moscow to increasingly flex its growing naval muscles there—as illustrated by the recent uptick in the Caspian Flotilla's exercises and port visits. The result of these shows of force by Russia will put growing pressure on small countries in the region as well as potentially disrupt strategic transnational Caspian-basin projects the West is involved in.

Altman, Jonathan. "Russian A2/AD In the Eastern Mediterranean: A Growing Risk." *Naval War College Review* 69 no. 1. (Winter, 2016). http://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1119&context=nwc-review.

It is important for policy makers and strategists alike to recognize the serious strategic implications of a Russian A2/AD envelope in the eastern Mediterranean. Such an envelope would present grave challenges to U.S. influence in the region and would imperil the free flow of commerce that is essential to U.S. and global prosperity. It would be wise to take steps now to prepare for this threat rather than attempting to address it after it becomes realized.

Kofman, Michael. "Russian Hybrid Warfare and Other Dark Arts." War on the Rocks. March 11, 2016. https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Following Russia's annexation of Crimea, hybrid warfare has become conversational short form in the West for describing Moscow's sneaky ways of fighting war. If there's one thing you've learned over the past two years about Russia, it's that it uses hybrid warfare, a dangerous Kremlin innovation the West must learn to grapple with.

Kasapoglu, Can. "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive

Control." *NATO Defense College, Research Division*, no. 121 (November 2015). November 2015. http://cco.ndu.edu/Portals/96/Documents/Articles/russia's%20renewed%20Military%20Thinking.pdf.

In both Crimea and the subsequent fighting in the Donbas region of Ukraine, Russia's signature tactic has been the use of so-called "Green Men," soldiers without identifying insignia whose identity as Russian soldiers the Kremlin denied. Ukraine, Georgia, and even NATO members like Estonia now fear that they could be the next target for Russia's Green Men. NATO, alarmed by the need to prepare for this unexpected tactic, has committed to develop new countermeasures to defend against this threat.

BALTIC INTERESTS

Schaub, Gary, Jr., Martin Murphy, and Frank G. Hoffman. "Hybrid Maritime Warfare: Building Baltic Resilience." *The RUSI Journal*, April 3, 2017. https://www.tandfonline.com/doi/full/10.1080/03071847.2017.1301631?scroll=top&needAccess=true.

Russia's use of hybrid warfare techniques has raised concerns about the security of the Baltic States. Gary Schaub, Jr, Martin Murphy and Frank G. Hoffman recommend a series of measures to augment NATO's Readiness Action Plan in the Baltic region, including increasing the breadth and depth of naval exercises, and improving maritime domain awareness through cooperative programmes.

Hicks, Kathleen, Lisa Sawyer Samp Andrew Metrick, and Kathleen Weinberger. *Undersea Warfare in Northern Europe*. CSIS International Security Program. July 21, 2016. https://www.csis.org/analysis/undersea-warfare-northern-europe.

In this report, the CSIS International Security Program analyzes Russian intentions and capabilities in the near to mid-term and the ability of NATO and partner nations to respond effectively to Russian activities in the undersea domain. The assessment identifies gaps in current Western organizations, capabilities, and posture and offers recommendations as to how NATO and partner nations can meet the Russian challenge in the undersea domain.

RUSSIAN PROXIES

Vojtiskova, Vladka, Hubertus Schmid-Schmidsfelden, Vít Novotny, and Kristina Potapova. *The Bear in Sheep's Clothing: Russia's Government-Funded Organisations in the EU*. Publication. July 2016. http://www.martenscentre.eu/sites/default/files/publication-files/russia-gongos.pdf.

This paper sheds light on organisations operating in Europe that are funded by the Russian government, whether officially or unofficially. These include government-organised non-governmental organisations, non-governmental organisations, and think

tanks. Their goal is to shift European public opinion towards a positive view of Russian politics and policies, and towards respect for its great power ambitions. In light of Russia's annexation of Crimea and Russian aggression in Eastern Ukraine, the overt or covert support for these organisations must become a matter of concern to the EU.

Lutsevych, Orysia. *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood*. Publication. Chatham House. Russian and Eurasia Programme. April 2016. https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-04-14-agents-russian-world-lutsevych.pdf.

Russia employs a vocabulary of 'soft power' to disguise its 'soft coercion' efforts aimed at retaining regional supremacy. Russian pseudo-NGOs undermine the social cohesion of neighbouring states through the consolidation of pro-Russian forces and ethno-geopolitics; the denigration of national identities; and the promotion of anti-US, conservative Orthodox and Eurasianist values. They can also establish alternative discourses to confuse decision-making where it is required, and act as destabilizing forces by uniting paramilitary groups and spreading aggressive propaganda.

RUSSIAN CYBER

Krekó, Péter, Lóránt Győri, Jekatyerina Dunajeva, Jakub Janda, Ondřej Kundra, Grigorij Mesežnikov, Juraj Mesík, Maciej Szylar and Anton Shekhovtsov. "The Weaponization of Culture: Kremlin's Traditional Agenda and the Export of Values to Central Europe." Political Capital Institute. August 4, 2016. http://www.politicalcapital.hu/search.php?article_read=1&article_id=66.

Political Capital's most recent study explores the topic of Russian soft power in Hungary, Slovakia, the Czech Republic, Poland and Austria. In the involved countries, the Kremlin purposefully aims at monopolising, manipulatively representing and disseminating "traditional" societal and Christian values used to ideologically underpin the system. Putin contrasts the allegedly "nihilistic" and "decadent" West with the Christian-conservative Russia and this way he tries to present his own autocracy's moral superiority.

Lucas, Edward, and Peter Pomeranzev. "Winning the Information War: Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe." Center for European Policy Analysis / Legatum Institute. August 2, 2016. https://cepa.ecms.pl/files/?id_plik=2715.

The Russian government uses disinformation, incitement to violence and hate speech to destroy trust, sap morale, degrade the information space, erode public discourse and increase partisanship. Our ability to respond is constrained by the mainstream media's loss of reach and impact. Its myth-busting and fact-checking reaches only a limited audience – and probably not the one the Kremlin is targeting. The response involves a

contradiction: our approach must be tailored to different audiences, yet must also seek to build trust between polarized groups. Our recommendations include tactical, strategic and long-term priorities, targeted partly at Kremlin disinformation and also aiming to strengthen media in democracies and educate audiences.

Rojansky, Matthew. "Tinker Tailor Soldier Hacker: The Russian Factor in the DNC Email Scandal." Kennan Institute. July 27, 2016. https://www.wilsoncenter.org/article/tinker-tailor-soldier-hacker-the-russian-factor-the-dnc-email-scandal.

Allegations that hackers linked to the Russian government have broken into DNC servers and leaked emails are consistent with the current dire state of U.S.-Russian relations. But not all of the implications that have been drawn, including about the Kremlin's likely motives, ring true. Let's take the key questions raised one at a time.

"Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia." NATO Strategic Communications Centre of Excellence. February 2016. http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

In order to analyse how pro-Russian trolling is used to influence the public opinion in NATO-member countries the NATO StratCom COE commissioned the study Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia. The study was conducted by the Latvian Institute of International Affairs in cooperation with Riga Stradins University, and was aimed at analysing organized pro-Russian trolling in internet media to measure its impact on public opinion in Latvia.

Paul, Christopher, and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." RAND Corporation. 2016. http://www.rand.org/pubs/perspectives/PE198.html.

Since its 2008 incursion into Georgia (if not before), there has been a remarkable evolution in Russia's approach to propaganda. The country has effectively employed new dissemination channels and messages in support of its 2014 annexation of the Crimean peninsula, its ongoing involvement in the conflicts in Ukraine and Syria, and its antagonism of NATO allies. The Russian propaganda model is high-volume and multichannel, and it disseminates messages without regard for the truth. It is also rapid, continuous, and repetitive, and it lacks commitment to consistency.

Chen, Adrian. "The Agency." *New York Times Magazine*. June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html.

From a nondescript office building in St. Petersburg, Russia, an army of well-paid "trolls" has tried to wreak havoc all around the Internet – and in real-life American communities.

Walker, Shaun. "The Russian troll factory at the heart of the meddling allegations." *The Guardian*. April 2, 2015. https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house.

Former workers tell how hundreds of bloggers are paid to flood forums and social networks at home and abroad with anti-western and pro-Kremlin comments.

CHINA:

GRAY ZONE STRATEGY

Holmes, James, Toshi Yoshihara. "Five Shades of Chinese Gray-Zone Strategy". *The National Interest*, May 2, 2017. http://nationalinterest.org/feature/five-shades-chinese-gray-zone-strategy-20450.

This typology of gray-zone tactics suggests that China is bringing to bear all elements of national power on the maritime disputes in the East and South China Seas. Beijing has employed legal, diplomatic, maritime and material elements of statecraft to chip away at the U.S.-led liberal international order. Even its construction prowess, honed over decades of massive infrastructure-building, has been on dazzling display in the heart of the South China Sea – contributing to strategic success.

Green, Michael, Kathleen Hicks, Zack Cooper, John Schaus and Jake Douglas. "Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence". Center for Strategic & International Studies. Lanham, MD: Rowman & Littlefield, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170505_GreenM_CounteringCoercionAsia_Web.pdf?OnoJXfWb4A5gw_n6G.8azgEd8zRIM4wq.

The inability of U.S. policymakers to deter coercive actions or to articulate a coherent gray zone strategy has raised questions about Washington's ability to protect U.S. interests, to integrate China into the international order, and to maintain existing alliance commitments. As a result, experts in the United States and in East Asia are searching for new approaches to counter coercion in the East and South China Seas.

Kania, Elsa. "The PLA's Latest Strategic Thinking on the Three Warfares." *China Brief 16*, no. 13. August 22, 2016. Jamestown Foundation. http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45723&tx_ttnews%5BbackPid%5D=7&cHash=229badbe854a0bdac91aaf401e3f9744.

Beijing's response to the unfavorable South China Sea arbitration outcome has highlighted an important aspect of its military strategy, the "three warfares" (三战). Consisting of public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (法律战), the three warfares have been critical components of China's strategic

approach in the South China Sea and beyond. In peacetime and wartime alike, the application of the three warfares is intended to control the prevailing discourse and influence perceptions in a way that advances China's interests, while compromising the capability of opponents to respond.

Harold, Scott W., Yoshiaki Nakagawa, Junichi Fukuda, John A. Davis, Keiko Kono, Dean Cheng, and Kazuto Suzuki. *The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains*. 2017. https://www.rand.org/pubs/conf_proceedings/CF379.html.

The United States and Japan face a dilemma: China is trying to change the status quo in the Indo-Pacific without firing a shot, gradually shifting the strategic playing field through the employment of gray zone coercion, or coercive moves that lie below the threshold that would trigger a military response. China's actions in the maritime, cyber, and (potentially) space domains challenge the status quo in ways that damage the interests of both Japan and the United States and are intended to erode trust in U.S. extended deterrence commitments. The RAND Corporation convened a pair of public conferences where experts from the United States and Japan presented papers focused on the challenges of deterrence by denial and deterrence by punishment in these three domains.

AFRICA

Asia Times Staff. "'Significant' Consequences if China Takes Over Djibouti Port, Says U.S. General." *Asia Times*, March 8, 2018. http://www.atimes.com/article/significant-consequences-china-takes-djibouti-port-says-us-general/.

The top US military commander in charge of US troops in Africa is worried about China's growing presence on the continent, he suggested in remarks in a congressional hearing on Tuesday. Marine General Thomas Waldhauser said in his remarks to lawmakers that China could theoretically cut off supplies to a US base in the northeast African nation of Djibouti, if they "took" the port there.

Fei, John. "China's Overseas Military Base in Djibouti: Features, Motivations, and Policy Implications". *China Brief*, December 22, 2017. https://jamestown.org/program/chinas-overseas-military-base-djibouti-features-motivations-policy-implications/.

The Chinese facility is near the U.S.' sole military base in Africa – Camp Lemonnier – and signals China's interest in protecting its growing economic and security interests in Africa and the Indian Ocean. While the base reflects China's growing economic and security ambitions, it is unclear at present whether the facility represents just an effort for China to enhance its peacekeeping and humanitarian and disaster relief capabilities, or suggests greater ambitions. If, as some reports suggest, China does open more military bases in African and the Indian Ocean region, then the Djibouti base would

mark the beginning of a sea-change in Chinese naval ambitions in the Indian Ocean region.

EAST & SOUTH CHINA SEAS

"Occupation and Island Building." Asia Maritime Transparency Initiative. https://amti.csis.org/island-tracker/.

Five claimants occupy nearly 70 disputed reefs and islets spread across the South China Sea. They have built more than 90 outposts on these contested features, many of which have seen expansion in recent years. AMTI has gathered satellite imagery of each outpost, along with other relevant information, to document their current status and any changes they have undergone in recent years.

Armour, Michael D. "The U.S. Coast Guard in the South China Sea: Strategy or Folly?" CIMSEC. November 6, 2017. http://cimsec.org/u-s-coast-guard-south-china-sea-strategy-folly/34648.

Recently there has been discussions at the highest level of the U.S. military concerning the deployment of U.S. Coast Guard assets to the South China sea and integrating them into the freedom of navigation operations conducted by the U.S. Navy relating to the manmade atolls constructed by the Chinese and subsequently claimed as Chinese sovereign territory. It may be that these U.S. Coast Guard units, if deployed to the area, may turn out to be a combat multiplier or a diplomatic plus. However, given the meager USCG budget and the limited assets of the service, their deployment may prove to be insignificant or even fraught with danger.

Lansing, Shawn. "The Coast Guard Can Reduce Risk in The South China Sea." United States Naval Institute. Proceedings. 143 no. 8 (August, 2017):26-31. https://search.proquest.com/docview/1933850606?accountid=322.

Lansing discusses how the US Coast Guard can reduce risk in the South China Sea. With its regional partnerships and experience strengthening maritime law enforcement regimes, the US Coast Guard is uniquely suited to address the need for greater governance in the disputed waters of the South China Sea. Debates over whether the US and China can escape violent confrontation or about China's use of "little blue men" to carry out "small-stick diplomacy" are fitting as tension in the South China Sea roils one of the world's most significant sea lines of communication.

Dutton, Peter. "A Maritime or Continental Order for Southeast Asia and the South China Sea?" Naval War College Review 69, no. 3. (Summer, 2016), 5-13. http://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1158&context=nwc-review.

Global maritime access and the security it provides, unlike the air we breathe, do not just exist as a state of nature. They must be established and then regularized through

laws and institutions that support them. And then ... they must be defended through political, economic, and military means when challenged.

Martinson, Ryan D. "China's Second Navy." *U.S. Naval Institute Proceedings Magazine*, 1346th ser., 141, no. 4 (April 2015). https://www.usni.org/magazines/proceedings/2015-04-0/chinas-second-navy.

While the world has been busy watching China's blue-water naval buildup, the People's Republic has been steadily exploiting maritime law enforcement – and its coast guard – as an instrument of statecraft.

Leaf, Paul J. "Learning from China's Oil Rig Standoff with Vietnam." *The Diplomat*, August 30, 2014. https://thediplomat.com/2014/08/learning-from-chinas-oil-rig-standoff-with-vietnam/.

China's overreach was costly, among other things it accelerated a developing arms race in Asia and amplified calls for Washington and Tokyo to counter Beijing. Still, China acquired useful information to hone its ongoing strategy in the South China Sea. Understanding why Beijing took this action and its attendant lessons will help Washington and its partners deal with China.

CHINESE PROXIES

Erickson, Andrew S., and Conor M. Kennedy. "Countering China's Third Sea Force: Unmask Maritime Militia Before They're Used Again." *The National Interest*, July 6, 2016. http://nationalinterest.org/feature/countering-chinas-third-sea-force-unmask-maritime-militia-16860.

When the Permanent Court of Arbitration in the Hague announces its rulings on the Philippines-initiated maritime legal case with China on July 12 – likely rejecting some key bases for excessive Chinese claims in the South China Sea – the Maritime Militia will offer a tempting tool for Beijing to try to teach Manila (and other neighbors) a lesson while frustrating American ability to calm troubled waters. This major problem with significant strategic implications is crying out for greater attention, and effective response. Accordingly, this article puts China's Maritime Militia under the spotlight to explain what it is, why it matters and what to do about it.

Erickson, Andrew S., and Conor M. Kennedy. "Irregular Forces at Sea: Not 'Merely Fishermen'-Shedding Light on China's Maritime Militia." CIMSEC. November 2, 2015. http://cimsec.org/new-cimsec-series-on-irregular-forces-at-sea-not-merely-fishermenshedding-light-on-chinas-maritime-militia/19624.

Maritime militia, dead ahead! In a just-published Defense News article, Chris Cavas has made an important contribution to our understanding of the operations and applications of China's irregular maritime forces. The forces he describes are almost

certainly neither ordinary merchant ship operators nor random fishermen, but rather militiamen operating in pre-planned roles in conjunction with USS Lassen's Freedom of Navigation Operation in the South China Sea on 27 October 2015.

Erickson, Andrew, Conor Kennedy. "Directing China's 'Little Blue Men': Uncovering the Maritime Militia Command Structure". *Asia Maritime Transparency Initiative*, September 11, 2015. https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/.

While Russia has employed "Little Green Men" surreptitiously in Crimea, China uses its own "Little Blue Men" to support Near Seas claims. As the U.S. military operates near Beijing's artificially-built South China Sea features and seeks to prevent Beijing from ejecting foreign claimants from places like Second Thomas Shoal, it may well face surveillance and harassment from China's maritime militia. Washington and its allies and partners must therefore understand how these irregular forces are commanded and controlled, before they are surprised and stymied by them.

CHINESE CYBER

Rogoway, Tyler, and Joseph Trevithick. "What Secretive Anti-Ship Missile Did China Hack from the U.S. Navy?" *The Drive*, June 8, 2018. http://www.thedrive.com/the-war-zone/21414/what-supersonic-anti-ship-missile-did-china-hack-from-the-u-s-navy.

China's relentless cyber espionage campaign against the Pentagon has been one of the central reasons why that country's technological warfighting capabilities have aggressively matured over a relatively short period of time. In fact, we now see the fruits of their hacking operations on a daily basis via advanced 'indigenous' weapon systems, some which are now entering into operational service. But a previously unreported intrusion into a Navy contractor's computer network has provided the Chinese military with information on the service's electronic warfare and threat library, cryptographic radio systems used on submarines, specific sensor data, and detailed information on a previously undisclosed and fast-paced initiative to field a supersonic anti-ship missile onto American nuclear submarines dubbed Sea Dragon.

Adams, Michael. "Why the OPM Hack IS Far Worse Than You Imagine." Lawfare. March 11, 2016. https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

The Office of Personnel Management ("OPM") data breach involves the greatest theft of sensitive personnel data in history. But, to date, neither the scope nor scale of the breach, nor its significance, nor the inadequate and even self-defeating response has been fully aired.

IRAN

GRAY ZONE STRATEGY

Gilmore, T.J. "Iran Owns the Gray Zone." *Proceedings Magazine*, March 2018. https://www.usni.org/magazines/proceedings/2018-03/iran-owns-gray-zone.

Iran's "gray zone" strategy has significant implications for the U.S. Navy despite the conventional maritime superiority the United States currently maintains in the eastern Mediterranean and throughout the Central Command area of responsibility. With proxies in Syria and Yemen, and the bulk of its navy based in Bandar Abbas, Iran is well positioned to hold the U.S. Navy at risk in the Strait of Hormuz, the Bab el-Mandeb, and increasingly the waters off the Levant. To meet this threat, the Navy needs to understand fully Iran's current capabilities and objectives in the gray zone, train and exercise to recognize and combat this unique type of aggression, and demonstrate a willingness to escalate the competition to be successful.

Ryan, Missy, and Thomas Gibbons-Neff. "Navy Patrol Ship Fires Warning Shots at Iranian Vessel in one of Several Confrontations." *Washington Post*, August 25, 2016. https://www.washingtonpost.com/news/checkpoint/wp/2016/08/25/u-s-navy-callshigh-speed-approach-by-iranian-ships-dangerous-harassment/.

The incidents are the latest sign of US-Iranian friction near Iran's coast. In January, a group of US sailors was detained overnight by Iranian personnel after their boats veered into Iranian waters. It was an embarrassment for the Obama administration and resulted in disciplinary action for some of the US personnel involved in that incident.

U.S. Office of Naval Intelligence. "Iran's Naval Forces: From Guerilla Warfare to a Modern Naval Strategy." Suitland, MD: Office of Naval Intelligence, 2009. https://www.worldcat.org/wcpa/oclc/772609558?page=frame&url=http%3A%2F%2Fhandle.dtic.mil%2F100.2%2FADA510110%26checksum%3D35c9bca545ab247801ebce015d748b9a&title=&linktype=digitalObject&detail=.

Iran's naval forces, like the country itself, have been shaped by the Islamic revolution, petroleum, and an often adversarial relationship with neighboring countries and the international community as a whole. These factors have influenced how Iran's naval forces are organized, how they are equipped and manned, and how they interact with external forces.

Kahwaji, Riad. "Iran's Strategy at Sea 'Guerrilla Warfare' by Small, Fast Ships would Greet U.S. If War Breaks Out." *Navy Times*, May 22, 2006. http://usnwc.idm.oclc.org/login?url=http://search.proquest.com/docview/203963287?accountid=322.

Boats and midget submarines loaded with high explosives also could ram giant oil tankers or aircraft carriers in suicide attacks, said Qassem Jaafar, a defense analyst based in Doha, Qatar. Kazemi assessed April's small-boat maneuvers in this way: "In an enclosed, narrow and rather shallow region such as the Persian Gulf, this tactic can be

very decisive against large units and can deny the enemy from effective deployment, sea lines of communication and power projection."

IRANIAN PROXIES

"Saudi-Led Coalition Foils Houthi Attacks on Red Sea Ships, Saudi and UAE Media Say." *Thomson Reuters*, May 23, 2018. https://www.reuters.com/article/us-yemen-security-tanker/saudi-led-coalition-foils-houthi-attacks-on-red-sea-ships-saudi-and-uae-media-say-idUSKCN1IO15P.

A Saudi-led military coalition foiled attacks by explosives-laden speedboats deployed by Yemen's Iran-aligned Houthi movement against commercial vessels, including an oil tanker, in the Red Sea, Saudi and Emirati state media said on Wednesday.

Farrukh, Maher, Tyler Nocita, and Emily Estelle. "Warning Update: Iran's Hybrid Warfare in Yemen." Critical Threats. March 26, 2017. https://www.criticalthreats.org/analysis/warning-update-irans-hybrid-warfare-in-yemen.

Iran may deploy more advanced military capabilities to Yemen to support the al Houthi-Saleh faction, which faces increasing pressure. Iran has provided al Houthi-Saleh forces with sophisticated arms and advisors from its proxy network, including Afghan and Shia Arab specialists. The deployment of interoperable proxy forces is part of Iran's evolution of a form of hybrid warfare that will allow it to project significant force far from its borders and fundamentally alter the balance of power in the region.

IRANIAN CYBER

Groll, Elias. "Spear Phishing in Tehran." *Foreign Policy*, August 9, 2016. http://foreignpolicy.com/2016/08/09/spear-phishing-in-tehran/.

Aggressive surveillance remains a key tool in the regime's attempt to maintain power, and today, having sophisticated snooping software installed on one's computer can be as easy as opening the wrong attachment or clicking on a pernicious link. Quietly, software is downloaded in the background and begins communicating with whomever has selected you for surveillance. Hackers working on behalf of Iran frequently turn to a method known as spear phishing - the use of an email that appears to come from a legitimate account but actually contains a malicious attachment or link – in order to install spyware on their targets' digital devices.

Scott-Railton, John, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola. "Group5: Syria and the Iranian Connection." The Citizen Lab. August 2, 2016. https://citizenlab.org/2016/08/group5-syria/.

Elements of the Syrian opposition have been targeted by malware campaigns since the early days of the conflict: regime-linked malware groups, the Syrian Electronic Army,

ISIS, and a group linked to Lebanon reported by FireEye in 2015 have all attempted to penetrate opposition computers and communications. Some of these operations are still active as of the time of writing. This report adds one more threat actor to the list: Group5, which we name to reflect the four other known malware groups.

III. Innovation & Adaptation

TECHNOLOGY

"Making Gray-Zone Activity More Black and White." DARPA News and Events. March 14, 2018. https://www.darpa.mil/news-events/2018-03-14.

To better understand and respond to an adversary's gray-zone engagement, DARPA's Strategic Technology Office today announced a new program called COMPASS, which stands for Collection and Monitoring via Planning for Active Situational Scenarios. The program aims to develop software that would help clarify enemy intent by gauging an adversary's responses to various stimuli. COMPASS will leverage advanced artificial intelligence technologies, game theory, and modeling and estimation to both identify stimuli that yield the most information about an adversary's intentions, and provide decision makers high-fidelity intelligence on how to respond—with positive and negative tradeoffs for each course of action.

Werner, Ben. "VIDEO: Houthi Forces Capture U.S. Navy Unmanned Underwater Vehicle Off Yemen." USNI. January 3, 2018. https://news.usni.org/2018/01/03/houthi-rebels-find-likely-u-s-navy-unmanned-underwater-vehicle.

In the video posted online by local media on Monday, four men described as members of the "Houthi Navy" in dive gear are surrounding what appears to be a REMUS 600 UUV with the name "Smokey" printed on the body. According to the AMN News web posting, the Houthis discovered the UUV within the past week somewhere off the coast of Yemen.

Jennings, Ralph. "What an American Naval Drone Could Tell Us about the Future of U.S.-China Relations." *Forbes*, December 19, 2016. https://www.forbes.com/sites/ralphjennings/2016/12/19/how-an-american-underwater-drone-reached-the-contested-south-china-sea/#566abd0cd507.

The Chinese seizure on Thursday of a U.S. Navy underwater drone that was exploring the widely disputed South China Sea raises the specter of another massive Sino-U.S. spat, even though President-elect Donald Trump loudly tweeted at China: "let them keep it!" But the discovery of a U.S. drone in a politicized ocean on the other side of the world raises sticky questions that will become ever more relevant as China and the United States square off in the months, or years, ahead.

Bana, Sarosh. "China's Underwater Great Wall." *The Washington Times*, August 30, 2016. https://www.washingtontimes.com/news/2016/aug/30/chinas-underwater-great-wall/.

The stakes in the South China Sea (SCS) are apparently reaching down to the murky depths of this contentious waterway as Beijing readies its undersea surveillance network to consolidate its presence in the region.

STRATEGY & OPERATIONS

LITTORAL CONFLICT

Vego, Milan. "On Littoral Warfare." *Naval War College Review* 68, no. 2 (Spring 2015): 30-68. https://search.proquest.com/docview/1660144761?accountid=322.

Naval warfare in the littorals has much in common with war conducted on the open ocean. However, there are also some significant differences, due to the extremely complex, dynamic, and challenging physical environment of the former. The peculiarities of the physical environment in the littorals offer many challenges – but also opportunities – in the employment of naval forces and aircraft. Distinctions between characteristics of war on the open ocean and in the littorals must be thoroughly understood; otherwise, commanders and their staffs simply cannot plan or employ their forces properly.

Galdorisi, George. "The Littoral Combat Ship: New Neighbor in the Asia-Pacific." *Defence Review Asia* 8, no. 5 (July 2014): 18-21. http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=96735516&site=ehost-live.

The article presents information on the Littoral Combat Ship (LCS) in the U.S. Navy. The LCS ship was designed to be a focused-mission ship and is the newest surface combatant operating in the Asia-Pacific region. Some of the primary missions of the LCS ship are antisubmarine warfare, mine countermeasures, and surface warfare against small boats.

SMALL BOATS

McNeil, Jena Baker. "Getting the Small-Boat Threat Right." Heritage Foundation. August 23, 2010. http://www.heritage.org/research/reports/2010/08/getting-the-small-boat-threat-right.

"Small craft" defines any boat that weighs under 300 tons and is less than 100 feet in length; the majority, however, are far smaller. Arguably, each one of these crafts represents a potential waterborne improvised explosives device or the means of delivering a weapon of mass destruction. Nevertheless, the small-boat threat is less acute than other security challenges, and despite the vast numbers of boats present, the threat may be managed.

"Small Boats." Robert Strauss Center for International Security and Law. https://www.strausscenter.org/hormuz/small-boats.html.

Small boats have been used throughout the last century in asymmetric warfare attacks on both military and civilian targets, combating a materially superior adversary without direct confrontation. The Iranian Revolutionary Guard Corps operates a fleet of "˜small boats' estimated at more than 1000 boats. The Iranians harassed tanker traffic during the Tanker War using small boats. Many, including the U.S. Navy, suspect that any Iranian effort to close the Strait would include the use of small boats, potentially in suicide attacks.

"Small Vessel Security Strategy" *Department of Homeland Security*. April 2008. http://www.dhs.gov/small-vessel-security-strategy.

The Small Vessel Security Strategy addresses the risk that small vessels might be used to smuggle terrorists or weapon of mass destruction into the United States or might be used as either a stand-off weapon platform or as a means of a direct attack with a waterborne improvised explosive device. This strategy also describes the small vessel community and the environment in which it operates.

NON-STATE NAVIES

Rawley, Chris, and Claude Berube. "The Non-State Navy: Sea Shepherd as a Case Study for 21st Century Maritime Non-State Actors." *Small Wars Journal*, July 23, 2013. http://smallwarsjournal.com/jrnl/art/the-non-state-navy-sea-shepherd-as-a-case-study-for-21st-century-maritime-non-state-actors.

Examining Sea Shepherd's goals, strategies, platforms, and tactics is a worthwhile endeavor because it serves as a model to understand the motives, operations, and threat posed by emerging maritime non-state actors. Understanding the irregular challenges these MNSAs pose can help navies and coast guards respond to similarly-structured groups in the future.

Povlock, Paul A. "A Guerilla War at Sea: THE SRI LANKAN CIVIL WAR." *Small Wars Journal*, September 9, 2011. http://www.dtic.mil/dtic/tr/fulltext/u2/a549049.pdf.

The rebel Tamil Tigers required secure sea lines of communication to supply their forces with the apparatus of modern warfare and used the open maneuver space of the sea to attack the Sri Lankan armed forces, government and economy. Over time, the Sea Tigers, the insurgent maritime force, developed into a highly capable and aggressive organization that was able to operate in all maritime domains across the spectrum of conflict.

SPECIAL OPERATIONS FORCES

Coffman, MAJ Sean, MAJ Rob Shumaker, and MAJ Jeff Givens. "Perception is Reality: SOF in

the Gray Zone." *Small Wars Journal*, June 20, 2016. http://smallwarsjournal.com/blog/perception-is-reality-sof-in-the-gray-zone.

This thesis examines two case studies of special operations forces use in the Gray Zone – in Somalia in 1992–1993 and the Philippines in 2000–2015. Using the bureaucratic politics model as a framework and evaluating players, decision games, and outcomes, the choice to employ SOF is replayed and outcomes are evaluated in an empirical light.

United States of America. United States Army. Special Operations Command. *SOF Support to Political Warfare*. March 10, 2015. http://www.soc.mil/swcs/ProjectGray/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20(10MAR2015)%20%20%20.pdf.

Political Warfare is a strategy suited to achieve U.S. national objectives through reduced visibility in the international geo-political environment, without committing large military forces. Likewise, Political Warfare can function as a critical, integrating element of U.S. national power against non-state adversaries such as the current Islamic State in Iraq and the Levant. Most often, the Department of Defense role in Political Warfare will be one of supporting other U.S. Government agencies that are more likely to lead strategy and planning development.

ENVIRONMENTAL & ECONOMIC ISSUES

MARINE RESOURCES

Stavridis, James G., and Johan Bergenas. "The Fishing Wars Are Coming." *The Washington Post*, September 13, 2017. https://www.washingtonpost.com/opinions/the-fishing-wars-are-coming/2017/09/13/05c75208-97c6-11e7-b569-3360011663b4_story.html?noredirect=on&utm_term=.47630a8a9829.

The deployment of both hard and soft power to acquire natural resources is nothing short of hybrid warfare. Countries on the receiving end of Chinese actions are responding in kind: Indonesia has blown up hundreds of vessels fishing in their waters illegally; Argentina sank a Chinese vessel illegally fishing in its waters last year; and South Africa continues to clash with Beijing over fishing practices.

Clarke, Alex. "Protecting the Exclusive Economic Zones – Part I." Center for International Maritime Security. November 18, 2014. http://cimsec.org/protecting-exclusive-economic-zones-part/13637.

An EEZ is the area of sea/sea bed that a nation administers, for want of a better phrase 'owns', and therefore can control/monetize the extraction of resources (such as Fish, Gas, Gold or Manganese) from, and which are becoming increasingly important to national economies – in fact their societies as a whole. However, a nation cannot control or monetize anything if it doesn't actually have control of it, and just as a city

cannot be policed from the secured, nor a battlefield secured just from air, neither can an EEZ.

THE OPENING ARCTIC

LaGrone, Sam. "Navy Reestablishes U.S. 2nd Fleet to Face Russian Threat; Plan Calls for 250 Person Command in Norfolk." USNI News. May 4, 2018. https://news.usni.org/2018/05/04/navy-reestablishes-2nd-fleet-plan-calls-for-250-person-command-in-norfolk.

Faced with a more active Russian fleet and increasing military competition across the world, the Navy has elected to reestablish U.S. 2nd Fleet to manage assets closer to the homeland, according to a memo announcing the command obtained by USNI News.

Nankivell, Justin D. "The Role of History and Law in the South China Sea and Arctic Ocean." Maritime Awareness Project. August 7, 2017. http://maritimeawarenessproject.org/2017/08/07/the-role-of-history-and-law-in-the-south-china-sea-and-arctic-ocean/.

This new episode in the evolving relationship of history, treaty law for UNCLOS, and customary international law may set the stage for contention in the South China Sea to dredge up historical problems surrounding the politics of international law in the Arctic Ocean.

Goodman, Sherri. "Changing Climates for Arctic Security." *The Wilson Quarterly*, Summer/Fall 2017. https://wilsonquarterly.com/quarterly/into-the-arctic/changing-climates-for-arctic-security/.

Shaped by changing climates – political as well as planetary – our understanding of security in the Arctic has morphed since the Cold War and continues to take on new forms.

Sergunin, Alexander. "Is Russia Going Hard or Soft in the Arctic?" *The Wilson Quarterly*, Summer 2017. https://wilsonquarterly.com/quarterly/into-the-arctic/is-russia-going-hard-or-soft-in-the-arctic/.

Is Russia igniting a new arms race in the Far North or taking justifiable steps to defend its interests in a changing environment? The answer to that question depends greatly on whom you ask, where they are, and just how much they appreciate the range of issues that factor into Russia's Arctic policy.

MARITIME LAW

Kraska, James. "How China Exploits a Loophole in International Law in Pursuit of Hegemony in

East Asia." *Foreign Policy Research Institute*, January 22, 2015. https://www.fpri.org/article/2015/01/how-china-exploits-a-loophole-in-international-law-in-pursuit-of-hegemony-in-east-asia/.

By using asymmetric maritime forces – principally fishing vessels and coast guard ships – China is slowly but surely absorbing the South China Sea and East China Sea into its domain. And it does so by exploiting a loophole in international law created by the International Court of Justice that makes it impossible for regional states to respond effectively. This legal dimension of the international politics of the maritime disputes in East Asia is not widely understood, but it is at the core of Chinese strategy in the region.

Smith, Jeff M., and Joshua Eisenman. "China and America Clash on the High Seas: The EEZ Challenge." *The National Interest*, May 22, 2014. http://nationalinterest.org/feature/china-america-clash-the-high-seas-the-eez-challenge-10513.

While working to construct better conflict resolution mechanisms and improve relations with the PLAN, Washington must continue to emphasize that its policy is not subject to fear, intimidation, coercion, or reckless behavior from Chinese naval or coastal defense forces. This should include maintaining an active schedule of surveillance activities, patrolling, and freedom of navigation operations. This position is not only within the U.S. national interest, but also supported by domestic and international law. Were the U.S. to accept China's interpretation of UNCLOS, U.S. military vessels could be barred from operating in the roughly one-third of the world's oceans that are now EEZs.