ARMADA DEL ECUADOR
ACADEMIA DE GUERRA NAVAL
Guayaquil
-o-

LECTURA RECOMENDADA

"OCO and Future Littoral Operating Concepts"

Autor: JD Work National Defense University

Lectura Recomendada por:
CPCB-EM Álvaro Genovese
Oficial Instructor de la Academia de Guerra Naval

2023

Resumen de la lectura:

Alvaro Genovese Cevallos
Capitán de Corbeta-EM
Oficial Instructor de la Academia de Guerra Naval

La introducción de nuevas opciones de misiles de crucero de lanzamiento terrestre para mantener en riesgo los objetivos navales adversarios con el fin de apoyar los objetivos de disuasión convencionales a través de misiones de control y negación del mar es la pieza central de la propuesta de reorganización de las fuerzas del Litoral Marino, como parte de las nuevas “Operaciones de Base Avanzada Expedicionaria”. ”y conceptos de “Operaciones litorales en entornos en disputa”. Los fuegos de control marítimo distribuidos eficaces contra las formaciones marítimas amenazantes requieren la derrota de los sistemas integrados de defensa aérea. Las capacidades de operaciones cibernéticas ofensivas pueden considerarse como un medio para alterar el cálculo de desgaste en los intercambios de disparos de misiles, pero debido a diversas sensibilidades, hasta la fecha ha sido difícil discutir estas opciones en la literatura no clasificada. Se utilizan enfrentamientos simulados en software de juegos de guerra comercial contemporáneo para ofrecer información única sobre el espacio del problema. Los hallazgos de enfrentamientos simulados sugieren opciones de alta rentabilidad para efectos integrados, además de resaltar la importancia de ciertas características de diseño de misiles, modos de operación del buscador y operaciones de batería. Los resultados de estas simulaciones validan una vez más los antiguos principios del combate naval y sugieren que las capacidades cibernéticas ofensivas pueden proporcionar una ventaja útil al exacerbar la inestabilidad de los fuegos tácticos. Sin embargo, este análisis resalta aún más los desafíos de acceso, explotación y adaptación de la carga útil que plantean las complejas y heterogéneas redes adversarias, lo que sugiere un espacio problemático que rápidamente pasa de la cuestión de los incendios cibernéticos en los problemas de las flotas a las cuestiones del dilema del saboteador.

Military Cyber Affairs

Volume 5
Issue 1 *HammerCon 2022 Special Issue*

Article 3

May 2022

Offensive Cyber Operations and Future Littoral Operating Concepts

JD Work
National Defense University

Offensive Cyber Operations and Future Littoral Operating Concepts

JD Work

Abstract

Introduction of new ground-launch cruise missile options to hold adversary naval targets at risk in order to support conventional deterrence objectives through sea control and sea denial missions is the centerpiece of proposed reorganization of Marine Littoral forces, as part of new "Expeditionary Advanced Base Operations," and "Littoral Operations in Contested Environments" concepts. Effective distributed sea control fires against pacing threat maritime formations requires defeat of integrated air defense systems. Offensive cyber operations capabilities may be considered as a means of altering the calculus of attrition in missile fires exchanges, but due to various sensitivities it has been difficult to date to discuss these options in unclassified literature. Simulated engagements in contemporary commercial off-the-shelf wargaming software are used to offer unique insights into the problem space. Findings from simulated engagements suggest high payoff options for integrated effects, as well as highlighting the importance of certain missile design characteristics, seeker operation modes, and battery operations. The results of these simulations once again validate longstanding principles of naval combat, and suggest that offensive cyber capabilities may provide useful advantage by exacerbating tactical fires instability. However, this analysis further highlights the access, exploitation, and payload tailoring challenges posed by complex heterogenous adversary networks - suggesting a problem space that rapidly moves from the question of cyber fires in fleet problems, to the questions of the saboteur's dilemma.

Introduction

"Far-called our navies melt away;
On dune and headland sinks the fire…"
Recessional, Rudyard Kipling (1897)

The U.S. Marine Corps has embarked upon a strategy of radical transformation in order to provide unique warfighting capabilities in service of a nation facing renewed great power competition and potential conflict far different than the kinds of fights encountered in the long years of the Global War on Terror. At the centerpiece of this effort is the forward deployment of mobile, anti-ship surface to surface missile armed forces capable of holding adversary naval formations at risk in order to contest revisionist claims to key strategic chokepoints and other littoral waters. In many ways, this "new" concept is a return to a fundamental early mission of the Corps, in support of the Fleet and aligned with the National Defense Strategy

that seeks to restore competitive military advantage in order to deter adversaries from challenging the present liberal international order.[1]

However, these adversary formations will not be undefended, and in fact each will represent a complex integrated air defense network that pose unique challenges for the selection, positioning, and employment of these Marine Littoral forces' new missile capabilities. The contest between littoral fires and afloat missile intercept is a kind of engagement that has been rarely observed in the real world to date since the first anti-ship missile was fired in anger during the Six-Day War in 1967.[2] Despite the proliferation of these capabilities in naval service worldwide, paucity of the historical case record has given some observers pause in evaluating the potential effectiveness of new force options given the need to defeat modern adversary surface to air missile systems. While the notable recent case of the reported success of Ukrainian coastal defense Neptune (modified SS-C-6 SENNIGHT / SS-N-25 SWITCHBLADE / 3M24 Kh35 URAN), batteries in sinking the Project 1164 Slava (Atlant) class cruiser Moskva in April 2022, offers strong potential evidence for the underlying proposition, questions of Russian fleet readiness still hang over the action.[3] Nonetheless, contemporary naval engagements are also likely to be marked by the introduction of novel offensive cyber operations capabilities that will also fundamentally change the outcomes of these intercept problems – capabilities for which there is no public historical record.

It is true that such capabilities have been considered for decades in the naval operations context, indeed arguably first arising as a military innovation from the requirement to hold at risk Soviet Fleet targets whose deployments proved otherwise challenging to then contemporary U.S. conventional forces.[4] However, unclassified discussion of such concepts has remained difficult. Potential cyber fires employment in support of conventional littoral operations for sea control and sea denial has not been addressed in academic, professional military education literature to date.

---

[1] James Winnefeld. "The 20th-Century Roots of EABO." U.S. Naval Institute Proceedings, Vol 147 No 2. February 2021.; Gordon Emmanuel. "Smash Bullies: Interpreting the 'why' behind our Commandant's Force Design Report." Marine Corps Gazette. June 2020.; Sascha H. Rackwitz. "Clausewitz, Corbett, And Corvettes." Center for International Maritime Security. 17 April 2020. http://cimsec.org/clausewitz-corbett-and-corvettes/43475 ; B. A. Friedman. 21st Century Ellis: Operational Art and Strategic Prophecy for the Modern Era. Naval Institute Press. 2015. ; David J. Ulbrich. "Clarifying the Origins and Strategic Mission of the U.S. Marine Corps Defense Battalion, 1898–1941." War and Society. Vol 17 Issue 2: 81-109. 1999. ; Earl H. Ellis. "Advanced Base Operations in Micronesia." U.S. Marine Corps. 1921.

[2] John C. Schulte. "An Analysis of the Historical Effectiveness of Anti-Ship Cruise Missiles in Littoral Warfare." Naval Postgraduate School. September 1994.; Alon Ben-David. "Israel Navy caught out by Hizbullah hit on corvette." Jane's Defence Weekly. 26 July 2006. ; Jeremy Binnie, Neil Gibson. "UAE's Swift likely hit by C-801 missile." Jane's Defence Weekly. 7 October 2016.; Jeremy Binnie. "U.S. says missiles launched against destroyer in Red Sea." Jane's Defence Weekly. 10 October 2016.

[3] Manash Pratim Boruah, "Ukraine conflict: Russian Navy's Black Sea Fleet flagship sinks." 15 April 2022.

[4] Craig J. Wiener. "Penetrate, Exploit, Disrupt, Destroy: The Rise Of Computer Network Operations As A Major Military Innovation." George Mason University. 2016.

This study explores the hitherto unexamined problem space through the use of unclassified wargaming and simulation tools, providing unique insights into the exchange of fires in salvo warfare where offensive cyber options may provide advantage in what would otherwise be a brutal calculus of attrition pitting incoming antiship missiles against area defense and point defense interceptors. We consider the challenges and outcomes involved in access to, and exploitation of, multiple complex heterogenous military systems and networks afloat. We identify the need for maximization of what may be scarce options to achieve most significant impact for high payoff systems targets. These high payoff outcomes include particular advantages obtained when focusing Offensive Cyber Operation (OCO) effects in support of low-observable, passive terminal seeker operating mode antiship missile designs and to degrade adversary cooperative air defense engagement processes.

Integration of OCO engagement options with optimized missile targeting allocation, autonomous dynamic terminal engagement re-allocation, and prospective new Electronic Warfare (EW) options are also discussed. These simulations highlight the complexities of Intelligence, Surveillance, and Reconnaissance (ISR) competition, and the need to focus on battery signature management. While OCO effects are shown to be most effective at the margins of engagement envelopes, these findings reinforce well known principles of naval combat and highlight disproportionate impact of even relatively small advantages. This is due to the tactical instability that characterizes contemporary naval missile exchanges arising from the concentration of combat power relative to survivability. Select OCO effects demonstrate the potential to exacerbate this instability, and contribute to victory in these types of engagements.

Background and Context – Fleet Problems

In May 1898, a Navy and Marine Corps element conducted one of the first expeditionary actions to deny and degrade adversary networks in the littoral environment, destroying a key communications node near Cienfuegos, Cuba—a small-but-strategic port named the city of a "Hundred Fires." [5] The raid completed the ongoing blockade of the Spanish controlled island, denying not only sea lanes of communication to the enemy, but also communications in the then nascent cyber domain of what has been called the "Victorian Internet." [6] The mission was not without cost—the small boats used by the cable-cutting teams were exposed to shore fires of murderous intensity from a responding Spanish infantry regiment as

[5] Evelyn M. Cherpak. "Cable Cutting at Cienfuegos." U.S. Naval Institute Proceedings. February 1897.; Hermann Jacobsen. "Sketches from the Spanish-American War." U.S. Naval Institute Proceedings. January 1899.; Caspar F. Goodrich. "The St. Louis' Cable Cutting." U.S. Naval Institute Proceedings. March 1900. ; Carlos C. Hanki. "The Cable Cutters of Cienfuegos." U.S. Naval Institute Proceedings. March 1931.; Jonathan Reed Winkler. "Silencing the Enemy: Cable-Cutting in the Spanish–American War." War on the Rocks. 6 November 2015. https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/

[6] Tom Standage. *The Victorian Internet*. London: Walker & Co. 1998.

the raiders struggled to destroy the hardened connection with improvised tooling ill-suited to the task, resulting in two Americans killed and fifteen wounded in action. Naval gunfire support and raiding party covering fires would nonetheless exact an estimated three hundred enemy killed. Since this early example, operations in the information environment have been inextricably intertwined with sea control.

One hundred twenty-two years later, we find ourselves once again grappling with the questions raised by missions to deny and degrade adversary networks as we explore new concepts for distributed maritime operations, expeditionary advanced base operations, and littoral operations in contested environments. We stand at a unique inflection point, as the Navy and Marine Corps look to the "Terrible 20's" and the hard choices that the geopolitical, strategic, and budgetary realities of the decade will bring for future fleet and force design.[7] These choices will play out against a constant optempo drumbeat of requirements imposed by combatant commands facing renewed great power competition and the continuing unresolved challenges of the "lesser included" transnational problems of counter-terrorism, counter-proliferation and other key priorities essential to defense of U.S., allied, and partner interests in every theatre.[8]

The Commandant of the Marine Corps (CMC) and Chief of Naval Operations (CNO) have sought sweeping changes they believe are needed to ensure Marine elements may effectively serve as the nation's naval expeditionary force-in-readiness, a force that will leverage the power of the integrated fleet in order to maintain a persistent naval forward presence enabling sea control and denial

[7] Bryan McGrath. "When (Bad) Strategy Drives Resources." cdrsalamander blog. 7 April 2022. http://cdrsalamander.blogspot.com/2022/04/when-bad-strategy-drives-resources.html ; CDR Salamander. "We Chose Decline." cdrsalamander blog. 29 March 2022. http://cdrsalamander.blogspot.com/2022/03/we-chose-decline.html ; CDR Salamander. "The Terrible 20s Emerge from the Fog." 21 September 2021. cdrsalamander blog. 21 September 2021. http://cdrsalamander.blogspot.com/2021/09/the-terrible-20s-emerge-from-fog.html ; CDR Salamander. "The Post-COVID-19 Natsec Environment." 28 April 2020. cdrsalamander blog. http://cdrsalamander.blogspot.com/2020/04/the-post-covid-19-natsec-environment.html; CDR Salamander. "The Terrible 20s meet the Tiffany Navy." cdrsalamander blog. 2 December 2014. http://cdrsalamander.blogspot.com/2014/12/the-terrible-20s-meet-tiffany-navy.html ; CDR Salamander. "What Does the Exit Point from the 'Terrible 20" Look Like?" U.S. Naval Institute Blog. 24 July 2019. https://blog.usni.org/posts/2019/07/24/what-does-the-exit-point-from-the-terrible-20-look-like; CDR Salamander. "The Terrible 20s is About More Than Money." cdrsalamander blog. 28 January 2016. http://cdrsalamander.blogspot.com/2016/01/the-terrible-20s-is-about-more-than.html; CDR Salamander. "The Terrible 20s in a Picture." cdrsalamander blog. 23 October 2013. http://cdrsalamander.blogspot.com/2013/10/the-terrible-20s-in-picture. ; CDR Salamander. "Towards the 'Terrible 20's'." U.S. Naval Institute Blog. 10 February 2010. https://blog.usni.org/posts/2010/02/10/towards-the-terrible-20s

[8] Andrew Kramer and Martin Schroeder. "The Navy Needs a Gray-Zone Strategy." U.S. Naval Institute Proceedings. Vol 146 Issue 6. June 2020. ; Bradford Dismukes. "The Return of Great-Power Competition—Cold War Lessons about Strategic Antisubmarine Warfare and Defense of Sea Lines of Communication." Naval War College Review. Vol 70 No 3. Summer 2020.; Hal Brands, Evan Braden Montgomery. "One War Is Not Enough: Strategy and Force Planning for Great-Power Competition." Texas National Security Review. Vol 3, Iss 2: 80-92. Spring 2020. ; Mark D. Miles and Charles R. Miller. "The Great Power Competition Paradigm." JFQ. Volume 94, 3rd Quarter 2019. ; Thomas P.M. Barnett. The Pentagon's New Map. Random House, 2005.

operations.[9] The idea that the current force and its legacy platforms are not organized, trained and equipped to execute these re-emerging missions is not without its controversy and debate, extending even to the most senior ranks of earlier generations of Marine leadership.[10] But guidance from the Corps' current leadership is clear.[11] They will develop new tactical means, and employ these means in new ways to provide future decisionmakers with better options, connecting these options to the strategic ends pursued through joint campaigns that are naval in character.[12]

---

[9] Commandant of the Marine Corps. *Force Design 2030*. March 2020.; Chief of Naval Operations. *A design for maintaining maritime superiority*. December 2019.; Commandant of the Marine Corps. *Commandant's Planning Guidance (CPG)*. July 2019.;

[10] Ben Wan Beng Ho/ "Shortfalls in the Marine Corps' EABO Concept." U.S. Naval Institute Proceedings. Vol 147 Issue 7. July 2020. ; Jeff Cummings, Scott Cuomo, Olivia A. Garard, And Noah Spataro. "Getting The Context Of Marine Corps Reform Right." War on the Rocks. 1 May 2020. https://warontherocks.com/2020/05/getting-the-context-of-marine-corps-reform-right/; Benjamin Jensen. "The Rest Of The Story: Evaluating The U.S. Marine Corps Force Design 2030." War on the Rocks. 27 April 2020. https://warontherocks.com/2020/04/the-rest-of-the-story-evaluating-the-u-s-marine-corps-force-design-2030/; T. X. Hammes. "Building A Marine Corps For Every Contingency, Clime, And Place." War on the Rocks. 15 April 2020. https://warontherocks.com/2020/04/building-a-marine-corps-for-every-contingency-clime-and-place/; Nathan Fleischaker and Christopher Denzel. "Force 2030 – Divesting: Maneuver Warfare." Marine Corps Association. 7 April 2020.https://mca-marines.org/force-2030-divesting-maneuver-warfare/ ; Mark Cancian. "The Marine Corps' Radical Shift toward China." Center for Strategic and International Studies. 25 March 2020. https://www.csis.org/analysis/marine-corps-radical-shift-toward-china; Mark Cancian. "Don't Go Too Crazy, Marine Corps." War on the Rocks. 8 January 2020. https://warontherocks.com/2020/01/dont-go-too-crazy-marine-corps/; Jake Yeager. "Expeditionary Advanced Maritime Operations: How The Marine Corps Can Avoid Becoming A Second Land Army In The Pacific." War on the Rocks. 26 December 2019. https://warontherocks.com/2019/12/expeditionary-advanced-maritime-operations-how-the-marine-corps-can-avoid-becoming-a-second-land-army-in-the-pacific/; David Barno And Nora Bensahel. "A Striking New Vision For The Marines, And A Wakeup Call For The Other Services." War on the Rocks. 1 October 2019. https://warontherocks.com/2019/10/a-striking-new-vision-for-the-marines-and-a-wakeup-call-for-the-other-services/; Scott Cuomo, Olivia A. Garard, Noah Spataro, And Jeff Cummings. "Not Yet Openly At War, But Still Mostly At Peace: The Marine Corps' Roles And Missions In And Around Key Maritime Terrain." War on the Rocks. 23 October 2018. https://warontherocks.com/2018/10/not-yet-openly-at-war-but-still-mostly-at-peace-the-marine-corps-roles-and-missions-in-and-around-key-maritime-terrain/ ; Paul K. Van Riper. "Jeopardizing national security: What is happening to our Marine Corps?" Marine Times. 21 March 2022. https://www.marinecorpstimes.com/opinion/commentary/2022/03/21/jeopardizing-national-security-what-is-happening-to-our-marine-corps/ ; Tim Barrick. "On Future Wars and The Marine Corps: Asking The Right Questions." War on the Rocks. 12 April 2022. ; Marinus. "Is the Marine Corps abandoning maneuver warfare?" Marine Corps Gazette. April 2022. ; Gary C. Lehmann and Brian Kerg. "A Response to Maneuverist #19." Marine Corps Gazette. April 2022.

[11] David H. Berger. "The Case for Change." Marine Corps Association. June 2020. https://mca-marines.org/wp-content/uploads/The-Case-for-Change.pdf; David H. Berger And Ryan Evans. "A Chat With The Commandant: Gen. David H. Berger On The Marine Corps' New Direction." War on the Rocks. 6 April 2020. https://warontherocks.com/2020/04/a-chat-with-the-commandant-gen-david-h-berger-on-the-marine-corps-new-direction/ ; David H. Berger. "Notes On Designing The Marine Corps Of The Future." 5 December 2019. War on the Rocks. https://warontherocks.com/2019/12/notes-on-designing-the-marine-corps-of-the-future/

[12] Art Corbett. "Restoring the Initiative: A Discussion on the Assumptions and Concepts Shaping the Next Paradigm of Naval Warfare." Marine Corps Warfighting Laboratory, Combat Development & Integration. 3 December 2019.

As the Corps pursues development of these new concepts, focus has been placed on new options for ground-based missile fires in support of sea denial and sea control operations. Such capabilities to hold adversary vessels at risk are intended to complicate adversary decision-making, and hopefully to deter future conflict and militarized adventurism by regional actors that would otherwise pursue revisionist objectives through the *fait accompli* gambits and other campaigns backed by the threat or use of force.[13] New Navy and Marine Corps concepts will exploit positional advantage in the littorals, leveraging core expeditionary and amphibious operations competencies, to sustain U.S. and Allied presence even in the face of adversary counter-intervention planning, and associated long-range precision fires that would threaten traditional deployments using legacy large platforms.[14]

The successful execution of engagements involving these smaller, distributed, highly mobile and lethal forces will demand integrated strategy and planning, joint all domain command and control, robust ISR, enabled through resilient survivable networks. These forces will be opposed by adversary forces that will seek to deny the advantages conferred by these networks, and who will attempt to degrade systems and their connectivity—including the spectrum, maritime communications infrastructure, and space-based architectures upon which much of that connectivity will rely. This will impose new demands on the Fleet to defend our networks, and contest adversary presence and potential accesses therein. Changing operational concepts will also present new opportunities to bring offensive cyber capabilities into the fight in order to deny and degrade adversary performance and introduce uncertainties for decision-makers already facing previously unprecedented challenges to their malicious behaviors.

This research examines a selection of offensive cyber operations engagements and their potential outcomes in support of sea control and sea denial missions leveraging ground-based maritime precision fires in accordance with publicly-disclosed, unclassified capabilities and employment options. Scenarios and engagement parameters were validated in part through collaborative analysis and discussion, including "Hundred Fires" events held at the Naval War College and Atlantic Council's Cyber Statecraft Initiative in May and June 2020.[15] This

[13] Feng Zhang. "China's long march at sea: explaining Beijing's South China Sea strategy, 2009–2016." The Pacific Review. March 2019.; Suisheng Zhao. "China and the South China Sea Arbitration: Geopolitics Versus International Law." Journal of Contemporary China. Vol 27, issue 109: pp 1-15. 2018. ; Sugio Takahashi. "Development of gray-zone deterrence: concept building and lessons from Japan's experience." The Pacific Review. Vol 31 Issue 6, pp 787-810. 2018.; James R.Holmes, Toshi Yoshihara. "Deterring China in the 'Gray Zone': Lessons of the South China Sea for U.S. Alliances." Orbis. Volume 61, Issue 3: pp 322-339. 2017. ; James J. Wirtz. "Life in the 'Gray Zone': observations for contemporary strategists." Defense and Security Analysis. Vol 33 Issue 2: pp 106-114. 2017.

[14] Ryan D. Martinson. "Counter-intervention in Chinese naval strategy." Journal of Strategic Studies. March 2020.

[15] The author would like to thank Dr. Nina Kollars, Dr. Trey Herr, Col Art Corbett (USMC ret.), Dr. Xavier Bellekens, Mr. David Strachan, and Ms. Katie Blankenship - along with the many

effort builds on prior work through the Marine Corps University, Krulak Center and Expeditionary Warfare School on behalf of 12th Marine Regiment, 3rd Marine Division, III Marine Expeditionary Force, in order to consider potential Concepts of Operations (CONOPS) and new Tactics, Techniques, and Procedures (TTP), as well as ongoing wargaming conducted by the Command and Staff College (CSC), the School of Advanced Warfighting (SAW) and the Training and Education Command (TECOM) Warfighting Society.[16] This work is also a follow on to earlier wargaming examining cyber operations and related EW / Electromagnetic Spectrum Operations (EMSO) through different software platforms conducted as part of prior Marine Corps University SEA DRAGON exercises.[17] Ultimately, the approach for this study is also informed by earlier work at the Naval Postgraduate School on offshore control, which identified the potential role of littoral missile forces in holding naval formations at risk, and explored critical missile fires allocation and defensive intercept questions in salvo warfare.[18]

Wargaming as a means of testing novel concepts of naval integration, especially involving new technologies, platforms, and weapons systems, is of course by no means a recent development. This activity traces its lineage in an unbroken tradition of exercises within the U.S. Navy and Marine Corps over the past hundred years, and earlier to the Royal Navy's first experiments with the Jane's naval wargame—albeit to varying degrees of attention and analytic rigor at varying points within this period. The instrument is at its most useful, however, when the services are seeking to make sense of changing character of warfare and pursuing acquisitions, refining strategy, developing doctrine and tactics, and restricting organization to meet new demands shaped by altered missions as well as differing adversary capabilities and intentions.[19] This almost certainly encapsulates the current moment in consideration of future Navy and Fleet Marine Force operations. The "Hundred Fires" study effort aligns with this tradition. However, given that it involves mere simulation rather than extensive large scale unscripted free maneuver at sea and in the littorals, the effort should certainly not be taken as guidance, nor

---

joint, interagency, and multinational event participants for their support to the "Hundred Fires" efforts; as well as to gratefully acknowledge the unique national perspectives offered by Gen James Cartwright (USMC ret.) during these conversations.

[16] Steven Stansbury. "Wargaming Fleet Problems with Off-the-Shelf Games." BruteTalk, Krulak Center. 30 June 2020. ; Thomas J. Gordon IV, James Joyner, and Jorge Benitez. "May Madness: Competitive Wargaming In A Pandemic." War on the Rocks. 1 June 2020.

[17] Cyber Conflict Documentation Project. "Integration of cyber capabilities in crisis and conflict simulation: insights from U.S. Marine Corps University SEA DRAGON 3.0 Wargame." March 2018.

[18] Jeffrey R. Kline, Wayne P. Hughes Jr. "Flotilla to Support a Strategy of Offshore Control." Naval Postgraduate School. 2013. ; Casey M. Mahon. "A Littoral Combat Model for Land-Sea Missile Engagements", Naval Postgraduate School. September 2007.

[19] Craig C. Felker. *Testing American Sea Power: U.S. Navy Strategic Exercises, 1923–1940* (College Station: Texas A&M Press, 2007) ; Albert A. Nofi. *To Train the Fleet for War: The U.S. Navy Fleet Problems, 1923-1940*. Historical Monographs, Naval War College. 2010 ; Christopher Yi-Han Choy. "British War-Gaming, 1870-1914." King's College London. August 2013. ; John M. Lillard. *Playing War: Wargaming and U.S. Navy Preparations for World War II*. Potomac Books. 2016. ; Roger C. Mason. "Wargaming: its history and future." The International Journal of Intelligence, Security, and Public Affairs, 20:2, 77-101 (2018)

should this work be mistaken for official Combat Development and Integration planning activity.

Methodology

Engagements between adversary forces and multiple proposed variants of U.S. Navy and Marine Corps forces were simulated using the commercial off-the-shelf Command Modern Operations software package. The use of the Command platform has precedent elsewhere throughout DoD for multiple problems associated with acquisition, logistics, and core warfighting tactical and doctrine development.[20] Its predecessor wargame Harpoon has been used since the 1980's in miniatures form, and in the 1990's as software editions including in early efforts at the Naval War College.[21] A TECOM Warfighting Society scenario, previously used for wargaming of similar engagements for analysis of future operating concepts and force design, was selected as baseline. Simulated engagements occurred within three separate notional littoral areas selected from specific key INDOPACOM area geographies, representing contested straits and other close and confined seas. Each engagement took place within a 200 nautical mile (nm) by 200 nm area, with variable opposing forces geometries representing the conduct of differing transit and other missions. Weather variables were set to represent low intermittent cloud and light fog, variable moderate to heavy rains, with sea state conditions 4 to 5.

Simulated engagements were placed within a broader context of theatre-wide posture under conditions of conflict. U.S. and adversary forces not taking part in specific simulation actions were nonetheless represented for independent missions, along with neutral shipping and other third-party vessels and aircraft operations, in order to represent complexity of the battlespace and to simulate higher echelon factors that may influence a specific engagement.

Theatre level ISR assets were simulated and contributed to engagements for both sides. Blue Force theatre assets included: representations of multinational allied national technical means providing imagery, Synthetic Aperture Radar (SAR), Signals Intelligence (SIGINT) and other Measurement & Signature Intelligence (MASINT) capabilities, commercial satellite imagery assets, P8 maritime patrol aircraft, MQ-4C Triton and RQ-180A unmanned aerial vehicle systems, U-2S reconnaissance platform, as well as E-2D Hawkeye, E-3 Sentry, E-767 and E-7A Wedgetail Airborne Early Warning (AEW) platforms. Adversary theatre assets included: Yaogan / Jian Bing overhead imagery, SAR, and SIGINT platforms, Over the Horizon-Backscatter (OTH-B) and Over the Horizon-Surface Wave (OTH-SW) radar, terrestrial SIGINT / Electronic Intelligence (ELINT) stations, EA-03 Soar Dragon, Wing Loong II, BZK-005, and CH-5 Rainbow Unmanned Aerial Vehicle (UAVs), and GaoXin YJ-8 special mission aircraft, and KJ-200 / YJ-9 AEW platforms.[22]

---

[20] Iain McNeil. "Bringing Commercial games to Defence." Military Operations Research Society. 15 April 2020.

[21] Matthew B. Caffrey Jr. *On Wargaming: How Wargames Have Shaped History and How They May Shape the Future*. Naval War College Press. 2019.

[22] Jane's Intelligence Review. "Satellite imagery shows UAV display at China's Malan air base." 26 November 2019.; Jane's. "Chinese Electronic Mission Aircraft." 27 June 2019. ; Jane's. "Reviewing militarisation in the South China Sea." 4 October 2018. ; Jane's Intelligence Review. "China expands short-range maritime ISR capabilities." 29 December 2017. ; Jane's Intelligence Review. "China integrates long-range surveillance capabilities." 1 November 2017.

Control group simulations

An initial series of engagements between were simulated between pacing threat adversary formations and Blue Force units in order to establish a baseline observation set encompassing differing sensor, weapons systems, and operating condition mixes. Since this activity is explicitly not intended to assess platform selection or other comparative capabilities choices currently under consideration as part of future force design efforts, but rather the contribution of OCO options in differing scenarios, a robust range of potential force options based on publicly disclosed planning factors were gamed in order to ensure neutral observations. Due to announced focus on specific strike platforms including Naval Strike Missile, Maritime Strike Tomahawk, and a ground-based anti-ship ballistic missile capability (GB-ASBM), some systems did receive greater attention as part of a larger number of scenarios.[23] However, other comparative U.S. and Allied missile systems were also simulated to control for variables associated with weapons system design characteristics—including Harpoon, Long Range Anti-Ship Missile (LRASM), Exocet, and Hsiung Feng III platforms.

Some additional allied systems were considered for simulation, but could not be accurately modeled in the absence of effective terminal seeker design information for engagement of naval targets where the original fielded system may not have been intended for such roles, including the MdCN (Missile De Croisière Naval, a SCALP-EG / STORM SHADOW variant), Hyunmoo-3B, and BrahMos. Other adversary missile capabilities were also simulated in order to provide an alternative baseline of foreign weapons systems observations, including CSS-N-8 Saccade / YJ-83 / C802, SS-C-6 SENNIGHT / SS-N-25 SWITCHBLADE / 3M24 (Kh35) URAN, SS-C-5 STOOGE / SS-N-26 STROBILE / K-300P Bastion-P, SS-N-27 SIZZLER / 3M54T Kalibr, Khalij Fars [Fateh 110 Mod] ASBM, DF21-D / CSS-5 Mod 5, and DF-26 ASBM. Alternative systems simulation provided control group data by which to evaluate variables of offensive cyber effects separately from variations in missile performance characteristics. Systems were modeled under the assumption that previous Intermediate Nuclear Forces Treaty restrictions would no longer remain in force, following U.S. withdrawal from this agreement after unaddressed Russian forces violations with the deployment of operational SS-C-8 SCREWDRIVER/ 9M729 ground-launched cruise missile (GLCM) batteries in February 2017.[24] Despite ongoing discussion of hypersonic glide vehicle weapons in both U.S. and foreign testing, current USMC thinking has not yet moved in this direction despite apparent foreign belief that such systems would be a natural evolutionary pathway of the concept. [25] These systems were therefore excluded from scope of this paper.

---

[23] Megan Eckstein. "Marines Will Field Portfolio of JLTV-Mounted Anti-Ship Weapons in the Pacific" U.S. Naval Institute. 11 March 2020. ; Richard Burgess. "Commandant: Tomahawks Will Enable Marines to Contribute to Sea Control, Denial." Sea Power Magazine. 5 March 2020. ; Sam LaGrone. "Raytheon to Arm Marine Corps with Anti-Ship Missiles in $47M Deal." U.S. Naval Institute. 8 May 2019. ; Megan Eckstein. "Marines Want to Field a Long-Range Anti-Ship Missile 'As Fast As Possible'." U.S. Naval Institute. 19 February 2019.

[24] Shannon Bugos, "U.S. Completes INF Treaty Withdrawal," Arms Control Today, 19:7, 24-25. (2019)

[25] Andrew Jensen. "China's Reactions to USMC Pursuit of GBASM Systems." Seeing Red. Deputy Commandant for Information, Vandegrift Team. 2 July 2020. ; Megan Eckstein. "DARPA Asked Marines to Consider Adding Land-Based Hypersonic Weapons to Arsenal, But USMC Not Interested." USNI News. 18 June 2020.

All Blue Force systems, regardless of individual munitions selection, were simulated as part of notional restructured USMC expeditionary elements consistent with the Marine Littoral Regiment concept. Opposing forces were modeled across five different notional adversary missions: a carrier strike group, an expeditionary strike group, a naval surface action group, an escorted shipping convoy, and a light patrol formation (representing adversary harassment or commerce raiding missions).[26] Forces were represented variably operating under Emissions Control (EMCON) for low signature maneuver, or using full active sensor options (including air search and surface search radars) for force protection. Forces under EMCON restrictions could be cued by theatre level ISR assets or organic passive sensor detection (including passive radar systems, or other radar warning receivers / Electronic Support Measure [ESM] / ELINT systems) alerting to incoming threats, in which case units would react with appropriate immediate use of active sensors.

Traditional current generation EW / EMSO capabilities were represented in control group simulations. These effects included Electronic Attack (EA) jamming and Electronic Protect (EP) defensive electronic countermeasures focused on the radio frequency spectrum, as well as defensive chaff and spectral decoy systems. Advanced cyber – electromagnetic activity (CEMA) options were not represented in conventional control engagements due to limited public detail; these were considered in abstracted fashion under the range of offensive cyber effects simulated as part of experimental engagements (as discussed below).

Simulating Offensive Cyber Effects

Wargaming offensive cyber operations often faces substantial challenges due classification limitations. However, the cyber warfighting domain is unique in that a high percentage of contemporary interactions play out across systems and networks owned and operated by the private sector. Industry cyber intelligence and other security research therefore can provide a robust foundation for unclassified simulation of representative cyber capabilities. While the fidelity of these options may not be fully representative of unique "NOBUS" (Nobody But U.S.) classified TTP that perhaps might be considered in other settings, there remains substantial utility in understanding the substantial insights possible solely from the open source. In particular, the open-source intelligence picture becomes even more important when considering that these topics have been the focus of specific Chinese government interest and similar analysis is almost certainly being conducted at the direction of Beijing.[27]

Access and Effects Abstractions

Based on open-source intelligence and other published analysis, one may observe a range of potential CONOPs for access and effects delivery against relevant systems and networks identified within the scenario set. For the purposes of this analysis, much of these activities

[26] A fictional scenario describing engagement of a convoy target may be seen in Dustin League and Dan Justice. "Sink 'Em All: Envisioning Marine Corps Maritime Interdiction." Center for International Maritime Security. 8 June 2020.
[27] Andrew Jensen. "China's Perspectives on the U.S. Marine Corps' Littoral Combat Regiments." Seeing Red. Deputy Commandant for Information, Vandegrift Team. 26 June 2020.

may be abstracted above the level of technical detail describing tactical interactions "on the wire" at the level of offensive operator visibility—much as the wargame's simulation engine abstracts the specifics of a fighter pilot's cockpit or ship's damage control team. Rather, the appropriate focus is placed at the level of operational effect: representing compromise of confidentiality, availability, and integrity of targeted compute and the military utility that depends on that compute. This is consistent with longstanding DoD and industry cybersecurity practices when evaluating hostile interactions across targeted systems and networks.[28] There is however a solid unclassified basis for asserting plausibility of these effects in abstracted fashion, briefly summarized as follows.

The maritime domain and littoral operating environment does pose certain unique problems that are not always specifically identified in finished cyber intelligence which is traditionally more focused on corporate enterprise and critical infrastructure networks ashore. These can include: questions of operations involving specific shipboard systems, satellite links, undersea nodes, and discrete weapons systems elements such as radar and sonar components, electro-optical and other sensors, missile and torpedo launchers, navigation components, electronic warfare suites, as well as emerging autonomous operations logic functions. However, while these unique systems pose new challenges of access and of exploitation, substantial industry research has identified both potential vulnerabilities and opportunities, as well as relevant capabilities observed in the wild. Such research has included exploration of potential compromise of communication datalink systems, with focus on unmanned systems command and control as well as cooperative engagement capabilities.[29] Satellite communications systems and navigation technologies have also seen particularly intense focus.[30] New research is further extending these intrusion concepts into novel undersea network technologies.[31] The notional compromise of ship systems also reportedly featured in NATO exercise SABRE GUARDIAN in 2017, in which planners were forced to consider options for offensive cyber intrusion against a

[28] Defense Science Board. *Security Controls for Computer Systems*. February 1970. DECLASSIFIED; James P. Anderson. "Computer Security Technology Planning Study." Electronic Systems Division, U.S. Air Force. 1972. ; J. H. Saltzer, & M. D. Schroeder, "The protection of information in computer systems." Proceedings of the IEEE, 63(9), 1278-1308. 1975 ; D. E. Bell, L. J. La Padula. "Secure Computer System: Unified Exposition and Multics Interpretation." Technical Report ESD-TR-75-306, The MITRE Corporation, Bedford, MA. 1975; K.J. Biba. "Integrity Considerations for Secure Computer Systems." Technical Report MTR-3153, MITRE Corporation, Bedford, MA. 1976; David Clark, David Wilson. "A comparison of commercial and military computer security policies." IEEE Symposium on Security and Privacy. 1987.

[29] Daniel Moore. "Targeting technology: Mapping military offensive network operations." In 10th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia. 29 May - 1 June 2018. ; Ugur Akyazi. "Possible Scenarios and Maneuvers for Cyber Operational Area." In Andrew Liaropoulos and George Tsihrintzis [eds]. 13th European Conference on Cyber Warfare and Security (ECCWS). University of Piraeus, Greece. 3-4 July 2014.; Richard S. Stansbury, Manan A. Vyas, Timothy A. Wilson. "A Survey of UAS Technologies for Command, Control, and Communication (C3)." Kimon P. Valavanis, Paul Oh, Les Piegl [eds]. Unmanned Aircraft Systems. Springer. 2008.

[30] Air Force Research Laboratory. "Space Security Challenge (SSC) 2020 Hack-A-Sat (HAS): Rules." 23 June 2020. ; Colby Moore. "Spread Spectrum Satcom Hacking." Black Hat USA, Las Vegas. 2015. ; Ruben Santamarta. "SATCOM Terminals: Hacking by Air, Sea, and Land." Black Hat USA, Las Vegas 2014. ; Adam Laurie. "Satellite Hacking for Fun and Profit." Black Hat DC. 2009.

[31] David Strachan. "Cyber in the Undersea." Strikepod Systems. 25 June 2020. https://www.strikepod.com/cuber-implications-for-microsubmarines/

merchant vessel carrying gray arms being smuggled to supply an adversary irregular force of "little green men," where OCO effects in this exercise were sought to enable Visit, Board, Search and Seizure (VBSS) operations. [32]

Public information regarding offensive cyber options against Integrated Air Defense (IADS) networks is more limited. This becomes highly salient when considering adversary reef fortifications that may provide overwatch to naval formations, or when analyzing effects against shipboard radar and surface to air missile systems that are navalized variants of known IADS components. However, open-source analysis has suggested operational employment of such capabilities in support of strike sorties by Israeli Air Force, which penetrated defended Syrian airspace to destroy undisclosed nuclear facilities. The capability employed in this action has never been acknowledged, however multiple analysts have characterized this as an early cyber network attack (CNA) example.[33] Chinese defense analysts have also quite intently focused on the case in numerous contexts, alleging similarities to U.S. experimentation and acquisition efforts known under the term "Project SUTER".[34] Only limited information regarding such capabilities have been disclosed to date by Department of Defense, and it remains unclear the extent to which PLA authors have accurately evaluated specific systems or programs.[35] However, it is clear that the topic remains quite prominent in their thinking.

---

[32]Cyber Conflict Documentation Project. "Russian navigation warfare: understanding hostile intentions and recent incidents." November 2017.

[33] Thomas Rid. "Cyber war will not take place." Journal of Strategic Studies 35, no. 1 (2012): 5-32.; Lior Tabansky, and Isaac Ben Israel. "Striking with Bits? The IDF and Cyber-Warfare." In *Cybersecurity in Israel*, pp. 63-69. (Cham: Springer) 2015. Slawomir Dygnatowski, Pawel Dygnatowski, Lukasz Domzal-Drzewicki. "Analysis Of Using Structural Solutions In Cybersecurity Based On Orchard Operation." Journal of Konbin (Air Force Institute of Technology, Poland). Vol 49. 2019.; Jason Healey, Divyam Nandrajog. "Understanding Cyber Effects on Battlefield Outcomes. Columbia University. June 2019. ; Robert Dalsjö, Christofer Berglund, Michael Jonsson. *Bursting the Bubble: Russian A2/AD in the Baltic Sea Region*. Defense Research Agency (FOI), Ministry of Defense, Sweden. 2019.

[34] Min Zhao. "Network Attack of Network Centric Warfare: Project Suter." Journal of Modern Defence Technology 39, no. 6 (2011): 139-143.; Liu Min, Xing Zhao. "Offense and Defense Technology in Cyberwar——Analysis on Project Suter." Command Information System and Technology 4 (2011).; Ren-Quan Huang, Wei-Min Li, Chun-Yang Wang, and Xiao-Jun He. "UML and petri net model of the air defense system countering the cyber attack." Journal of Modern Defence Technology 40, no. 2 (2012): 17-23.; Zhou Fang. "Human behavior description method of cyber countermeasure based on properties combination." Computer Engineering and Design 8 (2013): 17.; Su Kang, Huang Yan, and Wang Kui. "Study on cyberspace hierarchical structure and countermeasures function requirement in battlefield." Aerospace Electronic Warfare 3 (2013): 10; Sun Xin Feng, Fei Hong Zhao, and Zhu Hong. "U.S. Military Foundational Cyberwarfare Plan X." Command Information System and Technology 3 (2013).; Zhang Lu, Hong Liang, and Chen Wu. "Research of Cyberspace Countermeasure Based on Information Technology [J]." Computer Technology and Development 24, no. 6 (2014): 208-210.

[35] Michael W. Garrambone. "Human Factors: Conducting Over the Shoulder Assessment for Military Exercises and Experiments." MORS Workshop: Bringing Analytical Rigor to Joint Warfighting Experimentation: Design, Planning, Execution, Analysis and Reporting. Military Operations Research Society. 3-5 October 2006.; John F. Vona. "Global Effects: Pilot Explores Integrated Command and Control." High Frontier, The Journal for Space & Missile Professionals. Volume 5, Number 3, May 2009.; Matt J. Butler. "Rapid Delivery of Cyber Capabilities: Evaluation of the Requirement for a Rapid Cyber Acquisition Process" Air Force Institute of Technology, Air University. 2012.

Beyond generalized statements about alleged undisclosed prior operations, however, there is substantial open-source information upon which to identify a range of likely vulnerabilities and exploitation scenarios in contemporary threat Surface-to-Air Missile (SAM) systems. Of particular example are onboard computing architectures incorporated in the design of the S-300 / S-400 platform family. These systems were originally developed from the 1980's onward using a proprietary Soviet (and later Russian) processor architecture iterated across multiple generations.

The latest publicly known variant of this architecture is the ELBRUS chipset and associated operating system, a clone of Western SPARC processor designs running a modified variant of an older Linux kernel.[36] This Russian computing architecture is known to have been developed from designs stolen as part of technical espionage operations against Western firms by the Russian foreign intelligence service.[37] The developer claims proprietary modifications to this processor and its operating system intended to defeat a number of technical exploitation options commonly used against commercial enterprise architecture, features which the government of Russia has previously highlighted in earlier worm-able malware outbreak crisis events.[38] However, it remains likely that exploitation options known to be available against the original SPARC environments may be adapted to the ELBRUS target. These options include specific vulnerabilities and associated exploits that remained undisclosed for nearly twenty years in the West.[39] Similar options are almost certainly available against other Russian systems, and their later Chinese derivatives, including here relevant HQ-17A (a clone of the SA-15 GAUNTLET / TOR) and HQ-9 systems.

Representative capabilities

While the simulation software developer studio did incorporate some degree of cyber effects within scenarios intended for commercial release, these are relatively immature in existing form and were generally not suitable for robust comparative analysis as constructed. The designers did however offer scripting options to represent additional capabilities, as well as other robust scenario editing functions that in combination can deliver viable simulation of key capabilities and associated effects.

Representing the complex systems of systems which must be targeted to achieve relevant cyber effects under scenario conditions is a substantial challenge. The existing simulation at present models a wide range of ship, aircraft, and facility systems, along with their associated networks, and interoperability at varying levels of fidelity depending on unit type, technology generation, and relevance to previously defined tactical resolution

[36] Sudonull. "Climbing Elbrus - Reconnaissance in battle. Technical Part 1. Registers, stacks and other technical details." April 2019.; Sudonull. "Climbing Elbrus - Reconnaissance in battle. Technical Part 2. Interrupts, exceptions, system timer." April 2019.
[37] JD Work. "Early intelligence assessments of COMBLOC computing." Journal of Intelligence History. 2021.
[38] Roman M. Rusiaev, Murad I. Neiman-Zade, Alexandr V. Ermolitsky, Valery I. Perekatov, Vladimir Yu. Volkonsky. "Various Buffer Overflow Detection Means for Elbrus Microprocessors." International Conference on Engineering and Telecommunication (EnT). Moscow. 29-30 November 2016.; Andrew E. Kramer. "Russia, This Time the Victim of a Cyberattack, Voices Outrage." New York Times. 14 May 2017.
[39] Marco Ivaldi (raptor). "A Bug's Life: Story of a Solaris 0day." INFILTRATE. Miami, FL. 2 May 2019.

factors. Thus, designers have extensively modeled sensor systems and weapons functions, and have further incorporated elements considering radio communications and datalink performance (including those operating within a contested electronic warfare spectrum). Additionally, command and control factors are represented through an Observe, Orient, Decide, Act (OODA) loop model that simulates a time factor for receipt and action on changing information.

For the purposes of this study, offensive cyber effects resulting in compromise of systems and network confidentiality, integrity, and availability were represented through several mechanisms. The most frequently leveraged mechanism was to designate the involved specific systems components as having been damaged, as the simulation engine already incorporated robust mechanisms to model the loss of shipboard, sensor, and weapon systems functionality within engagements—along with damage control processes that would result in repair and restoration of components where recoverable. This mechanism simulated offensive cyber effects seeking to deny or degrade availability, encompassing both deliberately destructive and optionally reversible effects options. Additional integrity effects could also be represented, through introduction of simulated decoy contacts, distorted inventory / ships-stores management, and forced loss of sensor contact / weapons track. These effects required careful review and manual editing to ensure simulation fidelity in current generation of the software package. It is hoped that future software iterations will enable more seamless and robust automation.

Acknowledged simulation limitations

Simulation of offensive cyber effects did not extend to weapon sensor level interactions. There is likely utility in exploring these effects, especially for systems where the function of the terminal seeker may prove a critical variable in engagement scenarios. Likewise, integrity and successful function of individual munitions were not addressed, although prospective failures of complex systems and associated maintenance and update processes can readily be envisioned—especially for networked weapons systems reliant on datalinks, navigation systems, flight planning software, and adaptive fusing mechanisms.

Compromise of processing, exploitation, and dissemination architectures associated with ISR capabilities were also not simulated; where cyber effects may be introduced to complicate detection or alter integrity. Effects executed directly against national technical means, including on-orbit architectures, and their commercial systems counterparts were also considered out of scope of the current study.

Cyber physical effects through manipulation of shipboard industrial control systems networks to cause direct damage to the vessel were also not explored. Such damage mechanisms may be simulated at present, including through events such as failures of engine or electrical systems resulting in shipboard fire, but were outside the scope of the study.

Further, no attempt was made here to simulate offensive cyber operations against nuclear command and control targets. Nuclear weapons systems and their employment were not considered within the scope of these scenarios.

Key Insights from Simulated Engagements

Simulated engagement outcomes across 163 actions are presented in appendix, breaking down variable adversary losses and damaged vessels across various target formations for both control group engagements testing differing missile types under classic engagement conditions, versus engagements involving variable OCO options. Despite deliberate simulation of high numbers of engagements, engagement outcome results were not tested through quantitative analysis techniques due to the large number of nested variable conditions represented within the software package. These included changing conditions related to ISR and weapons sensor performance, unit command / control / communications and individual systems operator behaviors, electronic warfare / decoy effects, weapons behavior modeling, weather / environmental conditions, and other factors calculated as part of the designer's intent towards offering a high-fidelity representation of contemporary naval combat. Rather, this effort instead focused on identifying the high level, qualitative insights that may help inform complex decision-making regarding planning and integration of offensive cyber operations with new future joint and maritime operating concepts. A number of useful insights did indeed emerge from watching these simulated engagements unfold.

Complex Heterogenous Targets

The first and perhaps most central observation is that achieving significant offensive cyber effects at the tactical level supporting precision ground-based missile fires against targets afloat necessarily involves access to, and exploitation of, multiple complex heterogenous military systems and networks. There is no single cyber "silver bullet". The salient functional components within an adversary surface warship are substantially varied and demand unique consideration, especially in ship classes that have undergone modernization from legacy inventory to more current systems. These are further complicated by offboard capabilities—including supporting ISR architectures, logistics systems, precision navigation and timing systems, and communications links. While commonalities of exploitation options may be explored, there is undoubtably a need to tailor both delivery and payloads across these diverse equipment sets and configurations. It is unreasonable to believe that a capability will be in hand for every system, in every deployment and operational mode, at all times and in all geographic environments. The substantial investment required to provide high confidence options to combatant commanders across even a substantial fraction of relevant targets is highlighted.

Having acknowledged this difficulty, these constraints then demand focus on maximization of what may be scarce options to achieve most significant impact for high payoff systems targets. Effects intended to deny and degrade engagement management functions, cooperative engagement capabilities, and associated datalinks demonstrably offer advantage in achieving greater hit and kill percentages. BELL THUMB, LIGHT BULB, as well as the newer BAND STAND and HN-900 systems are therefore higher payoff targets.[40] Such advantage may however be fleeting where the adversary may revert to manual modes of operation. That fleeting window is nonetheless potentially important within the relentless pace of contemporary missile warfare. Likewise, the ability to deliver effects where adversary design may have unwisely created centralization of systems

[40] James C. Bussert and Bruce A. Elleman. *People's Liberation Army Navy: Combat System Technology, 1949-2010.* Naval Institute Press. 2011.

interdependencies suggests the potential for effects to be extended across clusters of intertwined components, such as where specific industrial control systems components may allow degradation of power distribution, or where common design features may allow disruption of shipboard systems. Vertical Launch System (VLS) automation appears to offer such a candidate target. Embedded VxWorks real time operating system components and other similar automation technologies are also promising candidate attack surfaces for such effects.[41] However, these unique opportunities may not be tactically addressable in the context of an immediate engagement—although such engagements were modeled with results demonstrating that if such targets may be serviced, benefits accrue to the attacker.

While simulation here focused largely on individual functional component impact, the combined capabilities offered by multiple systems performing variants of the same function become highly significant. For example, one sees such interactions between modern air search radars, and overlapping contributions to common operating picture from surface search radars designed to support detection of incoming sea-skimming cruise missile contacts. If not anticipated, such redundancy may render ineffective lengthy investment in certain complex, difficult OCO options.

Low Observable Missile Designs and Terminal Seeker Mode Role in Air Defense Detection and Intercept

In both control group simulations, and under differing OCO supported engagements, the design of specific missile systems emerged as a significant feature in outcomes of adversary ships sunk and / or damaged. Low-observable design characteristics demonstrated substantial value in all conditions. It is certainly of no surprise to note that stealth is a game changer in modern missile warfare and air defense problems, and is a finding consistent with longstanding research.[42] Low-observable designs reduce detection ranges for most air defense radar systems, thereby also reducing adversary reaction time and window for effective intercept through SAM fires. The percentage of successful intercepts by SAM and point defense systems is also reduced when operating against low-observable systems designs, over legacy designs.

Terminal seeker operating modes play a key role in this equation. Even where airframe signature reduction may have inhibited successful radar track, especially in sea-skimming flight profiles where background wave clutter can be significant in some sea states, active terminal guidance offers the adversary some improved engagement opportunities. As a result, weapon systems relying on passive infrared imaging sensors rather than active radar emitters suggest certain advantages, including reduced adversary reaction time provided by Radar Warning (RWR) and other Electronic Support Measures (ESM) systems. This advantage however faces tradeoffs when facing multi-spectral decoys, where multi-mode seekers may be less readily spoofed. In these engagements,

[41] James C. Bussert. "Chinese Warships Struggle to Meet New Command, Control and Communications Needs." SIGNAL. February 2009.

[42] Walter M. Locke. "Cruise missile system design." 16th Annual Meeting and Technical Display. American Institute of Aeronautics and Astronautics. Long Beach, CA. 12-14 May 1981. ; Jasper Welch. Assessing the Value of Stealthy Aircraft and Cruise Missiles. International Security. Vol 14 No 2 : 47-63. 1989. ; Myron Hura, Gary W. McLeod. Route Planning Issues for Low Observable Aircraft and Cruise Missiles. RAND. 1993. ; Lee O. Upton and Lewis A. Thurman. "Radars for the Detection and Tracking of Cruise Missiles." Lincoln Laboratory Journal. Vol 12 No 2. 2000.

OCO effects against adversary RWR / ESM systems may provide unique advantage. The growing trend towards integration of such systems into more complex, networked ELINT architectures also provides potentially useful exploitable attack surfaces. In particular, PLAN adapted Western equipment like the ELETTRONICA S.p.A. ELT / Newton family of ESM / ECM solutions is representative of such potential target architecture.[43]

The introduction of new passive radar systems into these equations likely changes engagement tactics for both sides. PLAN has actively pursued passive radar adoption for newer generation ship designs, including the Russian origin Mineral-ME complex.[44] Effective OCO and EW options against the interactions between these systems and other emitter sources in the environment may be unique in ways not simulated here by simple damage calculations.

High Payoff Effects Against Adversary Sensing and Engagement in Area and Point Defense

Observed simulated engagements suggest that the highest payoff for offensive cyber effects comes from impact to degrade adversary cooperative air defense engagement processes. While direct effects against specific air defense capabilities may be highly desirable, this is matched with concurrent difficulty in access, exploitation, and payload design. Actions against battle management functions may therefore yield good result for relative investment demand. In particular, actions which may degrade performance even where SAM or point defense systems performance is untouched show promise. These may include handoff between systems components, including from search to tracking radars, from radar to weapons datalinks, and from ship to ship. It is important to note that degraded-but-otherwise-apparently-operational equipment produces critical uncertainty for adversary leadership in response under fire. In these cases, failure to adapt to ensure defensive fires from alternative systems even where overlapping options exist may result in the creation of a window of attacker advantage not otherwise manifest.

These fleeting opportunities are further significant at faster engagement speeds involving both defender and attacker weapons selections. The performance of certain foreign supersonic cruise missile systems was highly notable in control group simulations, demonstrating more effective hits due to shortened defensive engagement windows. Even OCO effects that may seem marginal for other missile designs therefore may prove to be more important in engagements involving these systems. Likewise, one sees similar dynamics in the very short engagement timeframes and intercept envelops that characterize response to ballistic missile threats, and likely future hypersonic weapons systems.

The value of decoy systems and other penetration aids in defeating integrated air defense systems targets has long been understood. Substantial payoff is likely found in cyber effects duplicating these complications for the targeted formation. Where physical decoy platforms were simulated, key concerns regarding launch techniques emerged given that traditional decoy systems often did not offer volley fire options nor flight profile

[43] Joris Janssen Lok. "Integrated electronic warfare is critical to modern surface ships." Jane's International Defense Review. 1 July 2005. ; Garth Hekler. "Chinese Early Warning Aircraft, Electronic Warfare, and Maritime C4ISR." In Andrew Erickson and Lyle Goldstein [eds]. *Chinese Aerospace Power: Evolving Maritime Roles*. Naval Institute Press. 2012

[44] Paul Schwartz. "Russia's contributions to China's surface warfare capabilities." Center for Strategic and International Studies. 2015.

options to match cruise missile delivery system operations. Launch bottlenecks, formation assembly, and other factors may complicate effective utilization, especially in platforms with limited fuel inventories and operating ranges. It is therefore natural to look to OCO options to create similar effects, where kinetic systems pose difficulties. However, it should be noted that classic radio frequency EW techniques have long offered options to deliver false contacts, seductive decoys, and other similar effects, and these are complex interactions that may be less suitable as higher level OCO objectives.

Flight Profile and Pre-Planned / Autonomous Engagement Planning

The role of flight planning in cruise missile fires is also highlighted in these engagements. The problem of optimized allocation of missiles against multiple targets is a longstanding area of research interest, and particularly so in recent Chinese military thinking. Multiple engagement strategies may be considered under differing conditions and against differing adversary air defense approaches.[45]

These factors are further complicated by offensive cyber interactions, where different target system components may be denied or degraded in specific vessels that service differing roles in layered defense approaches, have different relative positions within a target formation, against the variables of differing axes of attack based on a given attacking fires allocation decision. Specific offensive cyber effects impacting attacker missile waypoint designation and flight profile performance may also be considered, but were not simulated in the current study. Likewise, allocation of defensive SAM and point defense fires may be impacted by offensive cyber effects, de-optimizing defender engagement strategies in ways that may be non-obvious but of substantial advantage in short, sharp confrontations, especially where surprise may result from successful ambush. Additional future research to test these variables is likely called for.

Missile flight logic representation in the current simulation engine also did not permit robust coordinated swarm behaviors. While this is consistent with current weapons

[45] Martijn van Ee. "On efficient algorithms for finding efficient salvo policies." Naval Research Logistics. Vol 67 Issue 2: pp 147-158. 2020. ; Zongang Liu ; Jiaguo Lu ; Zhen Dong. "Research on Penetration Technology of Intelligent Cluster Missile System." IEEE International Conference on Robots & Intelligent System (ICRIS). Haikou, China. 15-16 June 2019 ; Jie Zeng, Lihua Dou & Bin Xin. "Multi-Objective Cooperative Salvo Attack Against Group Target." Vol 31 : pp 244–261. 2018. ; Michael J. Armstrong. "The salvo combat model with area fire." Naval Research Logistics. Vol 60 Issue 8: pp 652-660. 2013. ; ZHANG Yi, JIANG Qing-shan, CHEN Guo-sheng. "Dynamic weapon-target assignment with conditional value-at-risk." Systems Engineering and Electronics. 2012. ; YANG Fei, DONG Chao-yang, WANG Qing. "Decision-making of Saturation Attack for Anti-ship Missile Weapon-target Assignment with multiple targets." Journal of System Simulation. 2011. ; Alexandra M. Newman Richard E. Rosenthal Javier Salmerón Gerald G. Brown Wilson Price Anton Rowe Charles F. Fennemore Robert L. Taft. "Optimizing assignment of Tomahawk cruise missile missions to firing units." Naval Research Logistics. Vol 58 Issue 3: pp 281-294. 2011. ; Stéphane LeMénec, Hyo-SangShin, AntoniosTsourdos, BrianWhite, Rafal Zbikowski, Keith Markham. "Cooperative Missile Guidance Strategies for Maritime Area Air Defence." 1st IFAC Workshop on Estimation and Control of Networked Systems. IFAC Proceedings, Vol 42 Issue 20: pp 264-269. 2009.; Michael J. Armstrong. "Effective Attacks in the Salvo Combat Model: Salvo Sizes and Quantities of Targets." Naval Research Logistics. Vol 54 Issue 1: pp 66-77. 2006. ; LI Da-jian, WANG Feng-shan. "Optimizing Research On Firepower Assigning of Cruise Missile's Attack Under Multiple Air Defense." Journal of Projectiles, Rockets, Missiles and Guidance. 2005.;

system platforms, ongoing efforts towards coordinated networked fires permitting dynamic re-allocation of missiles to targets are now sought by multiple services as part of aspirational, next generation capabilities. Such features would also be usefully simulated in future study iterations, and may introduce options for salient cyber effects. These engagements also point to the increasing future importance of algorithmic warfare, where operations are not merely aimed to create effects within a specific system or network but rather in the interactions and decision logics of sensor, processing, and application. These are new frontiers in offensive cyber operations, the outlines of which are only dimly glimpsed at present.

Integration with EW Options

Regardless of offensive cyber effects employment decisions, coordinating such effects with RF spectrum focused EW measures remains critical. EW platforms remain high demand, low density assets in the current and anticipated joint force. Simulated engagements highlight the need for a lower cost, attritable capabilities mix. These may include unmanned systems, expendable munitions, or other unconventional solutions. The need for integration of these options, including consideration of potential new organic capabilities for Marine Littoral Regiment force constructs, emerges clearly from simulation. In particular, a ground launched expendable escort jamming system with similar signature and flight characteristics as primary missile systems may yield substantial value for strike elements, especially if such a system is employed in conjunction with specific offensive cyber effects options. PLA authors have themselves focused recent interest in similar EW concepts, including development of their own organic capabilities to support PLAN naval surface action groups, as well as their own "Blue Teaming" analysis intended to identify countering options for likely anticipated U.S. and allied capabilities and their employment.[46] Further EW specific research is called for.

Battery Signature Management

The survivability of expeditionary advanced base elements will remain a key concern in any future operating concept. In these engagements, it became clear that the signatures associated with launch sites and firing batteries are a critical variable of survivability, especially in the face of increasingly robust adversary ISR capabilities ranging from new UAV platforms to national technical means and their commercial counterparts. This places a substantial premium on camouflage, concealment, and deception for forward positions that by their nature will be within the adversary's weapons engagement zone; and raises considerations of rapid hardening options. These dynamics also create new considerations for elements that may face detect on launch scenarios, where a new requirement may emerge for missile systems offering reduced signature fires options or operating modes. Likewise, flight planning considerations will become important where an adversary may initiate counter-fires using autonomous and loitering munitions along simple back-bearing vectors, or across other insufficient random features of engagement geometries where the

[46] GUO Junliang, QIN Jiandong. "Application of UAV in surface warship electronic warfare anti-missile combat." Electronic Design Engineering. Vol 27 No 3: 67-75. 2019. ; HE Yong-xi. "Tactics Deduction of Support Jamming for EW UAV." Shipboard Electronic Countermeasure. Vol 40 No 4: 14-19. 2017. ; XIE Jing, LIU Zhipeng. "UAV application and influence in maritime electronic warfare." Science and Technology Innovation Herald. No 1. 2014. ; YE Ruifang, WU Tanran, REN Xiangyu. "The future development of foreign military electronic warfare UAVs." Aerospace Electronic Warfare. Vol 29 No 2: 12-15. 2013.

theoretic advantage of littoral background clutter may be lost in practice. In the cyber domain, related concerns develop regarding hostile signals intelligence (SIGINT) and adversary OCO threat, especially where the adversary may be hunting autonomous systems and high data demand common operating picture architectures.

Within this context, study participants have identified concerns regarding operations in coalition environments where the adversary may have for years in advance of crisis pursued the compromise of Allied and partner critical infrastructure networks vital to supporting advance elements. This may include local telecommunications infrastructure, port facilities, and other entities that may provide appropriate contract logistics support needs. It is anticipated that the adversary will continue to enjoy the greater opportunities for access and operational preparation of the environment afforded by more open and commercially oriented societies, in comparison to the more difficult challenges faced by U.S. and allied planners in considering operations against closed networks supporting adversary deployment from within denied areas. In this, the future expansion of the (One) Belt and (One) Road Initiative (OBOR, BRI) may feature as prominent key network terrain for contested position and future objectives.

Implications and Outlook

This study in many ways validates and restates well known naval combat principles established since the dawn of the missile age, and in the antecedents of campaigns long before Goddard's inventions were adapted for the fleet. It remains clear that the adage "a ship's a fool to fight a fort" continues to be true, regardless of whether it was Lord Nelson or Admiral Sir "Jackie" Fisher that said it.[47] In control group simulations, the maxim that the victor "must fire effectively first" is also proven once again.[48] Effective fires—in the form of good hits from attacking munitions—are the *sine qua non* of sea denial and associated conventional deterrence achieved through surface to surface missile batteries deployed as envisioned in expeditionary advanced base operations concepts. These hits must be achieved even in the face of what will inevitably be robust surface to air missile and other point defense intercept attempts mounted by the targeted opposing force formations. The calculus for effective exchanges in salvo warfare involving missile systems remains at its heart an attrition problem, modified by the fleeting timespan of specific engagements based on range, detection characteristics, and engagement geometries.

Offensive cyber operations options promise the potential to change these calculations in favor of the side that can muster and employ such capabilities to their advantage. This is by no means an easy problem, and it requires a very different kind of thinking than is traditional within other warfare communities. There remains substantial pressure to reduce the complexity, nuance, and unique technical and tactical characteristics of cyber warfighting to a single expressed variable of "cyber fires" so that such non-kinetic effects may be treated interchangeably with other fires options by commanders, planners, and policymakers. These pressures are entirely understandable from the perspectives of

[47] Larrie D. Ferreiro. "Horatio Nelson Never Wrote 'A Ship's a Fool to Fight a Fort'; It Was Jackie Fisher Who Invented the Attribution." Journal of Military History. Vol 83 Issue 3 : pp 855-856. July 2016.
[48] Wayne Hughes, Robert Girrier. *Fleet Tactics and Naval Operations, Third Edition*. Naval Institute Press. 2018.

operational and strategic need. However, this often elides the substantial contest of access, position, and fleeting opportunity that is required to muster a capability at a given moment sufficient to allow for its invocation as in the joint and combined fires construct. This disconnect often gives rise to decision-maker skepticism—if not outright dismissal—regarding the reliability and repeatability of OCO options. Such reactions may be in part warranted when a commander has all of the resources, time, and advantage by which to employ them against an adversary that is only capable of responding by further hiding, or through asymmetric means. However, when facing a peer competitor that may possess hardened anti-access / area denial options, superiority in fires ranges, hull counts, warship tonnage, and afloat weapons systems capabilities it is perhaps wise to consider where additional options may generate advantage, even if one must accept that such advantage influences at the margins of specific engagement scenarios.

These features may at first seem to raise fundamental questions about the viability and purpose of the entire cyber warfighting enterprise, at least in this context. Yet, it is the very character of contemporary naval engagements that make these impacts at the margins something well worth striving to achieve. Salvo warfare involving missile exchanges is notable for tactical instability, arising from concentration of combat power relative to survivability that results in the difference between loss and victory based on even small changes between attacker and defender.[49] As is clear from simulation results in the appendix, "Appendix: Simulated Engagement Results," the changes introduced by select OCO effects indeed demonstrate the ability to exacerbate this instability to obtain advantage over the adversary, with greater numbers of adversary vessels damaged or sunk where OCO options were employed in support of missile fires.

The ability to achieve such advantage is subject to the success of operational action in and through the cyber domain, overcoming challenges of access, payload delivery, and effects orchestration in a complex range of targets. It is also subject to limitations of authorities, equities and associated approval processes not discussed here but that remain highly salient to potential engagement scenarios.

While the calculation of fires exchanges in Lanchester's Square Law, Hughes' salvo combat model, and its successive iterations is familiar to naval officers (and increasingly now to officers of Marines), the introduction of OCO also introduces another key set of equations into the full contact math of naval combat. These are the calculations inherent in the management of the arsenal of cyber capabilities.

Vulnerabilities in deployed systems and networks arise from bugs—defects in machine or its operation.[50] These bugs may be usefully exploitable, and the knowledge of an exploitation opportunity where the defender is either unaware of its existence, or has not been able to remediate the underlying vulnerability, is a key feature of offensive cyber exchange. Likewise, implant payloads intended to execute malicious instructions within the target system or network are also more useful when not known to the adversary, reducing probability of detection. However, even known vulnerabilities and previously observed implants may remain effective against certain targets, due to defender inattention, misconfiguration, or other factors. The operational choices about when, and how, to

[49] Wayne P. Hughes Jr. "A salvo model of warships in missile combat used to evaluate their staying power." Vol 42 : Issue 2. Naval Research Logistics. 1995.
[50] Peggy Aldrich Kidwell. "Stalking the Elusive Computer Bug." IEEE Annals of the History of Computing. Vol 20 Issue 4. 1998.

employ these capabilities feature prominently in the management and execution of offensive cyber operations, balancing tradeoffs of detection versus potential range of effects options.[51] These capabilities also carry an economic value, both on open markets and closed private exchanges as a commodity, as well as in the investments into research, development, testing and acquisition.[52] In cases where exploit options may have impact on civilian critical infrastructure and commercial enterprise environments, responsible states have pursued processes to balance the competing equities in the discovery and retention of unknown vulnerabilities, and the disclosure of these bugs as warning to private sector actors that may mitigate their exposure to other adversary action.[53]

The inventory of 0-days (i.e., unknown, undisclosed vulnerabilities), that may be viable exploited at any given moment to achieve access against target systems and networks is not infinite, and may in fact be scarce (although this has proven a difficult question to answer).[54] The population of military useful 0-days (exploitable vulnerabilities in relevant adversary deployed targets), is presumably smaller yet. Likewise, the options for operational effects against these targets are also constrained, and where codified into weaponized implants and tested for validation against threat representative targets, are a valuable capability which may be degraded following use and detection.[55] The manner in which a capability is used, and the character of its effects, and the capacity of the defender target may influence the viable lifespan of an OCO option.[56] Further, independent rediscovery of both vulnerabilities, and similar approaches to weaponizing these vulnerabilities into offensive capabilities portfolios, may result in disclosure by third parties that effectively removes a capability from the inventory of a cyber command.[57]

---

[51] Max Smeets, JD Work. "Operational Decision-Making for Cyber Operations: In Search of a Model." Cyber Defense Review. Spring 2020.

[52] Katie Moussouris and Michael Siegel "The Wolves of Vuln Street: The First Dynamic Systems Model
of the 0day Market." RSA Conference. San Francisco. 2015. ; Jaziar Radianti. "A Preliminary Model Of The Vulnerability Black Market." 25th International System Dynamics Conference. Boston, USA. 29 July-2 August 2007; Charles Miller. "The Legitimate Vulnerability Market: The Secretive World of 0-Day Exploit Sales." Workshop on the Economics of Information Security. June 2007.

[53] Tristan Caulfield, Christos Ioannidis, David Pym. "The U.S. Vulnerabilities Equities Process: An Economic Perspective." International Conference on Decision and Game Theory for Security). 2017. ; Jason Healey. "The U.S. Government and Zero Day Vulnerabilities: From pre-Heartbleed to Shadowbrokers." Columbia Journal of International Affairs. November 2016.

[54] Dan Geer. "For Good Measure: The Undiscovered." USENIX Login. April 2015.

[55] JD Work. "Who Hath Measured the (Proving) Ground: Variation in Offensive Capabilities Test and Evaluation." 15th International Conference on Cyber Warfare and Security. Old Dominion University, Norfolk, VA. March 2020. ; Forrest B. Hare. "Precision cyber weapon systems: An important component of a responsible national security strategy?" Contemporary Security Policy. Vol 40 Issue 2. 2019. ; Gary D. Brown, Andrew O. Metcalf. "Easier Said Than Done: Legal Reviews of Cyber Weapons." Journal of National Security Law & Policy. 2014. ; Dale Peterson. "Offensive Cyber Weapons: Construction, Development, and Employment." Journal of Strategic Studies. Vol 36 Issue 1. Pp 120-124. 2013. ; Thomas Rid, Peter McBurney. "Cyber-Weapons." The RUSI Journal. Vol 157 Issue 1. 2012.

[56] Max Smeets. "A matter of time: On the transitory nature of cyberweapons." Journal of Strategic Studies. Vol 41 Issue 2: pp6-32. 2018.

[57] Lillian Ablon, Andy Bogart. "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits." RAND. 2017.

These factors in combination create challenges for offensive planners and operators, who face uncertainty over the continued viability of a given capability.[58]

These considerations are highly salient to potential littoral fires exchanges where advantage is enabled by OCO capabilities. There is no small peril inherent in operational concepts that may rely upon transient instantiations of vulnerability that may change over anticipated lifespan of an adversary's acquisition, deployment, and spiral development upgrades of specific military equipment. The calculations of arsenal management in cyber operations also differ in short, sharp exchanges vice prolonged conflict within a given theatre. They are changed by joint and allied operations, particularly where coalition actions are conducted between partners with differing levels of established relationships and associated trust involving in liaison interactions around what are often closely held intelligence and cryptologic matters. These calculations may vary where critical target systems are used in multiple contexts at strategic and tactical levels across multiple adversaries, where certain options may be more optimally preserved in case of multiple simultaneous conflicts in different theatres, or against the potential that a conflict may climb further up the rungs of the escalation ladder.

The difficult challenges of arsenal management are compounded by the complexities of access, and of sustaining such access, against relevant target systems and networks. OCO options may require substantial advance lead, especially where they are intended to deliver impact against isolated, closed networks, including vessels underway. This rapidly changes the discussion from a question of cyber fires in fleet problems to the questions of the saboteur's dilemma. While such matters are easily considered in the abstract, the realities of such operations at the coal face are often high risk, against long odds of success, and frequently at great cost to the operators and the supporting elements involved. These matters often move out of the purely military domain, and beyond the discussion here.

These factors in summation suggest offensive cyber operations as a component of littoral and expeditionary advanced base operations in many ways become yet another iteration of the long familiar continual race of armor versus bullet. The Fleet and the Corps must recognize that they now compete in this race by virtue of nested requirements that flow from the new operating concepts. The manner in which this race is run may bring great advantage if successful, or risk terrible costs if not adequately resourced with appropriate talent, investment, and command attention.

About the Author

JD Work [59]
National Defense University & Columbia University

JD Work serves with the National Defense University, College of Information and Cyberspace. He holds additional affiliations with the Saltzman Institute of War and

[58] JD Work. "Calculating the Fast Equations: Arsenal management considerations in sustained offensive cyber operations**."** Harvard University, John F. Kennedy School of Government, Belfer Center for Science and International Affairs, Cyber Security Project. April 2019.
[59] The views and opinions expressed here are those of the author and do not necessarily reflect the official policy or position of any agency of the U.S. government or other organization.

Peace Studies at the School of International and Public Affairs at Columbia University, the Krulak Center for Innovation and Future Warfare at Marine Corps University, and the Cyber Statecraft Initiative at the Atlantic Council. He can be found on Twitter *@HostileSpectrum*.

Appendix: Simulated Engagement Results

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
CSG	NSM	No	Control	-	-
CSG	NSM	Yes	Control	-	-
CSG	Tomahawk	No	Control	-	-
CSG	Tomahawk	Yes	Control	-	-
CSG	GB-ASBM	No	Control	1x Type 052D, 1x Type 054A, 1x Type 901	-
CSG	LRASM	No	Control	-	-
CSG	LRASM	Yes	Control	-	1x Type 001 (light)
CSG	Harpoon	No	Control	-	-
CSG	Harpoon	Yes	Control	-	-
CSG	Exocet	No	Control	-	-
CSG	Hsiung Feng III	No	Control	-	1x Type 001 (light)
CSG	3M54T Kalibr	No	Control	2x Type 052D, 1x Type 054A	1x Type 901 (heavy)
CSG	P-800 Oniks	No	Control	2x Type 052D	1x Type 001 (moderate)
CSG	3M24 (Kh35)	No	Control	-	-
CSG	SSC-8 SACCADE	No	Control	-	-
CSG	DF-26 ASBM	No	Control	1x Type 001	-
CSG	DF-26 ASBM	Yes	Control	1x Type 001, 1x Type 055	-
CSG	Khalij Fars ASBM	No	Control	1x Type 052D	1x Type 054A (moderate), 3x merchant (moderate)
CSG	Tomahawk	No	Degraded datalinks	-	-
CSG	Tomahawk	No	Degraded radar (Type 054A and Type 055 all primary sets)	-	-
CSG	Tomahawk	No	Degraded radar (Type 052D and Type 054A all primary sets)	-	-

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
CSG	Tomahawk	No	Degraded radar (Type 055 all primary sets)	-	-
CSG	Tomahawk	No	Degraded point defense (30mm)	-	-
CSG	Tomahawk	No	Degraded point defense (HQ10 SAM)	-	-
CSG	Tomahawk	No	Degraded VLS (Type 052D)	-	-
CSG	Tomahawk	No	Degraded VLS (Type 054A)	-	-
CSG	Tomahawk	No	Degraded VLS (Type 055)	-	-
CSG	Tomahawk	No	Degraded VLS (Type 052D, Type 054A, Type 055)	-	1x Type 001 (light)
CSG	Tomahawk	No	Degraded radar (set 346)	-	-
CSG	Tomahawk	No	Degraded radar (Type 054A, set MR-710 / TOP PLATE)	-	-
CSG	Tomahawk	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	-	-
CSG	Tomahawk	No	Degraded radar (Type 001, set 381 RICE SCREEN)	-	-
CSG	Tomahawk	No	Degraded radar (Type 052D, set KNIFE REST)	-	-
CSG	NSM	No	Degraded datalinks	-	1x Type 001 (moderate)
CSG	NSM	No	Degraded VLS (Type 052D)	-	1x Type 001 (moderate)
CSG	NSM	No	Degraded VLS (Type 054A)	-	1x Type 001 (moderate)
CSG	NSM	No	Degraded VLS (Type 055)	-	1x Type 001 (moderate)
CSG	NSM	No	Degraded VLS (Type 052D, Type 054A, Type 055)	-	1x Type 001 (heavy); complete loss of air wing
CSG	NSM	No	Degraded radar (Type 052D, set KNIFE REST)	-	-
CSG	NSM	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	-	1x Type 001 (heavy); complete loss of air wing
CSG	NSM	No	Degraded radar (Type 054A, set	-	1x Type 001 (moderate)

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
			MR-710 / TOP PLATE)		
CSG	NSM	No	Degraded radar (Type 054A, set BAND STAND)	-	1x Type 001 (moderate), partial loss of air wing
CSG	NSM	No	Degraded radar (Type 001, set 381 RICE SCREEN)	-	1x Type 001 (light), partial loss of air wing
CSG	NSM	No	Degraded radar (set 346)		1x Type 001 (heavy); complete loss of air wing
CSG	NSM	No	Degraded point defense (30mm)	-	-
CSG	NSM	No	Degraded point defense (HQ10 SAM)	-	1x Type 001 (heavy); complete loss of air wing
CSG	NSM	No	Degraded CIC (Type 054A)	-	1x Type 001 (moderate), partial loss of air wing
CSG	NSM	No	Degraded CIC (Type 055)	-	1x Type 001 (moderate), full loss of air wing
SAG	NSM	No	Control	1x Type 054A	-
SAG	NSM	Yes	Control	2x Type 052D, 1x Type 054A	-
SAG	NSM	No	Control, penetration aid	1x Type 054A	1x Type 054A
SAG	Tomahawk	No	Control	-	-
SAG	Tomahawk	Yes	Control	-	-
SAG	NSM plus HIMARS	No	Control	-	-
SAG	GB-ASBM	No	Control	2x Type 052D, 1x Type 054A, 1x Type 903	
SAG	LRASM	No	Control	-	-
SAG	LRASM	Yes	Control	-	-
SAG	Harpoon	No	Control	-	-
SAG	Harpoon	Yes	Control	-	-
SAG	Exocet	No	Control	-	-
SAG	3M54T Kalibr	No	Control	2x Type 052D, 1x Type 054A	-
SAG	P-800 Oniks	No	Control	-	Type 055 (Heavy)

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
SAG	P-800 Oniks	Yes	Control	1x Type 052D, 2x Type 054A, 1x Type 903	-
SAG	3M24 (Kh35)	No	Control	-	-
SAG	SSC-8 SACCADE	No	Control	-	-
SAG	Hsiung Feng III	No	Control	1x Type 052D, 1x Type 054A	1x Type 055
SAG	DF-21D ASBM	No	Control	2x Type 052D, 2x Type 054A, 1x Type 903	-
SAG	DF-26 ASBM	No	Control	1x Type 054A, 1x Type 055, 1x Type 903	
SAG	NSM	Yes	Control	2x Type 054A	1x Type 055, 1x type 903
SAG	NSM	No	Control	-	1x Type 052 (heavy), 1x type 903 (light)
SAG	NSM	Yes	Degraded datalinks	1x Type 052, 1x Type 054A, 1x Type 055	1x Type 054A (moderate)
SAG	NSM	No	Degraded datalinks	1x Type 052D	None
SAG	NSM	No	Degraded VLS (Type 055, Type 054A)	1x Type 052, 1x Type 055	1x Type 054A (moderate)
SAG	NSM	No	Degraded CIC (Type 055)	-	1x Type 054A (moderate), 1x Type 052 (heavy)
SAG	NSM	No	Degraded radar (Type 055, set 346)	1x Type 055	None
SAG	NSM	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	2x Type 054A	1x Type 055 (light)
SAG	NSM	No	Degraded radar (Type 054A, set MR-710 / TOP PLATE)	2x Type 054A	-
SAG	NSM	No	Degraded radar (Type 055, set KNIFE REST)	-	-
SAG	NSM	No	Degraded radar (Type 055 and Type	2x Type 052D, 1x Type 054A	1x Type 054A (moderate)

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
			052, set KNIFE REST)		
SAG	NSM	No	Degraded radar (Type 054A and Type 055, all primary sets)	1x Type 052D, 1x Type 054A, 1x Type 055	1x Type 903 (light)
SAG	NSM	No	Degraded radar (set BAND STAND)	1x Type 052D, 1x Type 054A, 1x Type 055	1x Type 903 (moderate)
SAG	NSM	No	Degraded point defense (30mm)	1x Type 052D	1x Type 054A (light)
SAG	NSM	No	Decoy	-	1x Type 052D, 1x Type 054A, 1x Type 903 (light)
SAG	NSM plus HIMARS	No	Degraded datalinks	1x Type 052D	-
SAG	Tomahawk	No	Degraded datalinks	-	-
SAG	Tomahawk	No	Degraded radar (Type 054A and Type 055, all primary sets)	2x Type 054A, 1x Type 055	1x Type 903 (moderate)
SAG	Tomahawk	No	Degraded CIC (Type 055)	-	1x Type 052D (heavy)
SAG	Tomahawk	No	Degraded radar (Type 055, set 346)	-	-
SAG	Tomahawk	No	Degraded VLS (Type 055, Type 054A)	1x Type 054A	1x Type 054A (heavy)
SAG	Tomahawk	No	Degraded radar (Type 054A, set BAND STAND)	-	-
SAG	Tomahawk	No	Degraded radar (Type 055 and Type 052, set KNIFE REST)	-	1x Type 052D (heavy)
SAG	Tomahawk	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	-	-
SAG	Tomahawk	No	Degraded radar (Type 054A, set MR-710 / TOP PLATE)	-	-
SAG	Tomahawk	No	Degraded point defense (30mm)	-	1x Type 052D (heavy)
ESG	NSM	No	Control	1x Type 022	1x Type 052D (heavy), 1x Type 054A (moderate),

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
					1x Type 071 (moderate), 1x Type 903 (light)
ESG	NSM	Yes	Control	1x Type 052D, 1x Type 054A, 1x Type 071	Type 903 (heavy)
ESG	NSM plus HIMARS	No	Control	-	-
ESG	Tomahawk	No	Control	-	-
ESG	Tomahawk	Yes	Control	-	1x Type 071 (moderate)
ESG	LRASM	No	Control	-	-
ESG	Harpoon	No	Control	-	-
ESG	Exocet	No	Control	-	-
ESG	Hsiung Feng III	No	Control	-	-
ESG	3M24 (Kh35)	No	Control	-	-
ESG	SSC-8 SACCADE	No	Control	-	-
ESG	DF-26 ASBM	No	Control	1x Type 071, 1x Type 903	-
ESG	DF-26 ASBM	Yes	Control	1x Type 052D, 1x Type 071, 1x Type 903	-
ESG	Tomahawk	No	Degraded datalinks	-	1x Type 071 (heavy)
ESG	Tomahawk	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	1x Type 054A, 1x Type 071	1x Type 052 (heavy), 1x Type 903 (moderate)
ESG	Tomahawk	No	Degraded radar (Type 054A, set BAND STAND)	1x Type 054A, 1x Type 071	1x Type 903 (moderate)
ESG	Tomahawk	No	Degraded VLS (Type 054A)	1x Type 071	1x Type 903 (moderate)
ESG	Tomahawk	No	Degraded radar (Type 054A, all primary sets)	2x Type 022, 1x Type 054A, 1x Type 071	-
ESG	Tomahawk	No	Degraded radar (Type 052D, set KNIFE REST)	-	1x Type 054A (heavy)
ESG	DF-26 ASBM	No	Degraded radar (Type 054A, all primary sets)	1x Type 052D, 1x Type 071, 1x Type 903	-
ESG	DF-26 ASBM	No	Degraded radar (Type 071, set JUG PAIR)	1x Type 052D, 1x Type 071, 1x Type 903	-

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
ESG	NSM	No	Degraded datalinks	1x Type 022, 1x Type 071	1x Type 052D (heavy), 1x Type 054A (moderate), 1x Type 903 (moderate)
ESG	NSM	No	Degraded radar (Type 054, all primary sets)	1x Type 022, 1x Type 052D, 1x Type 071, 1x Type 903	-
ESG	NSM	No	Degraded radar (Type 054A, set MR-710 / TOP PLATE)	1x Type 022, 1x Type 054A, 1x Type 071	1x Type 052D (heavy), 1x Type 903 (moderate)
ESG	NSM	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	2x Type 022, 1x Type 054A	1x Type 052D (moderate), 1x Type 071 (heavy), 1x Type 903 (moderate)
ESG	NSM	No	Degraded radar (Type 054A, set BAND STAND)	1x Type 022, 1x Type 052D	1x Type 054A (moderate), 1x Type 071 (heavy)
ESG	NSM	No	Degraded radar (Type 052D, set KNIFE REST)	1x Type 022, 1x Type 052D, 1x Type 054A, 1x Type 071	1x Type 903 (light)
ESG	NSM	No	Degraded VLS (Type 054A)	2x Type 022, 1x Type 071	1x Type 052D (heavy), 1x Type 054A (moderate), 1x Type 903 (moderate)
ESG	NSM	No	Degraded point defense (30mm)	1x Type 022, 1x Type 071	1x Type 052D (heavy), 1x Type 903 (moderate)
Convoy	NSM	No	Control	-	1x Type 052D (heavy), 1x Type 054A (moderate),

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
					2x merchant (heavy), 1x merchant (light)
Convoy	NSM	Yes	Control	1x Type 052D, 1x Type 054A	3x merchant (light), 1x merchant (heavy)
Convoy	LRASM	No	Control	1x Type 052D, 1x Type 054A	2x merchant (light), 2x merchant (heavy)
Convoy	LRASM	Yes	Control	1x Type 052D, 1x Type 054A, 1x merchant	2x merchant (moderate), 1x merchant (heavy)
Convoy	3M54T Kalibr	No	Control	1x Type 052D, 1x Type 054A, 1x merchant	1x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	Hsiung Feng III	No	Control	1x Type 052D, 1x merchant	2x merchant (light), 1x merchant (heavy)
Convoy	3M24 (Kh35)	No	Control	-	1x Type 052D, 2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	P-800 Oniks	No	Control	1x Type 054A, 2x merchant	2x merchant (light)
Convoy	SSC-8 SACCADE	No	Control	-	2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	Khalij Fars ASBM	No	Control	1x Type 052D	1x Type 054A (moderate), 3x merchant (moderate)
Convoy	NSM	No	Degraded datalinks	1x Type 052D, 1x Type 054A	2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
Convoy	NSM	No	Degraded merchant propulsion, separating 2 vessels from escorts	1x Type 052D, 1x merchant	3x merchant (light), 1x merchant (moderate)
Convoy	NSM	No	Degraded VLS (Type 054A)	1x Type 052D, 1x Type 054A	2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	NSM	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	1x Type 054A	1x Type 052D (heavy), 2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	NSM	No	Degraded radar (Type 054A, set MR-710 / TOP PLATE)	1x Type 052D	1x Type 054A (moderate), 1x merchant (light), 2x merchant (moderate), 1x merchant (heavy)
Convoy	NSM	No	Degraded radar (Type 054A, set BAND STAND)	-	1x Type 052D (heavy), 1x Type 054A (moderate), 2x merchant (light), 1x merchant (moderate)
Convoy	NSM	No	Degraded radar (Type 054A, all primary sets)	1x Type 052D, 1x Type 054A	2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	NSM	No	Degraded radar (Type 052D, set KNIFE REST)	1x Type 052D, 1x Type 054A	2x merchant (light), 1x merchant (moderate), 1x merchant (heavy)
Convoy	Tomahawk	No	Control	-	2x merchant (light), 1x merchant (moderate),

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
					1x merchant (heavy)
Convoy	Tomahawk	Yes	Control	-	2x merchant (light), 2x merchant (moderate)
Convoy	Tomahawk	No	Degraded datalinks	1x Type 052D, 2x merchant	2x merchant (light), 1x merchant (moderate)
Convoy	Tomahawk	No	Degraded VLS (Type 054A)		3x merchant (light), 1x merchant (heavy)
Convoy	Tomahawk	No	Degraded radar (Type 054A, set MR-90 Orekh / FRONT DOME)	1x Type 054A, 2x merchant	2x merchant (light)
Convoy	Tomahawk	No	Degraded radar (Type 054A, set MR-710 / TOP PLATE)	1x merchant	2x merchant (light), 1x merchant (moderate)
Convoy	Tomahawk	No	Degraded radar (Type 054A, set BAND STAND)	1x merchant	2x merchant (light), 1x merchant (moderate)
Convoy	Tomahawk	No	Degraded radar (Type 054A, all primary sets)	1x Type 052D, 1x Type 054A, 1x merchant	1x merchant (light), 2x merchant (moderate)
Raiders	NSM	No	Control	4x Type 022, 1x Type 056	-
Raiders	NSM	Yes	Control	4x Type 022, 1x Type 056	-
Raiders	Harpoon	No	Control	4x Type 022, 1x Type 056	-
Raiders	Exocet	No	Control	4x Type 022, 1x Type 056	-
Raiders	NSM	No	Degraded datalinks	4x Type 022, 1x Type 056	-
Raiders	NSM	No	Degraded radar (Type 056, set 363)	4x Type 022, 1x Type 056	-
Raiders	NSM	No	Degraded point defense (HQ10 SAM)	4x Type 022, 1x Type 056	-
Raiders	Tomahawk	No	Control	4x Type 022, 1x Type 056	-
Raiders	Tomahawk	Yes	Control	4x Type 022, 1x Type 056	-
Raiders	Tomahawk	No	Degraded datalinks	4x Type 022, 1x Type 056	-
Raiders	Tomahawk	No	Degraded radar (Type 056, set 363)	4x Type 022, 1x Type 056	-

Adversary	Weapon	EMCON	OCO Effects	Sunk	Damaged
Raiders	Tomahawk	No	Degraded point defense (HQ10 SAM)	4x Type 022, 1x Type 056	-