Spring 2016 Vol. 7 No. 1

MCU Journal

Published by Marine Corps University Press

Call for Submissions

MCU Journal

Marine Corps University Press (MCUP) publishes full-length monographs and a scholarly journal focusing on contemporary issues. MCUP is looking for articles to publish in the *MCU Journal* on topics related to international relations, national security, policy issues, and geopolitical concerns. For the 2017 publishing year, we are especially interested in acquiring papers on Russian topics and manuscripts that address nuclear policies or concerns (e.g., energy or weapons).

MCU Journal is a peer-reviewed journal, and submissions should be 4,000–10,000 words, footnoted, and formatted according to *Chicago Manual of Style* (16th edition). Junior faculty and advanced graduate students are encouraged to submit. MCUP is also looking for book reviewers from international studies, political science, and contemporary history fields.

To receive a copy of the journal or to discuss an article idea or book review, please contact acquisitions editor Alexandra Kindell at alexkindell@gmail.com.

Cover: On the heels of Russian activity along the Ukrainian border in 2014, violence broke out in Kiev as anti-Russian protestors took to the streets.
Photo by Sasha Maksymenko.

MCU Journal

MCUP

Published by Marine Corps University Press
3078 Upshur Drive | Quantico, VA 22134

MARINE CORPS UNIVERSITY
BGen Helen G. Pratt, USMCR
President

Col Scott E. Erdelatz, USMC
Chief of Staff

Dr. James H. Anderson
Vice President, Academic Affairs

LtCol Owen Nucci, USMC
Acting Vice President, Student Affairs
and Business Operations

Dr. Charles P. Neimeyer
Director, Marine Corps History Division
and Gray Research Center

Mr. Paul J. Weber
Deputy Director, Marine Corps History
Division and Gray Research Center

EDITORIAL STAFF
Ms. Angela J. Anderson
Senior Editor

Mr. Shawn H. Vreeland
Managing Editor

Ms. Nora Ellis
Manuscript Editor

Dr. Alexandra Kindell
Acquisitions Editor

EDITORIAL BOARD
Col Gary D. Brown, USAF (Ret)
Professor of Cybersecurity, MCU

Dr. Rebecca Johnson
Dean, Marine Corps War College, MCU

Dr. James H. Joyner Jr.
Associate Professor of Strategic Studies
Command and Staff College, MCU

Dr. Benjamin P. Nickels
Academic Chair for Transnational Threats
and Counterterrorism
Africa Center for Strategic Studies, NDU

Dr. Paolo G. Tripodi
Ethics Branch Head
Lejeune Leadership Institute, MCU

Dr. Christopher D. Yung
Donald Bren Chair of Non-Western
Strategic Thought, MCU

Established in 2008, Marine Corps University Press (MCUP) recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Marine Corps University Journal* (*MCU Journal*) in 2010 to provide a forum for interdisciplinary discussion of national security and international relations issues and how they impact the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. The *MCU Journal* is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS

The editors of *MCU Journal* are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, cybersecurity, and natural resources and the environment. To submit an article or to learn more about our submission guidelines, please visit www.mcu.usmc.mil/mcu_press/Pages/journalsub.aspx.

BOOK REVIEWS

MCUP is also looking for reviewers from the international studies, political science, and contemporary history fields. Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS

Subscriptions to *MCU Journal* are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

INDEXING

The journal is indexed by EBSCO, OCLC ArticleFirst, JournalSeek, IBZ Online, British Library System, Lancaster Index to Defense and National Security Literature, and AU Library Index to Military Periodicals.

DISCLAIMER

The views expressed in the articles and reviews in this journal are solely those of the authors. They do not necessarily reflect the opinions of the organizations for which they work, Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government.

MCU Journal
(Print) ISSN 2164-4209
(Online) ISSN 2164-4217

Contents

Vol. 7, No. 1

From the Editors 5

FEATURES

Identity, Attribution, and the Challenge of Targeting in the Cyberdomain 9
Col Glenn Voelz, USA, and Sarah Soliman

Russia's Ambiguous Warfare and Implications for the U.S. Marine Corps 30
Mary Ellen Connell and Ryan Evans

The Dragon's Pearls: China's Road to Hegemony in the Indian Ocean 46
Capt David L. O. Hayward, Australian AR (Ret)

Can Refugees Be National Security Assets? Afghan American Contributions to U.S. National Defense since 1978 83
John Baden

REVIEW ESSAY

The Intelligence Dilemma in History, Fact, and Fiction 99
Robert J. Kodosky

BOOK REVIEWS

The Terrorist's Dilemma: Managing Violent Covert Organizations by Jacob N. Shapiro 105
Reviewed by LtCol Gregory Reck, USA

First, Fast, Fearless: How to Lead Like a Navy SEAL by Brian "Iron Ed" Hiner 107
Reviewed by Evan Haglund

Momentum and the East Timor Independence Movement: The Origins of America's Debate on East Timor 109
by Shane Gunderson
Reviewed by James DeShaw Rae

The Tail Wags the Dog: International Politics and the Middle East by Efraim Karsh 112
Reviewed by LtCol R. Nicholas Palarino, USA (Ret)

A War It Was Always Going to Lose: Why Japan Attacked America in 1941 by Jeffrey Record 113
Reviewed by Robert D. Eldridge

The Art of the Possible: Diplomatic Alternatives in the Middle East by M. Reisman 115
Reviewed by 1stSgt Timothy Schorn, ARNG

Ballots, Bullets, and Bargains: American Foreign Policy and Presidential Elections by Michael H. Armacost 118
Reviewed by Shoon Murray

Cyber Blockades by Alison Lawlor Russell 120
Reviewed by Austen D. Givens

Understanding Contemporary Africa 122
Edited by April A. Gordon and Donald L. Gordon
Reviewed by Col Henri Boré, French Marines (Ret)

From the Editors

After five years of publishing the *Marine Corps University Journal*, MCU Press looks forward to an exciting future by redesigning and reformatting the journal to emphasize its role in supporting the national conversation. The new *MCU Journal* will focus on publishing established authors along with young, emerging scholars, combining the strengths of both on themes of international relations, national security, political science, and other disciplines. By engaging authors in a variety of fields, we can cross disciplines to bring new knowledge, constructs, and solutions to our readers. Moreover, by bridging the civilian and military divide, our audience can read about different perspectives on policy and contemporary issues. For the spring 2016 issue, we have done just that with articles on domestic and international topics as well as book reviews, all of which represent the ideas being broached by academic scholars, think tank analysts, and military leaders.

Headlines so far for 2016 have highlighted the fact that the United States seems to be lagging on the cyberfront. Journalists, in such stories as "Federal Government Confirms That It Still Sucks at Cyber Security" and "New Military Outfit to Enhance China's Cyber Security, Espionage Prowess," point to a higher level of advances being made overseas as our own government struggles to safeguard what should be secure networks and the identities of millions. These recent issues might make the casual reader wonder how our military intends to counter cyberattacks from foreign soils when the government cannot seem to manage at home.

In the lead article, "Identity, Attrition, and the Challenge of Targeting in the Cyberdomain," Colonel Glenn Voelz and coauthor Sarah Soliman explore this new terrain for irregular warfare whereby the nation's adversaries manipulate the newest technology to gather intelligence, spread propaganda, and recruit and train combatants via an intricate web of cybertools, particularly in such austere environments as Iraq and Afghanistan where positive identification of fighters to support high-value targeting and to eliminate insurgent networks was virtually impossible. The boots on the ground must now work within the context of innovative doctrinal concepts and analytical methods. This new reality creates a

growing risk for conventional military forces without the necessary capabilities to adapt and react. The authors also focus on key aspects of developing the necessary methods to link the "abstract cyberpersonae" of the insurgents to real physical identities among the noise of urban battlespaces. To make the first step toward achieving national goals within the cyberdomain, the U.S. government must better educate midlevel leaders about the technical aspects of cyberoperations to support the slim margin of advantage our military currently enjoys.

Our second article illustrates how the Russian Federation continues to make its own strides on the world stage by way of ambiguous warfare strategies that allowed it to annex Crimea in 2014 but also encouraged additional instability in the Ukraine. Authors Mary Ellen Connell and Ryan Evans provide a summary of a CNA-sponsored discussion among military officers, regional specialists, and security experts in "Russia's Ambiguous Warfare and Implications for the U.S. Marine Corps." While a confrontation between the Marine Corps and Russian forces seems unlikely in the near future, the data collected by CNA indicates how critical it will be for U.S. forces to modify current strategies to adapt to the success wrought by Russia's tactics. Their doctrine of denial and deception kept NATO and the rest of the world wondering at Russia's involvement in what appeared a regional dispute. General Valery Gerasimov, chief of staff of the Russian Federation's military, developed doctrine that blurs the lines between war and peace. Using this concept as the basis of their discussion, CNA's assembled experts evaluated Russia's ability to successfully integrate military and nonmilitary forces. Russia seems to gain the most leverage by not employing their military in terms of "Services" but rather in terms of "fighting power" and "political impact." Please read the article to see what the authors have to say about what Russia may or may not be able to do considering the events of 2014 and their consequences.

Russia is not alone in its attempts to put up a smokescreen regarding its actions in areas that represent economic, logistical, geopolitical, and strategic importance. In our third article, Future Direction International's analyst Captain David L. O. Hayward presents a picture of China's roadmap for domination in the Indian Ocean Region (IOR) in his article "The Dragon's Pearls: China's Road to Hegemony in the Indian Ocean." China's seaborne pursuits in the IOR represent approximately 60 percent of the volume of all its global imports, particularly for gas and oil transportation. In the past, Chinese officials have been quiet about their activities there, denying the U.S. State Department's depiction of Chinese activity as building a "String of Pearls" in the IOR. The State Department witnessed the building of ports (or pearls) that could create a network of posts (the string) connecting China to the source of its oil and gas imports. In the last 12 to 18 months, however, China's President Xi Jinping has embraced his own version of events, referring to Chinese investments in the region as part of building a Maritime Silk Road. While not new, China's Maritime Silk Road activ-

ities now seem to point to attempts to expand its naval presence by means of a civilian maritime infrastructure bordering the IOR whereby each pearl created extends through a connected set of strings. Thus, Hayward examines China's past, current, and potential projects in the area that its leaders call commercial but have definite military import. While Western nations watch suspiciously from the sidelines, other nations in the IOR—India, Taiwan, South Korea, New Zealand, and Australia—use all the geopolitical resistance available to smaller nations to counter what appears to many as military expansion and maritime control and to evoke a vision of Chinese hegemony in the IOR.

In the final article, John Baden, a history doctoral candidate at Case Western Reserve University, addresses the collective American conscience regarding Middle Eastern refugees and the effects of anti-Muslim prejudice. Opponents of Afghan immigrants argue that they represent a serious national security risk, while advocates question how America can turn its back so easily on the promise of "Give me your tired, your poor, your huddled masses yearning to breathe free." Baden's article, "Can Refugees Be National Security Assets?," offers a brief account of the role that Afghan immigrants have had in shaping U.S. defense and foreign policy during the past three-and-a-half decades. From the Cold War era to the Global War on Terrorism, Baden proposes a more logical, quantifiable perspective on Afghan contributions to the United States to balance the fear and widespread mistrust of immigrants from the Middle East as international attacks plague the popular media.

In our penultimate section, the review essay titled "The Intelligence Dilemma" introduces the spring issue's book reviews. In it, reviewer Robert J. Kodosky discusses the nature of intelligence operations and the American government's approach to secrecy by comparing three recent monographs on the topic: *The Billion Dollar Spy, The Hidden Hand,* and *The Rise and Fall of Intelligence*. Terrorism, and the technology combatants use to wage war, has become the singular topic of national consideration. Kodosky ponders whether the United States can balance the safety of the nation against decades of government secrecy intended, at times, to protect us from ourselves.

Overall, our authors have broached a wide range of issues, but the themes of national security, U.S. policy, and the implications of past and present actions resonate throughout the articles and the reviews. In this next year, we look forward to another stimulating regular issue to be released in fall, as well as our first special issue, "Climate Change and Policy." Look for both of these issues, and feel free to give us your feedback via email or on social media. MCU Press can be reached on both Twitter and Facebook.

Identity, Attribution, and the Challenge of Targeting in the Cyberdomain

Colonel Glenn Voelz, USA, and Sarah Soliman

Abstract. The cyberdomain has become "key terrain" of irregular warfare with state and nonstate actors leveraging social media and other digital tools for command and control, intelligence gathering, training, recruiting, and propaganda. Department of Defense cyberstrategy highlights the urgent need for improved cyber situational awareness to reduce anonymity in cyberspace. This requires new technologies, doctrine, and analytical approaches for identifying and targeting adversaries operating in a digital landscape. This article examines identity-based targeting approaches developed during recent conflicts as a possible starting point for this effort.

Keywords: Cyberdomain, social media, targeting, identity intelligence, attribution, gray zone conflicts, hybrid warfare, Islamic State, terrorism, biometrics, network analysis, big data, activity-based intelligence, high-value individuals

One of the early lessons learned during the conflicts in Iraq and Afghanistan was how legacy intelligence systems and methods designed for waging conventional warfare against state-based adversaries could not provide the kind of information needed to effectively target irregular combat-

Col Glenn Voelz, USA, is the senior intelligence analyst on the International Military Staff at NATO Headquarters. He was previously the U.S. Army War College fellow in the Massachusetts Institute of Technology's Security Studies Program and at MIT's Lincoln Laboratory. He is a graduate of West Point and holds advanced degrees from the University of Virginia and the National Intelligence University.

Sarah Soliman spent two years in Iraq and Afghanistan as a technician supporting Department of Defense biometrics, forensics, and sensitive site exploitation, including time with U.S. Special Operations Command. She now studies emerging technology trends as a project associate at Rand in Washington, DC, and is pursuing a PhD through King's College London Department of War Studies.

MCU Journal vol. 7, no. 1
Spring 2016
www.mcu.usmc.mil/mcu_press
DOI:10.21140/mcuj.2016070101

ants.[1] These new adversaries were organized as distributed networks comprised of individuals often indistinguishable from surrounding populations. This operational challenge demanded new technologies and methods for identifying individual combatants, characterizing and geo-locating their activities, and analyzing the structure of their networks. Within this operational environment, combatant identity and pattern of life information became crucial elements of high-value targeting and the process of removing insurgents and terrorist networks from the battlefield.[2]

In many respects, this mode of warfare marked a major paradigm shift for the U.S. military. It demanded intelligence collection technologies and analytical methods very different from those designed for detecting motorized rifle battalions and targeting conventional weapons platforms. These adaptations evolved over a decade of intense counterinsurgency and counterterrorism campaigns against irregular adversaries that transformed methods of operational targeting and made combatant identity into a highly salient feature of modern combat. The evolution of identity-based targeting involved a process of doctrinal and technical innovation that brought new tools to the battlefield, such as biometrics, forensics, and DNA analysis.[3] These capabilities helped U.S. forces navigate the complex human terrain of the irregular battlefield and "put a uniform on the enemy" by reducing their ability to use anonymity for military advantage.

These technologies were applied within the context of new doctrinal concepts, such as Identity Intelligence (I2) and Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD). In I2, various identity attributes (biologic, biographic, behavioral, and reputational information) were fused with other tactical information to connect individual combatants to other persons, places, events, and materials on the battlefield. The F3EAD cycle was enabled by data-intensive analytical methods deeply influenced by social network theory and targeting processes specifically designed for engaging high-value individuals and dismantling their networks.

The next evolution in warfare is likely to reflect elements of continuity with these recent experiences even as specific tools and methods evolve. Future adversaries will continue to seek out asymmetric means to circumvent U.S. conventional force advantages. To do this, they will most certainly exploit cutting-edge commercial technologies and communications to generate tactical leverage against well-equipped militaries. As in recent conflicts, these adversaries are likely to avoid direct engagement by using anonymity to conceal operations, protect networks, and complicate targeting for U.S forces. Some of these methods resemble what commentators have dubbed "gray zone" conflicts, or wars characterized by " 'hybrid' threats that may combine subversion, destabilizing social media influence, disruptive cyber attacks, and anonymous 'little green men' instead of recognizable armed forces making overt violations of international borders."[4]

Moreover, these methods are likely to be adopted by state as well as nonstate actors. As General Joseph L. "Joe" Votel, commander of U.S. Special Operations Command, recently noted, such conflicts are likely to be defined by ambiguity and even uncertainty regarding the parties involved.[5]

Within this operational paradigm, the cyberdomain is likely to emerge as "key terrain" of these future battlefields.[6] Over the last few years, a range of nation-state and nonstate actors from Russia to the Islamic State have aggressively leveraged cybertools as part of their intelligence gathering, operational planning, internal communications, recruiting, and strategic messaging—all directed toward creating tangible effects in the physical battlespace. As such methods expand, they are likely to present conventional military forces with targeting challenges similar to those experienced during the last decade in Iraq and Afghanistan. Specifically, modern irregular adversaries have been empowered by their ability to hide among the populace, avoid attribution, and complicate the targeting process for conventional military forces.[7] These methods apply to the cyberdomain as well as the physical battlespace. Adversaries are already leveraging cybertools to create demonstrable effects in the physical landscape while manipulating their digital identities to hide, deceive, and confuse observers as to the nature of their activities. Furthermore, the technical tools and methods for masking identity and obscuring attribution are increasingly available even to those with limited technical expertise.

One U.S. Department of Defense (DOD) cyberspace policy report observed how the technical protocols of the Internet provide the means of protecting anonymity and veiling attribution in a manner that "both nations and non-state actors clearly understand."[8] Such methods are likely to be used in the future as a means for generating strategic advantage. Yet even as U.S. forces increasingly maneuver within this digital landscape, they lack sufficient situational awareness concerning the other actors seeking to influence the operational environment. This situation presents a growing risk for conventional military forces, particularly at the operational level where units lack the robust capabilities to identify, monitor, and target key actors in the cyberpersona layer.[9] Problems include a lack of technical tools and expertise enabling commanders to visualize the cyberpersona layer (see figure 1) as well as a doctrinal framework for assessing risks and making effective targeting determinations within this environment.

Adapting to these new challenges will likely require a paradigm shift equal in scope and complexity to the recent evolution of identity-based targeting. In fact, this example may offer several useful parallels in this process, including a template for the process of military innovation and the development of technical tools and supporting doctrine to enable military forces to operate against these new threats. Similar to the complex human terrain of Iraq and Afghanistan, the cyberdomain represents an ill-defined and unbounded battlespace. It contains

adversaries who may not wear uniforms or even occupy a discrete physical area on the battlefield. These virtual combatants are likely to have the technical means to conceal identities, veil attribution, and mask movements across the digital landscape. Within this environment, the issue of combatant identity is likely to persist as one of the most challenging aspects of effective targeting.

Given these concerns, it may be shortsighted to simply view cyberthreats in a narrow technical sense by limiting them to data packets and malware. As this article suggests, there are several important parallels between the identity-based targeting methods applied in the physical domain and what will be needed for military forces to effectively target future adversaries in the cyberdomain. A key aspect for consideration involves developing new methods that link abstract cyberpersonae to actual physical identities, which reveal the nature of individuals' networks, methods, objectives, and functions. As one group of experts recently observed, even in the highly technical and abstract domain of cyberspace, "all operations still begin with a human being."[10]

Anonymity and Power in the Cyberdomain

The dramatic rise of the Islamic State in Iraq and the Levant (ISIL) perhaps offers the most vivid example of how the cyberdomain has become a highly relevant aspect of the contemporary operational environment. Over a relatively short period, ISIL has demonstrated how a combination of digital technologies, global communications networks, and social media platforms can be combined to generate powerful effects in the physical battlespace. The group has made extremely effective use of these tools for operational planning, disseminating training materials and technical information, and coordinating among widely dispersed affiliates and supporters. ISIL famously proliferates high-quality media content across multiple platforms as part of its strategic messaging and recruiting campaigns.[11] Its social media presence and distribution of digital magazines, such as *Dabiq* and *Konstantiniyye*, provide dramatic examples of how terrorist organizations are now using cyberspace to amplify the power of propaganda and extend their influence. ISIL has even developed original web applications providing its supporters with direct access to video and text updates about life under the Islamic State and announcements of battlefield victories.[12]

Social media in particular has become a key enabler for insurgent groups and terrorist organizations in recent years. Popular applications like Twitter, YouTube, Facebook, Tumblr, and Instagram have created a digital ecosystem providing such nonstate actors with unprecedented global reach. Militant groups in Gaza, terrorist cells in Mali, oil traffickers in Nigeria, and pirates off the Somali coast have all used social media as ad hoc communication networks and as platforms for conducting information operations. In many respects, social media provides the ideal medium for adversaries who operate as highly distributed entities but

lack the technical capabilities and financial resources to build and manage formal command and control networks. The recent National Intelligence Council report, *Global Trends 2030*, noted how these social media architectures have become "inherently resistant to centralized oversight and control," enabling individuals, small groups, and ad hoc coalitions of nonstate actors to shift traditional power sources and authorities.[13]

The Syrian conflict provides perhaps the most powerful example of how the cyberdomain has become fully interwoven into the fabric of modern conflict. This war has been called "the most socially mediated civil conflict in history," with fighters routinely using Facebook, YouTube, Twitter, Diaspora, and Snapchat for a variety of operational, communication, and propaganda functions.[14] Analysis from late 2014 identified at least 46,000 Twitter accounts used by members and supporters of the Islamic State while the Federal Bureau of Investigation (FBI) estimated that some 200,000 people each day access the group's messaging via social media to include "videos, instruction manuals, and other material posted on militant Islamist social media sites."[15] While ISIL has perhaps become the most adept user of such tools, the phenomenon is by no means limited to the Islamic State. In Syria, the al-Qaeda linked al-Nusra Front has also used social media for posting press releases and issuing informal communiqués including text, photographs, and videos detailing recent fighting, even posting personalized eulogies for its members killed in combat.[16] Al-Qaeda is often credited with establishing the early model for Internet-based jihadist propaganda with the publication of its online magazine *Inspire*, designed for outreach to English-speaking Muslims. More recently the group has launched a new branch focused on cyberoffensive operations, allegedly executing a campaign of digital defacements, data exfiltrations, and denial of service attacks against Western interests.[17]

Cyberplatforms have also been used extensively for dissemination of operational information, recruiting, and training purposes.[18] For example, hundreds of websites and online forums host information on the use of explosives, fighting techniques, and links to encryption programs designed to help followers protect their sensitive communications. The director of Great Britain's National Security Agency counterpart, Government Communications Headquarters, recently described Twitter, Facebook, and WhatsApp as the "command-and-control networks of choice for terrorist and criminals."[19]

One important characteristic distinguishing the cyberdomain from a conventional physical battlespace is the variety of means for adversaries to anonymize their activities. This issue represents a significant dilemma for military commanders who increasingly are unable to identify actors seeking to exert influence within a given area of operations, whether they are nation-states, foreign intelligence services, hackers, criminals, or terrorists. From a targeting perspective, the primary challenge is linking the cyberpersona to an actual identity behind the digital repre-

sentation. As one cryptographer and security expert recently noted, "We're living in a world where we can't easily tell the difference between a couple of guys in a basement apartment and the North Korean government."[20] This phenomenon has led to a virtual "arms race between attackers and those that want to identify them."[21] One recent report has suggested that approximately 90 percent of terrorist activities taking place online now use social media as a networking tool for their operations, a situation that has created "a virtual firewall to help safeguard the identities of those who participate."[22]

These adversaries are actively exploiting technologies designed to conceal identity and veil attribution for operations conducted in the cyberdomain. Online jihadist forums routinely advise participants on how to avoid detection when web browsing, including steps for removing geo-location and metadata from cell phone images and social media content.[23] ISIL in particular has been adept at modifying its cyberbehavioral profiles by changing computers, cell phones, and messaging apps after one becomes compromised.[24] Some ISIL members are reportedly moving to more secure private messaging apps, such as Telegram, Kik, and WhatsApp, as a means of protecting internal communications.[25] These methods include the use of encryption and data-destroying software designed to frustrate surveillance methods.[26] FBI Director James B. Comey has been outspoken over his concerns that adversaries are increasingly "going dark" by employing tools that make it difficult for legitimate authorities to identify and track emerging threats. This issue, however, has been controversial and opened a vigorous debate among security experts and privacy advocates on the emerging challenges of encryption.

Shortly after ISIL's November 2015 attacks in Paris, the group announced that it would move some of its propaganda materials to the so-called Dark Web as a means of thwarting efforts by social media firms to identify and remove extremist content from their sites.[27] ISIL and other groups have already made use of such tools as the Onion Router (Tor) that enable users to communicate, post, and view online content anonymously.[28] While not offering perfect protection, Tor and similar technologies help mask IP addresses and server locations while encrypting data packets and routing messages through multiple nodes, which make it difficult for authorities to track and identify users. These anonymity-granting systems form the architecture for a sizable portion of Internet traffic that is virtually inaccessible by means of standard web browsers. Tor and other anonymizing software evolved as classic dual-use technologies with many legitimate uses; however, they have also created a virtual safe haven for illicit activities.[29] More recently there has been suggestion that these tools have become shadow command and control networks for terrorist recruitment, financing, and planning.

In addition to the Dark Web, the evolution of digital cryptocurrencies, such as Bitcoin, provide another means for conducting pseudonymous transactions that

are difficult for authorities to monitor and trace.[30] For example, Bitcoin is considered pseudonymous because an individual user is represented by a random, cryptographically generated string of digits that do not directly reveal a participant's identity. These architectures generally enable users to transfer funds with lower risk of detection and greater ability to conceal their physical location.[31] There is also evidence that some terrorist groups are using digital currencies to finance activities, a trend that is likely to be a growing concern as Western governments close off terrorist access to the legitimate international financial system.[32] The head of the U.S. Treasury Department's Financial Crimes Enforcement Network recently cited the growing risk from global point-to-point transactions and digital pseudonymity that enables these groups to move funds instantly across borders, often without detection.[33] Highlighting these concerns, National Security Agency Director Admiral Michael S. Rogers recently revealed the increasing amount of time his agency spends monitoring threats on the Dark Web and tracking people who cannot easily be found through conventional digital surveillance methods.[34]

Protected identities and complicated attribution have also made the cyberdomain an ideal space for conducting digital "denial and deception" operations. Denial and deception describes actions taken by an adversary to degrade or neutralize an opponent's intelligence collection or efforts that deliberately mislead observers as to the true nature of an activity. Cyberspace offers many tools and methods for crafting such misperception. The Internet is rife with fake Twitter accounts, digital avatars, and anonymizing software that can be used toward such ends. One such example was observed in early 2015 when a group known as the Cyber Caliphate, originally believed to be affiliated with ISIL, gained notoriety by briefly taking control of U.S. Central Command's Twitter account and exposing the personal information of some senior U.S. military members. Several months later, however, a private cyberintelligence firm called into question the group's ISIL affiliation and revealed possible links to a Russian-backed cyberespionage group that had been associated with previous attacks against "NATO, the Ukrainian government, and European Union networks."[35] These connections became evident only after a thorough forensic analysis revealed technical indications of a digital false flag operation used as a deliberate attempt to conceal the source of the attacks.[36]

Another example of spoofed digital identities used for military purposes was seen recently when a pro-Syrian regime group known as the Syrian Electronic Army (SEA) created fake online avatars to identify and target opposition members.[37] In this example, fictitious personae were used as part of a phishing campaign to gather detailed personal information including names, locations, and IP addresses of opposition members, media activists, humanitarian aid workers, and other individuals deemed dangerous to the regime.[38] From this information, SEA was able to access users' Skype accounts, mobile apps, and social media sites to

exploit address books, SMS messages, and email contacts from their targets. This kind of aggressive social media exploitation produced what was described as "actionable military intelligence for an immediate battlefield advantage" that enabled pro-Assad forces to identify, track, and target key opposition members.[39] SEA in effect operated as a de facto national cyberforce conducting cyberoperations on behalf of the regime; however, the identities of the individuals behind these operations and the nature of their relationship to the government remain ambiguous.[40] According to experts in the field, such methods are predicted to become "a routine part of even the most low-tech, if brutal, civil wars and available to those operating on a shoestring budget."[41]

All of these examples demonstrate the degree to which use of the cyberdomain by irregular adversaries has altered the relative balance of power vis-à-vis conventional military forces. The first digital revolution—based on advances in data processing, remote sensing, and satellite communications—was instrumental for enabling well-resourced state militaries to operate on a global scale, share real-time information, and concentrate combat power across time and space. Due to the complexity and expense of these systems, the operational benefits of this first revolution were generally limited to a handful of large military forces; however, the democratization of digital technologies has arguably overturned this dynamic.

Social networking, mobile communications, and global access to the Internet have enhanced the power of individuals and small groups relative to that of nation-states and hierarchical bureaucratic entities. The second digital revolution has lowered the barrier of access to advanced technical capabilities previously limited to first tier militaries. Now, relatively sophisticated cybertools are available even to poorly resourced actors. This rapid diffusion of digital technology has arguably become a key enabler for irregular warfare and accelerated the disaggregation of power away from conventional military forces.[42] The cyberdomain provides nonstate groups with a means to communicate, coordinate, and project influence on a global scale without requiring significant investment in research and development infrastructure or even a formalized program of procurement. These developments present a number of operational challenges for U.S. forces as well as questions on how to properly place these emerging threats within an appropriate doctrinal framework.

An Evolving Doctrinal Framework for Targeting in the Cyberdomain

The aforementioned examples of how ISIL and other nonstate actors are using the cybertools to create effects in the physical battlespace presents a number of challenging doctrinal questions. Technically speaking, most of these activities do not constitute cyberoperations per se, even as adversaries use cybertools to

produce demonstrable effects on the ground. The purposes of these activities—command and control, intelligence gathering, training, recruiting and propaganda—do not in fact represent cyberoperations in a doctrinal sense.[43] Nevertheless, they do exploit some of the unique characteristics of the cyberdomain to protect identity, veil attribution, and complicate targeting. The U.S. military has only recently begun considering the implications of how emerging cybertools may be applied on future battlefields as well as how to categorize such activities to develop appropriate responses, protocols, and targeting methodologies.

One expert in the field recently noted how the lack of historical example and the cross-domain nature of cyber makes it extremely difficult to fit these concepts into an existing doctrinal framework.[44] One important catalyst for these discussions was the 2011 publication of the *Department of Defense Strategy for Operating in Cyberspace*. This document marked a doctrinal paradigm shift by designating cyberspace as a distinct yet interdependent operational domain equivalent to that of air, land, maritime, and space.[45] This designation tacitly acknowledged the militarization of cyberspace and highlighted the fact that cyberoperations are expected to play a critical role in future conflicts.[46]

The DOD strategy paper also acknowledged the unique characteristics of cyberoperations that complicate the direct application of conventional warfighting concepts to this domain. Most obviously, threats in cyberspace do not recognize national boundaries or formally declared zones of conflict. They are ill defined, asymmetric, and often difficult to attribute.[47] They do not always have a discernable kinetic parallel in terms of generating unambiguous physical effects. Furthermore the nature of the technical tools used in this domain can make it difficult to draw clear operational distinctions between cyberwar, cyberterrorism, cyberespionage, and cybercrime. These characteristics impose certain limitations on the application of state-centric security concepts such as deterrence, escalation, and proportionality in the development of military cyberstrategy.[48] Nevertheless, when it comes to targeting in the cyberdomain, existing doctrine still generally applies a conceptual framework that more or less mirrors the methods applied to conventional maneuver warfare.[49] This fact seems to reflect a degree of doctrinal inertia that dangerously underestimates the unique operational characteristics of this domain.

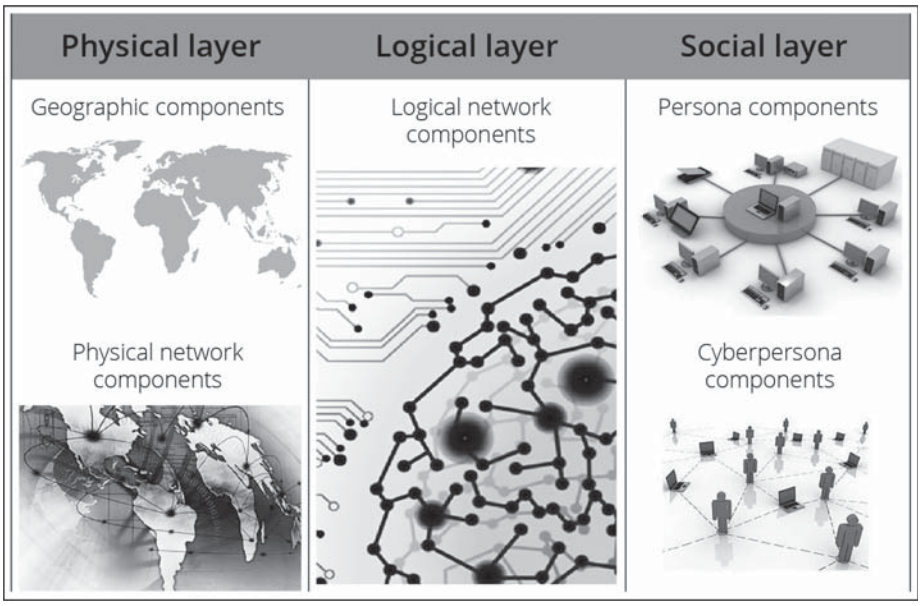
As already discussed, one of the most important characteristics making the cyberdomain uniquely challenging from a targeting perspective is the issue of attribution. As a basic technical matter, this differs significantly from conventional military operations where uniforms, weapons systems, and physical geography generally produce detectable signatures that can reveal an adversary's identity, location, and activities.[50] The conventional Intelligence, Surveillance, and Reconnaissance capabilities at the operational level, however, presently offer relatively few tools to help commanders visualize the cyberpersona layer

of their immediate operational environment.[51] At these echelons, cyberintelligence focused primarily on issues of network defense and information assurance. This situation is partly due to a lack of cyber-resources and technical expertise below the strategic level; however, there is also a conceptual component that has slowed progress on this front.

U.S. military organizations generally remain focused on conventional warfighting concepts and consequently struggle with the more abstract implications of how adversaries might apply cybertools to create effects in the physical battlespace. This mindset also applies generally to operational planners who are more comfortable thinking in terms of the traditional elements of combat power: mass, maneuver, and firepower. Yet, these factors are less obviously applicable as conceptual anchors for understanding the military effects of cybertools or selecting the best means of targeting adversaries operating within this domain.

Recent doctrinal publications have made some progress in offering a framework for understanding how the cyberdimension shapes the overall operational environment. *Cyberspace Operations* describes this space in terms of three distinct layers: a physical network forming the medium where data travels, a logical network representing the signal topology and arrangement of devices on the network, and finally the cyberpersona layer representing the digital representation of individuals or entities operating in cyberspace (figure 1).[52] The cyberpersona layer is the abstract representation of the actors behind the network and represents the most challenging aspect from a targeting perspective. For example, complex

Figure 1. The three layers of cyberspace



Adapted from U.S. Army, Cyberspace Operations Concept Capability Plan 2016–2028 *by MCUP.*

digital identities could manifest concurrently at multiple locations while some may not even be traceable to a single discrete physical node. A single entity may have multiple cyberpersonae, such as the case with Russian Internet trolls who conduct information campaigns by using dozens, sometimes hundreds of digital identities.[53] Alternatively, a single cyberpersona could represent numerous different user identities, such as the case with the online activist group Anonymous.[54] For this reason, the actions of a cyberpersona may not be easily be attributed to a state, an army, or an individual actor.

These abstractions make it difficult to conceptualize how military forces might effectively integrate cybereffects into a conventional targeting plan. Without a clearly defined adversary identifiable as a dot on a map, much of the basis for conventional targeting doctrine becomes untenable. Furthermore, in the cyberdomain, launching attacks against an adversary's computers, cell phones, and social media accounts may actually have the adverse effect of eliminating the only source of insight on the identities and operations of the network. In light of these challenges, the latest DOD cyberstrategy moves in the right direction by emphasizing the need for improved "intelligence and attribution capabilities help to unmask an actor's cyberpersona, identify the attack's point of origin, and determine tactics, techniques, and procedures" to support credible deterrence, response, and denial operations.[55]

One recent paper on cyberintelligence noted how dealing with these threats must go beyond the issue of network defense.[56] As doctrinally defined, cyberoperations do not encompass the growing scope of influencing activities that are now taking place in the digital domain. Therefore, cyberintelligence must evolve as an all-source discipline and not be limited only to the technical aspects of network protection. This means that cyberanalysts must also have an understanding of the human dimension of cyberoperations. This includes techniques for identifying the actors behind the keyboards; knowing how adversaries plan, coordinate, and execute their operations; and understanding what motivates them toward action.[57] In many respects, this makes targeting in the cyberdomain a logical extension of the identity-based approaches refined during recent conflicts.

New Technologies and Methods for Building Cyber Situational Awareness

As the cyberdomain increasingly represents "key terrain" of irregular warfare, the task of developing situational awareness will become a critical need for conventional military forces. This will involve integrating new technical tools and analytical methods designed specifically for identifying, tracking, and targeting anonymous actors using cybertools as a medium for creating effects in the physical landscape. The urgent need for "strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confi-

dence in attribution" was recognized in the DOD's most recent cyberstrategy document.[58] At the present time, however, military commanders, particularly at the operational level, still lack the technical means and analytical methods for identifying these actors, mapping their activities, and understanding how they exert influence on the battlefield. The high-profile case of Jihadi John demonstrated the power of being able to identify an unknown actor on social media and then link digital patterns of life information to an actual person, a physical location, specific activities, or associations; however, the hunt required national level assets far removed from operational commanders.[59]

Traditional computer network analysis can provide methods for obtaining some contextual information through technical means. For instance, an anonymous cyberpersona must still interface through a physical plane that contains information about device hardware and operating characteristics. Additionally, analysis of the logical plane may reveal such information as network addresses and configuration settings, and in some cases, even the geographic location of a user. While these attributes can help to characterize how a cyberpersona operates, they do not necessarily expose the identity of the individual behind the screen. To derive this type of information, a cyberpersona would need to be linked to an identifiable user account, digital certificates, or stored biometric data, but even this information may not provide a definitive picture of whose fingers are on the keyboard. This offers the cyberequivalent of signature-based targeting where analysts infer a target's identity based on the characteristics of observed activity. This method does not necessarily reveal exactly who is using a SIM card, however, only whether or not the users' activities fit a known behavioral pattern.

This example also highlights the point that insurgents, terrorists, and irregular combatants do not emanate the same technical signatures as conventional military forces, therefore characterizing and targeting these entities requires different collection methods and analytical approaches. This is true regardless of whether the adversary occupies a physical presence on the battlefield, hides among an indigenous population, or operates as a cyberpersona maneuvering through the digital landscape. Also, unlike professional armies that function on doctrinal precepts, irregular forces generally have less discernable templates guiding their actions, making predictive analysis a much more daunting challenge. For these reasons, identity-based targeting in the cyberdomain requires tools and methods that are better able to exploit remotely accessible attributes and indicators.

As one example, behavioral biometrics offers some potential techniques for establishing identity by indirect means that may be well suited to the challenges of cyberoperations. In general terms, behavioral biometrics refers to identifying characteristics that are learned or acquired over time rather than those based primarily on biology—for instance, using such features as "style, preference, knowledge, motor-skills or strategy" that people use in "human actions which result

from specific to everyday human skills."[60] Some common examples of measurable traits include handwriting, keystroke movements, or mouse dynamics. Other examples include distinguishing behavioral patterns that can be derived from common online activities, including email routines, digital device interactions, or credit card usage.

Where traditional biometrics can be limited in use, behavioral biometrics often provides missing benefits; most notable is behavioral biometrics' potential for "stand off" or noncompliant collection. For instance, patterns of email usage or web surfing offer the possibility of deriving unique user identifications with the advantage of nonobtrusive collection. Multiple studies have demonstrated how unique behavioral profiles can be derived from the peculiarities of message stylization, temporal activity, sentence structure, and other variables.[61] This has obvious applications for resolving ambiguous identities derived from user accounts or devices shared among multiple individuals. Similar applications have been developed to spot aberrant behavior on social media platforms, such as detecting fake Twitter and Facebook accounts. Behavioral biometrics can also be applied to help identify online deception campaigns by analyzing linguistic cues, usage patterns, social connections, and physical locations to help characterize the identities behind the posts.

Behavioral biometrics is also being used to modernize the analysis of "digital handwriting" or dynamic signatures derived from the unique way a user types or manipulate a digital device. These cognitive-biometric attributes are being used for identity authentication on mobile devices by analyzing such factors as handedness, hand tremor, eye-hand coordination, keystroke analysis, and other identifiable patterns derived from human–machine interactions.[62] Researchers have found these behavioral patterns to be "complex, nuanced and instinctive," thereby offering a highly accurate method for identifying individuals based on their use of digital devices.[63]

Another recent experiment has identified unique "egocentric video biometrics" derived from raw video footage taken from head- and body-mounted cameras.[64] One potential application of this technique would be the ability to locate all videos shot by a single user from within a large database of digital files even without the benefit of descriptive metadata. Similar techniques have been developed for generating biometric authentication from computer mouse manipulation and fitness tracking devices. Such information could be invaluable for identity verification when combined with precise geo-location derived from a mobile device or when correlated with other social media activity. As humans increasingly maintain nearly continual interaction with their digital devices, the field of behavioral biometrics potentially offers a range of techniques well suited for deriving identity information from online activities.

The ability to apply digital forensics or behavioral biometrics to positively

identify cyberpersonae will also increase the value of social media exploitation. While this remains a complex technical challenge due to vast amounts of low-value raw data, it does offer some means for mapping out an increasingly complex digital landscape and identifying key nodes of activity that could influence the physical battlespace. For example, in early 2014, analysts were able to track Russian military movement into Crimea using social media "bread crumbs" dropped by personnel preparing for mobilization. Separately, YouTube videos and Twitter messages posted by Russian irregulars provided the first hints of attribution for the downing of Malaysia Airlines Flight 17 in eastern Ukraine in July 2014.[65]

The ability to derive useful identity information of threat actors from a vast sea of digital activity will depend on major advances in computing power and new analytical methods. Artificial Intelligence, machine learning, and methods for dealing with the challenge of interpreting "big data" are areas where technology is expected to improve the ability of analysts to sort through large amounts of unstructured information to discern patterns, trends, and embedded associations among actors.[66] These tools could be particularly useful for discovering unseen correlations between the online activities of cyberpersonae and identity signatures in the physical domain. These tools have already demonstrated significant potential for improving the accuracy and power of standard biometric modalities, such as increasing the speed and accuracy of the image recognition applications used by Facebook, Google, Microsoft, and Twitter.[67]

In addition to new collection modalities, U.S. forces will need innovative approaches to informational management that are better suited for processing the vast amounts of data generated by a world of networked adversaries. A recent white paper by the under secretary of defense for intelligence highlighted the nature of this new environment by noting how individuals are increasingly becoming "self-documenting" by creating digital trails of potentially useful data during the conduct of their daily lives.[68] Ubiquitous interconnectivity via email, social media, digital commerce, and interface with the "internet of things" all combine to create a dense layer of interactions that expose much of who we are, where we go, and how we live our lives. This phenomenon presents a significant analytical challenge to derive meaning and actionable intelligence from the deluge of big data.[69]

Relatively new concepts—for example, Activity-Based Intelligence (ABI) and Object-Based Production (OBP)—provide some examples of analytical approaches that may be well suited for identity-based targeting in such data-rich environments. For example, ABI exploits the potential of big data by replacing collection discipline-centric analysis with an activity-based approach that focuses on all of the physical and virtual transactions associated with a specific entity.[70] ABI was originally conceived as an analytical approach optimized for identity-

based targeting on an irregular battlefield by focusing on the interactions and associations that define adversary networks.[71] This methodology was used to generate the kind of pattern of life analysis needed to dismantle insurgent groups in Iraq and Afghanistan.

Similarly, OBP is designed to deal with the challenge of information discovery and attribute correlation in an environment defined by disaggregated and heterogeneous data. As a method, OBP focuses on organizing information around a single object such as "people, places, and things [that become] the single point of convergence for all information and intelligence produced about a topic of interest."[72] This way of organizing data enables an analyst to visualize an entity's attributes, associations, and activities. For example, the information relating to an individual or group can be correlated with all information linked to that object, such as related attributes, common activities, or associations with other similar entities.[73] This could also include linkages to physical attributes from biometric, biographic, or forensic data. These novel approaches to information management may be better able to support the kind of data-intensive analyses that are needed to uncover deeply embedded associations from within large amounts of unstructured identity data scattered across the digital landscape.

As the military searches for new technologies to improve cyber situational awareness, it is likely that the commercial sector will provide some of the most powerful and innovative tools. As one example, the world of online advertising provides a useful model for how such cybercapabilities might evolve. In recent years, these firms have refined methods for resolving the identities of cyberpersonae using algorithms designed for probabilistic matching. Based on IP addresses, browser activity, authorship analysis, behavioral cues, and other digital signatures, these companies have been able to correlate identifiers so that entities can be tracked as they move across the cyberlandscape.[74]

Similarly, online retailers routinely gather detailed information about "spending habits, credit histories, web-surfing histories, social network postings, demographic information, and so on" for the purpose of market research and generating "precisely targeted advertising."[75] These activities can be linked and used to accurately track a single user across multiple devices and platforms by creating a "digital fingerprint" that correlates the cyberpersona to an actual physical identity. Social media companies are also becoming skilled at using geo-tracking, metadata, speech, and content analysis as methods for spotting unauthorized users or detecting fraudulent activities. In many ways, these examples offer precisely the kinds of tools needed by military cyberanalysts to help identify and analyze key influencers within an operational environment and potentially provide the kind of fidelity to target cyberpersonae across the digital landscape that the military has used to observe actors in the physical battlespace.

Conclusion

In recent years, there have been several vivid examples of adversaries using cybertools to create substantive military effects in the physical domain. These have included many activities falling outside of the strict doctrinal definition for cyberoperations. In particular, these tools have played an increasingly visible and consequential role in a wide range of irregular conflicts as part of terrorism activities and in gray zone or hybrid conflicts. One commonality among these examples is that both state and nonstate actors have leveraged the anonymity offered by cybertools as a means of creating strategic ambiguity and confusion over attribution of their activities. While deception and surprise have always been elements of warfare, these recent examples of state and nonstate actors using sophisticated technologies to mask identity present a significant challenge to conventional military targeting methods.

Dealing with this new kind of threat will require a paradigm shift in thinking about the meaning of situational awareness and targeting in the cyberdomain. A first important step will be better educating mid-level military leaders about the technical aspects of cyberoperations. This includes offering a clear doctrinal framework that integrates cyberconsiderations into the overall planning cycle and targeting process at the tactical and operational levels. This will require improved tools and analytical methods so that military commanders below that strategic level can have a common operational picture that takes into account all entities influencing the battlespace, including actors in the cyberpersona layer.

For the larger DOD enterprise, these solutions must also consider the looming challenge of encryption and other technical tools enabling adversaries to operate anonymously and avoid attribution. This problem will only become more acute as both state and nonstate adversaries continue to erode the slim relative advantages that the United States still enjoys with regard to cyberoperations—an edge that many experts suggest has already disappeared.

One starting point for designing a conceptual approach for cybertargeting may be to view it as a logical extension of the identity-based targeting techniques developed during recent campaigns. These examples share similarities in terms of the challenges faced by military forces when targeting irregular adversaries as well as the issues of identity and attribution in modern warfare. Expanding existing concepts such as I2 to the cyberdomain would provide a doctrinal framework for linking digital identities to corresponding biologic and biographic information in the physical domain. As a model for military innovation, the recent examples of biometrics and expeditionary forensics offer useful lessons learned for integrating nonmilitary technologies onto the battlefield and devising effective doctrinal frameworks for their use. These capabilities reflect an important operational need as adversaries increasingly use cybertools in order to create meaningful effects on the physical battlefield.

Notes

The views expressed in this article are the authors' own and do not reflect the official policy or position of the Department of Defense (DOD), the U.S. government, or NATO.

1. Among other studies, see Defense Science Board Task Force on Defense Intelligence, *Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2011).
2. In the context of this discussion, the term *targeting* is applied in a broad doctrinal sense referring to "the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities." See U.S. Joint Chiefs of Staff (JCS), *Joint Targeting*, Joint Publication (JP) 3-60 (Washington, DC: JCS, 2013), vii.
3. The JCS defines biometrics as "the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics." See JCS, *Joint Intelligence*, JP 2-0 (Washington, DC: JCS, 2013), GL-5. Intelligence information derived from biometric data helps link an unknown identity to places, activities, and networks and supports related pattern analysis to facilitate operations, such as high-value individual targeting. Forensics describes the scientific analysis of materials, such as DNA, used to link persons, places, things, and events.
4. David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone'," *War on the Rocks* (blog), 19 May 2015, http://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/. While there are multiple definitions of "hybrid conflict," the salient point for this discussion is the prevalence of irregular combatants using anonymity and ambiguous legal status for operational advantage. This may include a range of state, nonstate, and proxy actors whose uncertain identity and affiliation becomes a defining feature of the operational space. For a useful discussion on this topic, see Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly*, no. 52 (1st Quarter 2009): 34–39, http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf.
5. Howard Altman, "'Gray Zone' Conflicts Far More Complex to Combat, Says Socom Chief Votel," *Tampa* (FL) *Tribune*, 28 November 2015, http://www.tbo.com/list/military-news/gray-zone-conflicts-far-more-complex-to-combat-says-socom-chief-votel-20151128/.
6. According to JCS, *Cyberspace Operations,* JP 3-12(R) (Washington, DC: JCS, 2013), GL-4, the term *cyberspace* refers to the "global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
7. Attribution refers to the task of positively identifying threat actors and linking these entities to activities within the operational environment where JCS, *Information Operations,* JP 3-13 (Washington, DC: JCS, 2014), x, defines "operational environment" as a "composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."
8. DOD, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: DOD, 2011), 4, https://fas.org/irp/eprint/dod-cyber.pdf.
9. "The cyber-persona layer consists of the people actually on the network" according to JCS, *Cyberspace Operations*, I-3.
10. Intelligence and National Security Alliance (INSA), Cyber Intelligence Task Force, *Operational Levels of Cyber Intelligence* (Arlington, VA: INSA, 2013), 1.
11. *Worldwide Threats to the Homeland, Hearing Before the Senate Committee on Homeland Security* (17 September 2014) (statement of Matthew G. Olsen, director National Counterterrorism Center).
12. Elias Groll, "Welcome to the Future of War: ISIS Has a Smartphone App," *Foreign Policy*, 8

December 2015, http://foreignpolicy.com/2015/12/08/welcome-to-the-future-of-war-isis-has-a-smartphone-app/.

13. National Intelligence Council (NIC), *Global Trends 2030: Alternative Worlds* (Washington, DC: NIC, 2012), 86.
14. Marc Lynch, Deen Freelon, and Sean Aday, "Blogs and Bullets III: Syria's Socially Mediated Civil War," *Peaceworks*, no. 91 (2014), www.usip.org/sites/default/files/PW91-Syrias%20Socially%20Mediated%20Civil%20War.pdf.
15. J. M. Berger and Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, Brookings Project on U.S. Relations with the Islamic World, Analysis Paper No. 20 (Washington, DC: Brookings, 2015), 2; and Brian Bennett, "With Islamic State Using Instant Messaging Apps, FBI Seeks Access to Data," *Los Angeles Times*, 8 June 2015, www.latimes.com/world/middleeast/la-fg-terror-messaging-20150608-story.html#page=1 1/5.
16. Gabriel Weimann, *New Terrorism and New Media* (Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014), 2; and Haroro J. Ingram, "Three Traits of the Islamic State's Information Warfare," *RUSI Journal* 159, no. 6 (2004): 4–11, doi:10.1080/03071847.2014.990810.
17. Eric Liu, *Al Qaeda Electronic: A Sleeping Dog?* (Washington, DC: American Enterprise Institute Critical Threats Project, 2015), http://www.criticalthreats.org/sites/default/files/Al_Qaeda_Electronic.pdf.
18. Joseph A. Carter, Shiraz Maher, and Peter R. Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks* (London: International Centre for the Study of Radicalisation and Political Violence, 2014), www.icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf.
19. Robert Hannigan, "The Web Is a Terrorist's Command-and-Control Network of Choice," *Financial Times*, 3 November 2014, http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3yXscPso1.
20. Bruce Schneier, "Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle," *Christian Science Monitor*, 4 March 2015, www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0304/Hacker-or-spy-In-today-s-cyberattacks-finding-the-culprit-is-a-troubling-puzzle.
21. Ibid.
22. Weimann, *New Terrorism and New Media*, 1.
23. Ibid., 10.
24. Brian Bennett, David S. Cloud, and W. J. Hennigan, "Pentagon Weighs Cybercampaign against Islamic State," *Los Angeles Times*, 20 December 2015, http://www.latimes.com/world/la-fg-cyber-isis-20151220-story.html.
25. Scott Shane, Matt Apuzzo, and Eric Schmitt, "Americans Attracted to ISIS Find an 'Echo Chamber' on Social Media," *New York Times*, 8 December 2015, http://nyti.ms/1NKAFzy.
26. Bennett, "With Islamic State Using Instant Messaging Apps."
27. "Islamic State Unfriended," *Economist*, 12 December 2015, http://www.economist.com/node/21679805/print.
28. "Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by the military, journalists, law enforcement officers, activists, and many others." See "Inception," Tor, 28 January 2016, https://www.torproject.org/about/torusers.html.en. For one recent overview on the national security implications, see Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, Global Commission on Internet Governance Paper Series 21 (Waterloo, ON, Canada: Centre for International Governance Innovation, London: Chatham House, 2015).
29. Michael Chertoff and Tobby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, Global Commission on Internet Governance Paper Series No. 6 (Waterloo, ON, Canada: Centre for International Governance Innovation, London: Chat-

ham House, 2015), 1, https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

30. For a discussion of the potential for anonymous use of Bitcoin, see Edward V. Murphy, M. Maureen Murphy, and Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues* (Washington, DC: Congressional Research Service, 2015), 3.
31. Although Bitcoin does not reveal the user's actual identity, the record of transactions is completely public in the form of a block chain that could be used in some instances to infer identity. For a discussion, see Joshua Baron et al., *National Security Implications of Virtual Currency: Examining the Potential for Non-state Actor Deployment* (Santa Monica, CA: Rand, 2015).
32. Aaron Brantly, "Financing Terror Bit by Bit," *CTC Sentinel* 7, no. 10 (October 2014): 1–5.
33. Tim Fernholz, "Terrorism Finance Trackers Worry ISIS Already Using Bitcoin," *Defense One*, 13 February 2015, www.defenseone.com/threats/2015/02/terrorism-finance-trackers-worry-isis-already-using-bitcoin/105345/?oref=defenseone_today_nl.
34. Patrick Tucker, "How the Military Will Fight ISIS on the Dark Web," *Defense One*, 24 February 2015, www.defenseone.com/technology/2015/02/how-military-will-fight-isis-dark-web/105948/?oref=defenseone_today_nl.
35. Doug Bernard, "Crime and Espionage Becoming Tangled Online," *Voice of America*, 5 September 2015, http://www.voanews.com/content/crime-and-espionage-becoming-tangled-online/2949167.html.
36. Ibid.
37. Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," *Comparative Strategy* 34, no. 2 (2015): 133–48, doi:10.1080/01495933.2015.1017342.
38. Daniel Regalado, Nart Villeneuve, and John Scott Railton, *Behind the Syrian Conflict's Digital Front Lines* (Milpitas, CA: FireEye, 2015), 5.
39. Ibid., 18.
40. Grohe, "The Cyber Dimensions of the Syrian Civil War," 140.
41. David E. Sanger and Eric Schmitt, "Hackers Use Old Lure on Web to Help Syrian Government," *New York Times*, 1 February 2015, www.nytimes.com/2015/02/02/world/middleeast/hackers-use-old-web-lure-to-aid-assad.html?_r=0.
42. Robert A. Johnson, "Predicting Future War," *Parameters* 44, no. 1 (Spring 2014).
43. JCS, *Joint Operations*, JP 3-0 (Washington, DC: DOD, 2011), GL-8, defines *cyberspace* operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." DOD, Office of the General Counsel, *Law of War Manual* (Washington, DC: DOD, June 2015), para. 16.1.2, states that "cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace." This second tenet presents the ambiguity for the described situations above because many of the intended effects are for the ground or physical battlespace, rather than cyberspace.
44. Erick Waage, "Phreaker, Maker, Hacker, Ranger: One Vision for Cyber Support to Corps and Below in 2025," *Small Wars Journal* (blog), 11 August 2015, http://smallwarsjournal.com/jrnl/art/phreaker-maker-hacker-ranger-onevision-for-cyber-support-to-corps-and-below-in-2025.
45. DOD, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: DOD, 2011), http://www.defense.gov/news/d20110714cyber.pdf.
46. This viewpoint is implicitly articulated in the establishment of U.S. Cyber Command as a subunified command of U.S. Strategic Command, responsible for coordinating the cyberactivities of the individual military Services. *Department of Defense Strategy for Operating in Cyberspace* specifically states on page 5 that "DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace."
47. Catherine Lotrionte, "Statecraft in Cyberspace," *Cipher Brief*, 13 December 2015, https://www.thecipherbrief.com/article/statecraft-cyberspace.
48. William J. Lynn III, ed., "Defending a New Domain: The Pentagon's Cyberstrategy," *Council on Foreign Relations*, September/October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain?gp=66687%3A31ac65264c9a4440.
49. JCS, *Joint Targeting*, C-7.

50. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1 (2014): 9, doi:10.1080/01402390.2014.977382.
51. The Army and other Services have recognized these shortfalls and prioritized establishment of capabilities at this level. One means to do so is developing cyberteams that can find, fix, and mitigate currently undetected malicious actors in military networks and provide capabilities to integrate cyberexpertise into Army land operations to support tactical and operational cyberplanning and integration. See, Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications* (Carlisle Barracks, PA: U.S. Army War College Press, 2015), http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1246.pdf.
52. JCS, *Cyberspace Operations*, I-2.
53. Paul Roderick Gregory, "Putin's New Weapon in the Ukraine Propaganda War: Internet Trolls," *Forbes*, 9 December 2014, http://www.forbes.com/sites/paulroderickgregory/2014/12/09/putins-new-weapon-in-the-ukraine-propaganda-war-internet-trolls/.
54. For a discussion on this point and cybertargeting methodology, in general, see Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in *2012 4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence, 2012).
55. DOD, *The Department of Defense Cyber Strategy* (Washington, DC: DOD, 2015), 12, www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
56. Cyber Intelligence Task Force, *Operational Levels of Cyber Intelligence*, 11.
57. Ibid.
58. DOD, *Department of Defense Cyber Strategy*, 11.
59. Patrick Tucker, " 'Jihadi John' and the Future of the Biometrics Terror Hunt," *Defense One*, 27 February 2015, http://www.defenseone.com/technology/2015/02/jihadi-john-and-future-biometrics-terror-hunt/106263/.
60. Liang Wang and Xin Geng, *Behavioral Biometrics for Human Identification: Intelligent Applications* (Hershey, PA: Medical Information Science Reference, 2010), 26.
61. Roman V. Yampolskiy and Venu Govindaraju, "Behavioural Biometrics: A Survey and Classification," *International Journal of Biometrics* 1, no. 1 (2008): 81–113.
62. For one recent example of these applications, see patent filing for Israeli behavioral biometrics firm BioCatch and the related article, Stephen Mayhew, "BioCatch Granted Behavioural Biometric Patent for Mobiles," Planet Biometrics, 24 February 2015, www.planetbiometrics.com/article-details/i/2746.
63. James Vincent, "Behaviosec Uses 'Behavioral Biometrics' to Find if the Person Using a Mobile Device Is Really Who They Claim to Be," *Economic Times*, 2 September 2014, www.economictimes.indiatimes.com/news/international/business/behaviosec-uses-behavioural-biometrics-to-find-if-the-person-using-a-mobile-device-is-really-who-they-claim-to-be/articleshow/41463585.cms.
64. Yedid Hoshen and Shmuel Peleg, "Egocentric Video Biometrics," Hebrew University of Jerusalem, 27 November 2014, www.arxiv.org/pdf/1411.7591v1.pdf.
65. Julian E. Barnes, "U.S. Military Plugs into Social Media for Intelligence Gathering: Defense Intelligence Agency Head Says Online Postings Played Crucial Role in Ukraine Jet Shootdown Investigation," *Wall Street Journal*, 6 August 2014, http://www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557.
66. Babak Hodjat, "Myth Busting Artificial Intelligence," *Wired Magazine*, http://www.wired.com/insights/2015/02/myth-busting-artificial-intelligence/.
67. Quentin Hardy, "Facebook Offers Artificial Intelligence Tech to Open Source Group," *New York Times Bits* (blog), 16 January 2015, http://bits.blogs.nytimes.com/2015/01/16/facebook-offers-artificial-intelligence-tech-to-open-source-group/.
68. Gabriel Miller, "Activity-Based Intelligence Uses Metadata to Map Adversary Networks," *Defense News*, 8 July 2013.
69. For a useful, recent introduction, see Paul B. Symon and Arzan Tarapore, "Defense

Intelligence Analysis in the Age of Big Data," *Joint Forces Quarterly*, no. 79 (4th Quarter 2015): 4–11, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_4-11_Symon-Tarapore.pdf.

70. Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Forces Quarterly*, no. 77 (2d Quarter 2015): 24–33, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_24-33_Atwood.pdf.
71. Mark Phillips, "A Brief Overview of ABI and Human Domain Analytics," *Trajectory Magazine*, 2012, http://trajectorymagazine.com/civil/item/1369-human-domain-analytics.html.
72. Catherine Johnston et al., "Transforming Defense Analysis," *Joint Forces Quarterly*, no. 79 (4th Quarter 2015): 12–18, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_12-18_Johnston-et-al.pdf.
73. Shawn Riley, *Science of Cybersecurity: Developing Scientific Foundations for the Operational Cybersecurity Ecosystem* (Washington, DC: Centre for Strategic Cyberspace + Security Science), 11 August 2015, http://cscss.org/wp-content/uploads/2015/08/CSCSS-Science-of-Security-Developing-Scientific-Foundations-for-the-Operational-Cybersecurity-Ecosystem.pdf.
74. Adam Tanner, "How Ads Follow You from Phone to Desktop to Tablet," *MIT Technology Review*, 1 July 2015, www.technologyreview.com/news/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/.
75. NIC, *Global Trends 2030*, 88.

Russia's Ambiguous Warfare and Implications for the U.S. Marine Corps

Mary Ellen Connell and Ryan Evans

Abstract. The Russian Federation used ambiguous warfare strategies to annex Crimea in 2014 and propagate Ukrainian instability. Rapidly generated, highly trained, and well-disciplined Russian forces on the ground in Ukraine unofficially coordinated with pro-Russian separatists to conduct psychological operations, intimidation, and bribery among the population to undermine nationalist resistance. Illustrating warfare's expanding reach, these activities obscure the factors that the North Atlantic Treaty Organization traditionally uses to identify the need for the cooperative defense of a member nation. This summary of a CNA-organized meeting of experts captures these topics and their implications on the U.S. government's current warfighting strategy.

Keywords: Gerasimov Doctrine, Russia, Ukraine, Crimea, Donbass, Baltic states, Spetsnaz, U.S. Marine Corps, *maskirovka,* ambiguous warfare, warfighting strategy, unmanned aerial vehicle, drone use

In 2014, "little green men"—strongly suspected to be Russian Federation soldiers—surged into Crimea and drove out all elements and symbols of Ukrainian authority.[1] Peace now prevails on the Crimean peninsula under Russian control, but as of this writing, war still rages in Ukraine's eastern region of Donbass, where Russian-backed separatists wield Russian weapons, drive Russian

Mary Ellen Connell is a research scientist with CNA's Center for Strategic Studies and a graduate of the National War College. A former counselor in the U.S. Senior Foreign Service, Connell served at U.S. embassies in Africa and Europe and the U.S. mission to NATO.

Ryan Evans is a research analyst at CNA's Center for Strategic Studies and the founder and editor in chief of *War on the Rocks*.

MCU Journal vol. 7, no. 1
Spring 2016
www.mcu.usmc.mil/mcu_press
DOI:10.21140/mcuj.2016070102

tanks, and reportedly fight alongside unacknowledged Russian troops to wage war against the Ukrainian military.[2]

Annexing the Crimean peninsula and supporting instability in Ukraine's eastern provinces, the Russian Federation and its armed forces have used so-called ambiguous warfare to great tactical and operational effect (map 1). This brand of warfare, or Gerasimov Doctrine, involves rapidly generating highly trained and disciplined forces who enter the battlespace out of uniform and in coordination with local supporters, using psychological operations, intimidation, and bribery to undermine nationalist resistance.[3]

Although direct confrontation between U.S. Marines and Russian Federation forces is unlikely in the near future, other nations and nonstate actors that Marines may encounter within the battlespace are closely observing Russia's use of ambiguous warfare. Since these potential adversaries will likely modify their own warfare strategy and tactics, the Corps must also understand the lessons from Crimea and Ukraine and how other adversaries might militarily adapt as a result of Russia's success.

Ambiguous Warfare and the Gerasimov Doctrine

Although formally undefined, U.S. government professionals have used the term *ambiguous warfare* since at least the 1980s to refer to situations in which a state or

Map 1. Ukraine following Russia's 2014 annexation of Crimea

Adapted by MCUP.

nonstate belligerent actor deploys troops and proxies in a deceptive and confusing manner with the intent of achieving political and military effects while obscuring the belligerent's direct participation. Russia's actions in Crimea and Ukraine clearly align with this concept, and discussion participants pointed out that it was not a new concept for Russia.

The events in Crimea and Ukraine were foreshadowed by an article published by the Russian Chief of the General Staff Valery Gerasimov.[4] Gerasimov urged the academy to study and engage in the formulation of new doctrine and tactics to win future wars by explaining the rules of war have changed:

> In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template.
>
> The experience of military conflicts—including those connected with the so-called coloured revolutions in north Africa and the Middle East—confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war. . . . The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.
>
> The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population.
>
> All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.[5]

Experts in the CNA discussion agreed that the Gerasimov Doctrine evolved out of necessity, driven by Russian vulnerability rather than strength. Russia currently perceives itself to be reacting to a pressing external threat from a powerful adversary: the North Atlantic Treaty Organization (NATO). In December 2014, President Vladimir Putin signed the revised Russian Military Doctrine, which identifies NATO and its enlargement as a fundamental threat to the Russian homeland. Anticipating that the Russian Federation's largely conscript military forces would not prevail against NATO in conventional combat, the Gerasimov Doctrine advocates the use of a modern version of partisan warfare that targets an adversary's weaknesses and avoids direct, overt confrontations. Gerasimov

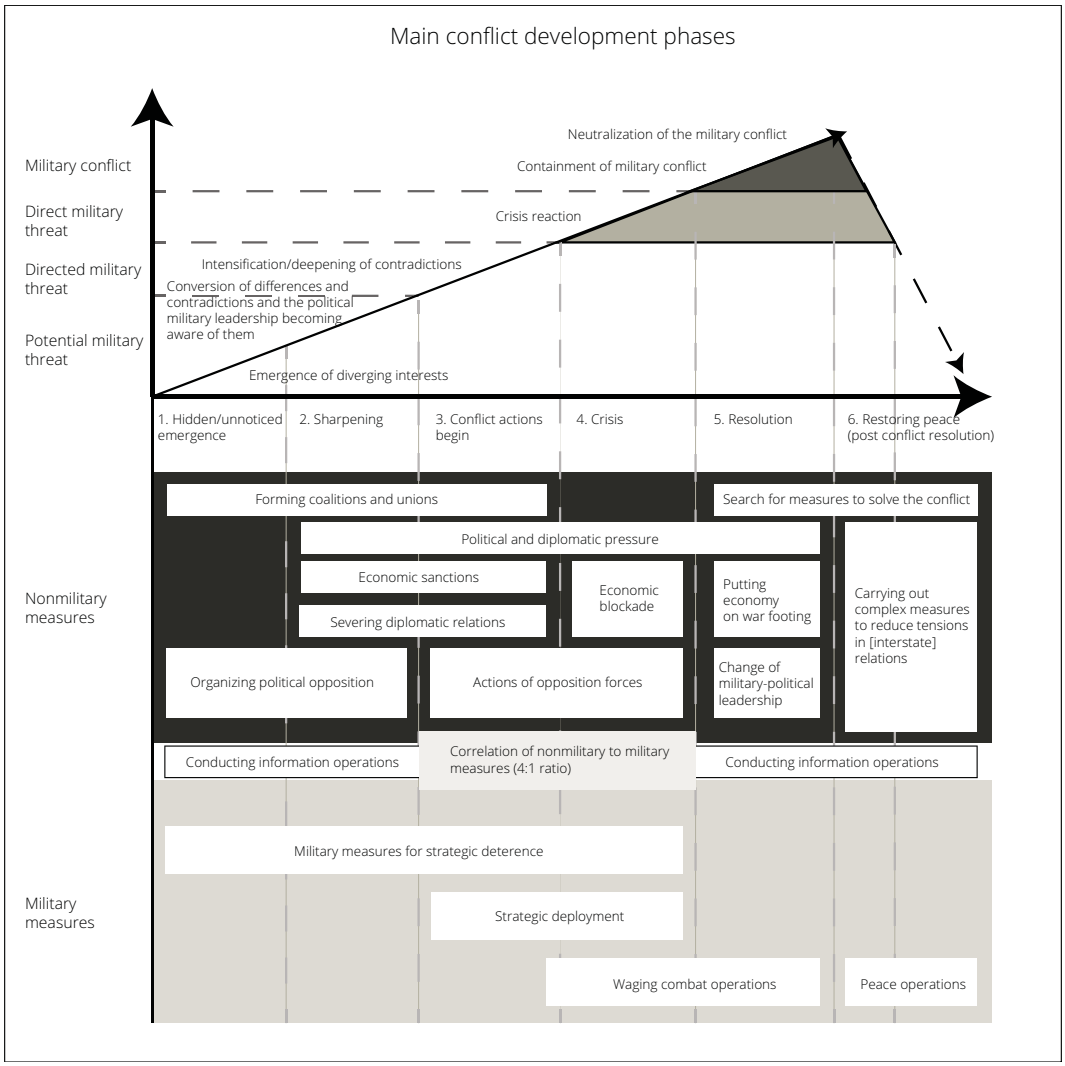
proposed a 4 to 1 ratio of nonmilitary to military measures. The nonmilitary measures in Gerasimov's doctrine include efforts to shape the political, economic, and social landscapes of the adversarial state through subversion, espionage, propaganda, and potentially a combination of these acts with cyberattacks. Grounded in *maskirovka*, the Soviet doctrine of denial and deception, use of ambiguous warfare keeps opponents wondering and hesitating by resolutely denying Russian involvement while working through as many agents as possible.[6] In Ukraine, for example, third-party deniable (covert) agents included pro-Russian loyalists and local paramilitary commanders, as well as local gangsters who spotted an opportunity for profit and power.

During the discussion, an expert described how Russia applied Gerasimov's concepts in six main phases: emergence, sharpening, initiating, crisis, resolution, and restoration. Figure 1 illustrates that, although the phases are not sequential, they contain overlapping actions. In the emergence phase, Russia uses ethnic and pro-Russian populations within the target state to foment protests and resistance to the country's government. Potentially, these actions initiate tension in the target country by generating backlash and discrimination against ethnic Russians by the government and majority populations. In essence, Russia activates a self-reinforcing mechanism to escalate conflict.

In the sharpening phase, Russia uses economic warfare and political pressure to intimidate, coerce, punish, and undermine governments in target states to further weaken them. In the initiating phase, Russia uses ambiguous military and security personnel to infiltrate the target country and activates criminal networks to further foment unrest and ignite open conflict. In the crisis phase, the military isolates government positions, seizes key terrain, and destroys the defense and security apparatuses of the target country. In the resolution phase, Russia conducts information operations to deny involvement and sow doubt and discord in the minds of foreign governments about the developing situation and possible responses. The restoration phase concludes the offensive; Russia consolidates its gains within the target country, takes actions to de-escalate the conflict and reduce tensions, and installs a government amenable to Russian influence.

As one expert noted, ambiguous warfare requires the deliberate integration of military and nonmilitary forces, and while it is a less expensive form of warfare than open, conventional war, it does not always lead to a clear military outcome. Another expert commented that credible escalation dominance is key to making ambiguous warfare work and added that Russia has adeptly maintained a carefully calibrated balance between low-intensity, ambiguous actions and credible, high-intensity (possibly even nuclear) threats.[7] Clearly, Russia's military has put Gerasimov's ideas to good practice in Crimea and Ukraine, though overwhelming success in Crimea has not been similarly replicated in eastern Ukraine to date.

Figure 1. Phases of Russia's ambiguous warfare



Adapted from Voenno-Promyshlennyi Kurier, *No. 8, 27 February 2013 by MCUP.*

Russia's Military and Special Forces

The Russian Military

To get a better sense of how Russia's military operationalizes Gerasimov's Doctrine, meeting participants discussed the structure of the Russian military generally, as well as its special forces, the Spetsnaz, specifically. One expert who has extensively studied the Russian military commented that nuclear weapons still play a central role in Russia's strategic thinking by allowing Russia to maintain a credible deterrent against Western action, as well as put forth a significant threat as part of the fourth phase of ambiguous warfare.

Russia also maintains a considerable military force with a sizeable reserve.

For example, one expert noted that, in less than one week, Russia could mobilize about one army (four brigades) and one airborne brigade. That said, however, Russia's military is spread thin over the longest land border of any single country. Additionally, Russia sees threats in all directions. As such, the experts discussed how Russia's military is aligned into different military districts. The Western District—the district concerned with Ukraine—has a large share of Russia's air force and air defense assets arrayed against possible NATO air threats from the West. Southern District forces are based in the volatile Caucasus region, which includes the Russian republics of Chechnya, Dagestan, and Ingushetia. Russians may now consider Crimea to be part of the Southern Military district, but the United States does not recognize the incorporation of Crimea into the Russian Federation. Eastern District forces protect the largely unpopulated eastern flank of Russia against potential threats from China. The Central Asia District largely serves as Russia's strategic reserve. This posture provides Russia's military with a limited ability to mass forces in any one direction without leaving gaps in the nation's defense elsewhere. Because ambiguous warfare does not require the higher resource demands of a sustained conventional campaign, the Russian armed forces find it an attractive option to mitigate the impact of overextended border defenses.

One expert noted that, unlike the West, Russia does not think about employing its military forces in terms of Services, such as army, navy, or special operations forces. Rather, its forces are primarily geared toward "fighting power" or "political impact" and use organizational constructs that place fighting power in support of political impact.

The Spetsnaz

One of Russia's major forces for political impact, the Spetsnaz played a significant role in the government's actions in Crimea and Ukraine. As Russia's special purpose forces, the Spetsnaz have historically conducted deep reconnaissance and nuclear missions, as well as disrupted adversary command and control structures in the context of large-scale conventional warfare. More recently, the force has gone through a painful but ultimately successful adaptation process to fight small wars more effectively.

In the past, the Russian military lacked a doctrinal base for small wars; however, in the wake of significant challenges in Russia's wars in Afghanistan and Chechnya, the military purposely evolved the Spetsnaz toward a more deliberate role in small wars. In 2011, Russia reorganized the Spetsnaz to serve as a support element to its ground units, as opposed to its traditional role supporting Russia's main intelligence directorate, the Glavnoye Razvedyvatel'noye Upravleniye (GRU). In 2012, Russia created its own special operations command, Komanda Spetsialnogo Naznacheniya, which was given oversight of the Spetsnaz for a time. The bureaucratic battles, however, in the Kremlin continued and, by

2013, the Spetsnaz returned to their original supporting role with the GRU. The 2014 Sochi Winter Olympics and the threats of terrorism that accompanied them were used to justify a major expansion of the Spetsnaz, and all of its units were brought to full strength.

Due to this level of readiness, one expert considers the Spetsnaz perhaps the GRU's most important political asset to their risk-taking organization and likely to remain so, given their practice of employing unorthodox agents, such as private sector individuals, warlords, mercenaries, and organized crime syndicates to conduct unconventional operations and ambiguous warfare. All present at the discussion agreed, however, that not all Spetsnaz are Tier 1 operators similar to personnel in U.S. military units, including the Army's Delta Force, the Navy's Seal Team 6, and the Marine Corps' Special Operations Command.[8] Of approximately 17,000 Spetsnaz, perhaps only 500 are trained as Tier 1 operators, while as many as 20–30 percent of the total number of Spetsnaz personnel are conscripts as opposed to professional special operators. In essence, these special purpose forces closely resemble U.S. light infantry intervention forces.

Russia's Current and Future Application of the Gerasimov Doctrine

Crimea

Russia's Crimea operation in late February 2014, apparently long considered a viable military option, went relatively smoothly. In the first-of-its-kind documentary, "Crimea: The Way Home," broadcast in Russia on 15 March 2015 (first anniversary of Crimea's disputed independence referendum), Russian president Vladimir Putin boasted that he had given the order on 22 February 2014 to rescue embattled Ukrainian leader Victor Yanukovych who had just fled Kiev and to "start working on returning Crimea to Russia."

In a 3 September 2014 article in the *Military-Industrial Courier*, cited by the Jamestown Foundation's *Eurasia Daily Monitor*, Colonel-General Anatoly Zaitsev enumerated the successes of the Crimea operation. Russia's normal resupply activities for its naval base leased in Sevastopol formed a convenient cover for the insertion of elite forces and equipment. Russian forces maintained strict radio silence, thus foiling NATO monitoring efforts. Partisan teams of Russia's Spetsnaz and naval infantry forces moved quickly and covertly throughout the peninsula to take control of key infrastructure. These teams isolated Ukrainian bases by cutting communications and disorganizing the Ukrainian troops' support systems. Simultaneously, Russia applied information warfare techniques to persuade Ukrainian forces to switch sides.[9]

Ultimately, Russia's operations in Crimea resulted in the annexation of key terrain for the Russian military at very low cost. Certainly, these operations surprised the West and served as a wake-up call regarding Russia's future intentions in the region.

Donbass, Eastern Ukraine

In April 2014, a pro-Russian insurgency erupted and quickly intensified within the Donbass coal mining region in Ukraine. The heartland of former Ukrainian president Viktor F. Yanukovich, Donbass borders the Russian Federation and most of the population speaks Russian.

Advised by Russian GRU officers, an odd collection of deniable agents—such as foreign volunteers, paid mercenaries, radical Russian nationalists, local mobsters, and former members of the disbanded Ukrainian Berkut special police force—took control of government institutions and key infrastructure in Luhansk and Donetsk, and proclaimed the cities independent people's republics. Despite the many factors favoring Moscow's design for the Donbass operation, experts discussing the operation doubt it went exactly as planned. The Russians found less support for the separatist agenda in Donbass than they had expected. The deniable agents who first assumed power in the Luhansk and Donetsk People's Republics were harsh, erratic administrators who often alienated the local population. Donbass residents able to escape the fighting did so by either going to Russia or by moving to safer areas in Ukraine. Military coordination among the separatists was poor, and they used sophisticated Russian-supplied equipment recklessly, as seen in the downing of Malaysia Airlines Flight MH17 on 17 July 2014.

By massing 40,000 troops on the Russian side of the border, Moscow heightened uncertainty and temporarily paralyzed decision making within the Kiev government while simultaneously deterring the West from offering significant military aid to Ukraine. Russian forces crossed the border at will, frequently under the cover of white-painted humanitarian convoys.[10] In August 2014, the Ukrainian military regrouped, closed in on separatist strongholds in Donbass, and reclaimed 65 towns and villages. It looked as though the military endgame was approaching. At that point, the Russians were forced to take on more visible roles to prevent the defeat of the self-proclaimed republics. All the while, Moscow continued to deny Russian military presence in eastern Ukraine, while orchestrating an unrelenting media campaign to reinforce the narrative that the Russian-speaking population needed to be rescued from right-wing fascist extremists and chaos.

In September 2014, talks to halt the fighting in Donbass were held in Minsk, Belarus, under the auspices of the Organization for Security and Co-operation in Europe (OSCE). Representatives from the Ukraine, the Russian Federation, the Donetsk People's Republic, and the Luhansk People's Republic signed a cease-fire protocol known as Minsk I. It failed.

In February 2015, a second cease-fire agreement known as Minsk II was negotiated under OSCE auspices, though it remains imperfectly observed. Ukraine is unable to control its border with Russia, and Russia continues to resupply the separatists. Some experts predicted further escalation of tensions in the coming

months as a prelude to Russia's renewed push to create a land bridge to Crimea. Others believed that Russia does not have the wherewithal to expand the conflict zone substantially but will continue engaging in low-intensity conflict in the Donbass region.

Having made multiple trips to the Ukrainian front line recently, an expert shared the following observations about Russia's ambiguous warfare:

- Forces operate unmanned aerial vehicles and remotely pilot vehicles proficiently throughout the battlespace to gather operational intelligence and lock-on tactical targets, achieving approximately 10–15 minutes of separation between drone reconnaissance and strike missions.
- Separatists use horrific violence extensively to cow populations. Russian separatists not only abduct torture, assassinate, kill en masse, rape, and execute prisoners, they also record their activities and post the videos on the Internet.
- Field units resupply under the guise of humanitarian convoys; a direct, observable correlation exists between these convoys and separatist activities.
- Mechanized infantry conscripts do not fight as well as such contract units as the Spetsnaz, and conscript units suffer disproportionate casualties. Ground maneuver units employ a combination of contract and irregular forces.
- T-90 main battle tanks, protected by reactive armor, remain central to high-intensity combat. Deep armored raids are prevalent on the dispersed battlefield, and the T-90's reactive armor deters most single-warhead infantry-fired antitank weapons used by NATO forces.
- Body armor and body armor piercing ammunition overwhelm normal infantry, especially when delivered with night vision and snipers.
- Artillery and multiple-rocket launchers propel advanced munitions, which caused 85 percent of all casualties in Ukraine and reduced battalion-size units to combat ineffectiveness in a single strike. These weapons become more effective when used in combination with remotely piloted vehicles' target acquisition capabilities.
- Light infantry fighting vehicles succumb on the modern high-intensity battlefield without tank-equivalent protection.
- Air defense components densely overlap to keep Ukrainian Air Force close air support and attack helicopters, which lack sophisticated electronic countermeasures and air defense suppression capabilities, out of the battlespace.
- Armies lack digital radios and depend on national communications networks that are vulnerable to jamming, interception, and real-time targeting.

Five Lessons on Russian Aggression from Crimea and Eastern Ukraine

The assembled experts agreed that five lessons could be learned from Russia's activities in Eastern Ukraine and Crimea:

1. Russia's ambiguous warfare strategy requires fertile soil. Russian-sponsored operations in neighboring lands have been more successful with support from large ethnic Russian populations and have fallen short in areas where those conditions do not exist.
2. Moscow's aggression strategy arises from plans, not impulses. With operations in Ukraine planned and prepared well in advance, Moscow may have similar plans for other former Soviet states.
3. Russia's residual fear of NATO means the government avoids a blatant Article V trigger.[11] Ambiguous warfare stems from this weakness, but Russia's lack of traditional state power should not be equated to a lack of serious threat.
4. A nation-states' national defense depends on credible, integrated military and security forces. Ukraine has underfunded its military since the end of the Cold War, failed to modernize its forces, and constantly hobbled its own security efforts by tolerating corruption. Additionally, steps taken to eliminate conscription negatively impacted military morale and effectiveness. Countries with aggressive neighbors should heed this lesson. Furthermore, potential target states should foster collaboration, cooperation, and connectivity among not only their own military and security forces, but also allied forces.
5. These nation-states' political stability necessitates the integration of Russian descendants and immigrants into the national identity. Otherwise, dissention develops among the pro-Russian population that creates an entry point for Moscow to influence the internal affairs of neighboring states.

Russia's Next Moves

Russia aspires to replace the current Western-dominated world order with one in which great powers divide the world into internationally recognized spheres of influence. Seizing pieces of Ukraine will probably not be enough to achieve this goal. In the near term, however, the experts assembled agreed that Russia is likely to shift its aggression toward the Baltic States and Black Sea region.

The Baltic States

The three small Baltic seaside states of Estonia, Latvia, and Lithuania were part of the former Soviet Union and are home to sizable Russian-speaking popula-

tions. With their standing armed forces at about 5,000–10,000 troops each, the Baltic States certainly perceive themselves to be vulnerable despite their membership in NATO. Should Russian aggression occur against the Baltics, the offensive would likely take the form of ambiguous, destabilizing operations to avoid triggering NATO's Article V. This strategy sows doubt in the minds of the populations of the Baltic States about Western resolve to defend them and contributes to Moscow's goal of undermining the NATO Alliance.

When the Baltic republics joined NATO in 2004, they were encouraged to develop niche military specialties rather than worry about territorial defense, which the international community thought unnecessary. Each nation's government is addressing this mistake, but finding a solution will take time. The national armed forces of Lithuania meanwhile have no current mandate to intervene in internal affairs, while the police and the ministry of interior of the Republic of Lithuania share responsibility for domestic security and would be the first to respond to an influx of pro-Russian actors similar to the Crimean annexation. Lithuania's efforts to develop a more comprehensive defense plan involve coordinating all national bodies of executive power. A January 2015 pamphlet written by the Lithuanian Ministry of Defense titled *How to Act in Extreme Situations or Instances of War* even instructed Lithuanians on surviving foreign occupation and organizing nonviolent resistance.

Black Sea Region

Russia's seizure of Crimea and its continuance of military operations in eastern Ukraine changed the strategic balance in the Black Sea region. With Moscow's military presence no longer constrained by former legal agreements with Ukraine, Russia can fully exploit Crimea and its former Ukrainian air bases, using both as a platform to project power. This base access enabled the Ministry of Defense of the Russian Federation to deploy conventional and nuclear capabilities of Tupolev TU-22M3 Backfire-C medium-range bombers and Iskander-M (9M72) short-range ballistic missile systems to the peninsula by 2016. An ambitious modernization program underway for the Russian Black Sea Fleet in Sevastopol will add six new frigates, six new submarines, several smaller naval vessels, and possibly a Mistral-class amphibious assault ship. The fleet and other military units enhance Crimean antiship and antiaircraft capabilities. Russia's air defense systems in Crimea reach nearly half of the Black Sea while surface attack systems reach almost all of the Black Sea area. These military systems create a strong line of defense for the Russian homeland.

Historically, a Russian military build-up of this magnitude on the northern shore of the Black Sea would be of great concern to Turkey. The prospect of Russian–Turkish energy collaboration, however, may prove a critical factor toward mitigating Turkish concerns. Vladimir Putin, the current Russian president,

recently announced that, instead of completing the South Stream pipeline for Russian gas under the Black Sea to Bulgaria, construction will instead link the pipeline with existing Turkish systems. In contrast, Russian companies are investing in shipping companies and port facilities on the Turkish Black Sea coast, which are also useful for gathering intelligence and serving as entry points for Russian forces if necessary.

Seeking reassurance, Romania and Bulgaria (NATO members) and Moldova and Georgia (Partnership for Peace members) look to NATO and the European Union (EU) for security support because they are also targeted by active Russian influence operations.[12] Romania's foreign minister, Titus Corlăţean, openly expressed concern over Russian pursuits in the region.[13] Bulgaria depends heavily on Russian energy supplies and military equipment maintenance and was subject to intense Russian pressure to go forward with its long-planned role as the entry point for the South Stream pipeline. But when the EU demanded Bulgaria suspend construction on the pipeline while it investigated the way contracts were awarded and then froze political talks between the EU and Russia over the crisis in Ukraine, Russia announced that the South Stream would not be built.[14] Moscow hobbles Moldova and Ukraine by controlling the pro-Russian separatist enclave of Transnistria and trammels Georgia by formally controlling the foreign and security affairs of Abkhazia and South Ossetia, located within Georgia's internationally recognized national borders.[15] Transnistria, Abkhazia, and South Ossetia are also focal points for Russia-linked organized crime in the region in the regard that local gangsters meld with Russian-backed forces to metastasize organized crime in eastern Ukraine. This social and political evolution suggests that we can anticipate further strengthening and utilization of criminal networks around the Black Sea littoral region.

The Future of Ambiguous Warfare: Implications for the U.S. Marine Corps

Beyond understanding and studying the Gerasimov Doctrine as it has been applied to ambiguous warfare in Crimea and Ukraine, the Marine Corps must be able to view the strategy more conceptually. Just as the experts left the discussion with more questions than answers, Marines should extend their learning to consider such questions as:

- How did the Russians arrive at and apply this doctrine?
- Where has it been successful and where has it failed?
- What are the offensive lessons from its application?
- What are the adversarial lessons from Russia's actions?
- Can ambiguous warfare be applied in other theaters?
- How might other potential adversaries adapt this doctrine?

Return to High-Intensity Conflict

While the ongoing conflict in eastern Ukraine has shown that ambiguous warfare can be highly kinetic and extremely intense, the assembled experts noted that battalion-size forces have been rendered combat ineffective in a single wave of artillery strikes. Discussion participants considered the following implications:

- What kind of expeditionary crisis response force does the Marine Corps need to be successful in this environment?
- What does combined arms and maneuver warfare look like in this environment, particularly when U.S. forces will have lost much of their technological edge, along with air and information superiority?
- Can a modern Marine Corps infantry survive on this kind of battlefield? What impact will sustained high casualty rates have on how we fight, especially given political sensitivities?
- Could the armored vehicles being used and developed by the Corps survive on the modern battlefield?
- Does the Marine Corps have a partner in this kind of fight? How will Marines integrate with those allies and other Joint forces (e.g., special operations forces) to operate on an ambiguous battlefield?

Fighting in the Information Environment

Moscow has displayed its ability to launch covert and overt information operations on a mass scale to global, regional, and local audiences. It has also shown the ability to rapidly spread carefully crafted lies and disinformation to generate discord at local and international levels. Marines must begin framing Military Information Support Operations by answering how the Corps will

- counter hostile messaging in an ambiguous warfare theater;
- transition countermessaging efforts from early in the enemy's campaign of street protests, agitation, and subversion to the later campaign of open warfare; and
- overcome political and strategic decisions that limit and constrict the use of Military Information Support Operations on the battlefield.

Political and Economic Subversion

Because the initial phases of ambiguous warfare are often hard to detect, experts agreed that nation-states might maintain a persistent presence in at-risk countries as one way of sensing the application of Gerasimov's concepts. With that in mind, the Marine Corps must consider

- how to work with allied and partner nations to counter political and economic subversion in at-risk countries;
- what partnerships the Marine Corps and U.S. military can build with allied military, security, intelligence, or policing institutions in a stable, preconflict environment to inhibit ambiguous conflict;
- which foundations of cultural knowledge are most beneficial during each stage of ambiguous warfare; and
- if additional education and training on building and sustaining relationships with local actors would be beneficial.

Official versus Nonofficial Armed Forces

The complicated network of ambiguous actors Russia employed in Crimea and Ukraine intertwined irregular and proxy forces, special forces, militias, criminal syndicates, and unidentified regular military forces. These relationships necessitate an examination of how future adversaries will challenge and exploit U.S. rules of engagement by incorporating nonofficial and official forces.

Insights for Strategic Planning

Participants in this discussion clearly recognized the importance of understanding Russia's employment of ambiguous warfare in Crimea and Ukraine as well as what the strategy might mean for future Marine Corps force structure, capabilities, operations, and tactics. Russia's use of population shaping measures before the hostilities phase included leveraging Russian-speaking populations in target countries. A mélange of ambiguous actors, including special forces, militias, and criminals; resupply missions disguised as humanitarian assistance convoys; and deliberate disinformation and misinformation about events on the ground furnished particularly effective components of Russia's ambiguous warfare strategy. Participants also pointed to how Russia's unmanned aerial vehicles provided near real-time targeting information for artillery strikes. In addition, reactive armor, horrific violence, and advanced munitions were particularly effective tactics on the ground to intimidate and subdue local populations as well as counter Ukrainian national defense forces. Thinking more broadly, experts considered how these elements of Russia's strategy and tactics could be generalized to other regions of the world and be employed by potential U.S. adversaries, such as China and Iran.

The implications of Russia's ambiguous approach are mostly at the Marine Corps' strategic level. At the tactical level, the actions of Russia's panoply of forces are no less ambiguous than other forces Marines have faced during the insurgencies in Iraq and Afghanistan. As such, panel participants felt that the basic principles of Marine Corps warfighting remain valid in this kind of environment. Moreover, the situation in Ukraine—while ambiguous in attribution—still

amounts to state-sponsored warfare with a high intensity battlespace that looks significantly different from Iraq or Afghanistan. Success in this environment demands Marines consider how to apply their warfighting principles on a battlefield that may include the instantaneous loss of air, fire, and information superiority; rapid fluctuations between highly lethal, low- and high-intensity actions; significant increases in casualty rates; interspersed fighting among populations familiar with extreme violence; and unlimited adversary warfare in the information space. Perhaps the best way for the Marine Corps to prepare for the future of ambiguous warfare is to answer this question: if the Corps gets the call to fight, how will it overcome the loss of all advantages?

Notes

This article was taken in part from a CNA report published in 2015 titled *Russia's "Ambiguous Warfare" and Implications for the U.S. Marine Corps,* coauthored by Mary Ellen Connell and Ryan Evans. It summarizes a discussion among experienced regional specialists, senior military officers, and internationally renowned security experts that was coordinated by CNA on 25 February 2015, which followed the Chatham House Rule of nonattribution to encourage a candid exchange of ideas between participants. Experts did not quote official sources during the meeting; however, supplemental information has been added to expand readers' purviews. For more on Chatham House Rule, see Royal Institute of International Affairs, "Chatham House Rule," https://www.chathamhouse.org/about/chatham-house-rule.

1. Russia amalgamates forces that cannot be accurately categorized into traditional units that have become known colloquially as "little green men." See Anton Shekhovtsov, "Who Is Afraid of the 'Little Green Men'?," *Intersection Project*, 21 September 2015, http://intersection-project.eu/article/security/who-afraid-little-green-men.
2. Russia began staging logistical support for military operations in the Donbass region of eastern Ukraine at least as early as December 2014. See James Rupert, "Thousands of Russian Troops in Airport Push," *Newsweek*, 23 January 2015, http://www.newsweek.com/thousands-russian-troops-airport-push-301608; and Gianluca Mezzofiore, "Igor Strelkov: I Started War in Eastern Ukraine," *International Business Times*, 21 November 2014, http://www.ibtimes.co.uk/igor-strelkov-i-started-war-eastern-ukraine-1475982.
3. For more on the distinction between nonlinear and hybrid warfare, see Roger McDermott, "Myth and Reality—A Net Assessment of Russia's 'Hybrid Warfare' Strategy since the Start of 2014 (Part One)," *Eurasia Daily Monitor* 11, no. 184 (17 October 2014), http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42966&no_cache=1#.VjufITThjNJ.
4. Valery Gerasimov, "The Value of Science in Prediction," *Voenno-promyshlennyi kur'er* (*Military-Industrial Courier*), 27 February 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.
5. As quoted in Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (blog), 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.
6. For more on miskirovka, see Charles L. Smith, "Soviet Maskirovko," *Air Power Journal* (Spring 1988), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj88/spr88/smith.html; and Paul Huard, "'Maskirovka' Is Russian Secret War: Sneaky Tactics Are an Old Russian Tradition," *War is Boring* (blog), 26 August 2014, https://medium.com/war-is-boring/maskirovka-is-russian-secret-war-7d6a304d5fb6.
7. Escalation dominance refers to controlling conflict tempo. See Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Frederick A. Praeger, 1965).
8. For more on special operations forces' tiers, see Nick Irving, "How Would Our SOF

Perform in North Korea?," *Special Operations Forces Situation Report* (blog), 12 April 2013, http://sofrep.com/19396/how-would-our-sof-perform-in-north-korea/.

9. Roger McDermott, "Myth and Reality—A Net Assessment of Russia's 'Hybrid Warfare' Strategy since the Start of 2014 (Part Two)," *Eurasia Daily Monitor* 11, no. 185 (October 2014), http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=42972&cHash=a0aafae8f09b44fb11874373984c8b87#.VknXGoSof8s.
10. For one example, see Andrew Roth and Andrew Higgins, "Russian Convoy Draws Stern Warning from Ukraine and Stops Short of Border," *New York Times*, 14 August 2014, http://www.nytimes.com/2014/08/15/world/europe/russian-convoy.html?_r=1.
11. Article V of the Washington Treaty signed in 1949 establishes that NATO will view an attack on one NATO nation-state as an attack on all members. While NATO nations may come to the defense of other members, the NATO Security Council strives for peace. See NATO, *The North Atlantic Treaty* (Washington, DC: NATO, 1949), http://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf; and "NATO and the Scourge of Terrorism: What Is Article 5?," 18 February 2005, http://www.nato.int/terrorism/five.htm.
12. NATO's Partnership for Peace program allows nation-states to build cooperative relationships between individual NATO allies as well as the collective organization. See NATO, "The Partnership for Peace Programme," 31 March 2014, http://www.nato.int/cps/en/natolive/topics_50349.htm.
13. Titus Corlăţean, interview by Lally Weymouth, 30 April 2014, *Washington Post Opinions*, https://www.washingtonpost.com/opinions/the-russian-threat-is-a-reality/2014/04/30/ac19c2d0-cffb-11e3-937f-d3026234b51c_story.html.
14. Tim Boersma, "The Cancellation of South Stream is a Pyrrhic Victory, At Best," *Up Front* (blog), Brookings Institution, 18 December 2014, http://www.brookings.edu/blogs/up-front/posts/2014/12/18-south-stream-pipeline-boersma
15. A narrow strip of land bound between the Dniester River and the Ukrainian border, Transnistria initially declared its independence from Moldova in 1990, but has never been recognized by the international community. A 2006 referendum brought the issue to bear again, with the additional intention to join Russia.

The Dragon's Pearls
China's Road to Hegemony in the Indian Ocean

Captain David L. O. Hayward, Australian AR (Ret)

Abstract. In this article, the author argues that China is moving toward hegemony in the Indian Ocean Region to secure its ability to obtain the gas and oil supplies it needs for commercial development and possibly for national security and military purposes. He argues further that the China–Pakistan Economic Corridor projects and ideas, such as the One Belt, One Road and Maritime Silk Road initiatives, among others, are benign sounding ways to obscure China's more complex desires, previously referred to as a String of Pearls by Department of Defense analysts.

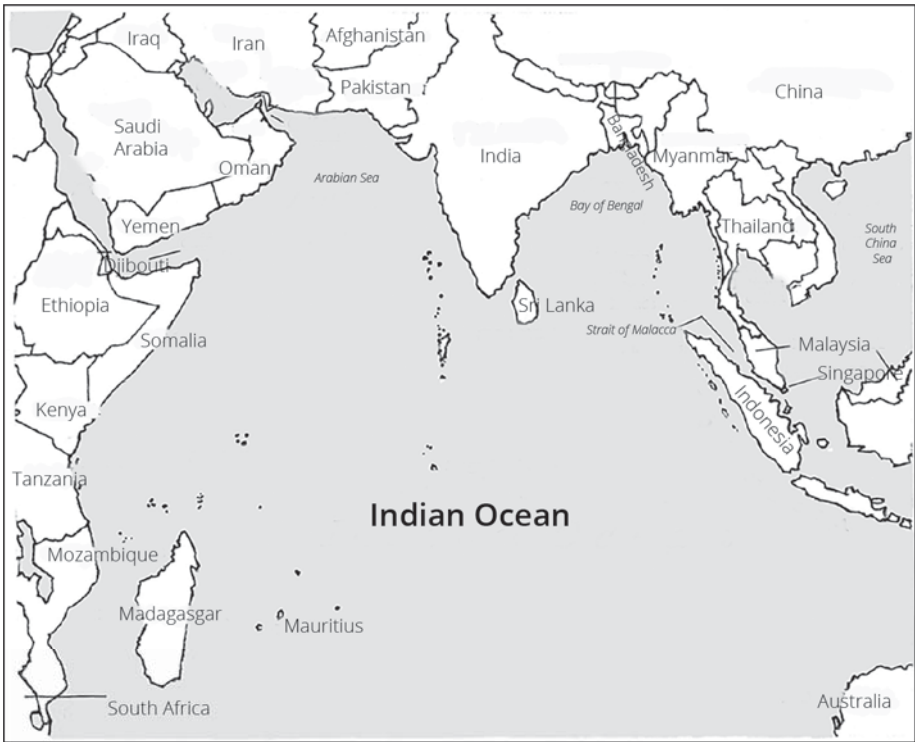
Keywords: China, *waishi,* maritime strategy, String of Pearls, Maritime Silk Road, China–Pakistan Economic Corridor, foreign direct investment, logistics, supply chain, oil, crude oil, gas, fossil fuel reserves, consumer market, global economy, Chinese shipping lane, Chinese port, Indian Ocean Region, China's Near Seas, People's Republic of China, People's Liberation Army Navy, Association of Southeast Asian Nations, Strait of Malacca, Malacca dilemma

This article focuses attention on the northern reaches of the Indian Ocean Region (IOR). This ocean constitutes the third largest body of water in the world (map 1). The countries' littorals to selected reaches discussed or briefly mentioned, geographically traversing from west to east, include Djibouti (Gulf of Aden and Red Sea); Pakistan (Arabian Sea); India and Sri Lanka

Capt David L. O. Hayward, Australian Army Reserve (Ret), is a freelance defense analyst. His defense papers have been posted to 16 websites worldwide. Hayward is an associate at Future Directions International (FDI), a member of the Royal United Service Institute Queensland, and an intern at the Intelligence Community in Washington, DC.

MCU Journal vol. 7, no. 1
Spring 2016
www.mcu.usmc.mil/mcu_press
DOI:10.21140/mcuj.2016070103

Map 1. Indian Ocean Region



Map courtesy of Future Directions International, adapted by MCUP.

(Indian Ocean); Bangladesh, Myanmar, and Thailand (Bay of Bengal); Malaysia (Strait of Malacca); and Singapore and Australia (Timor Sea). For multiple and complex reasons summarized below, China places immense geopolitical, strategic, logistical, economic, and military value on the IOR. This article supports the argument that China intends to achieve maritime hegemony in both the IOR and its declared Near Seas to ensure sustainability of its oil and gas shipments, raw materials, and mercantile trade.[1]

The Indian Ocean is the main conduit for China's seaborne trade and mercantile traffic representing approximately 60 percent volume of all Chinese global imports including a large percentage of oil and gas shipments. It provides essential transit routes for vital strategic hydrocarbons and raw materials largely sourced in the Middle East (Arabian Gulf), Africa (ports on the East Coast), and Australia (ports in Queensland and Western Australia). Thus, the Indian Ocean, with its indispensable sea lines of communication (SLOCs), is key to China's economic health and for sustainability of its gross domestic product (GDP) and other indicative economic indices, including the provisions for the wellbeing and standard of living for its people. China's GDP was estimated at $9.49 trillion (2013), almost six times that of India.[2] China's GDP represented 16.71 percent of the world's economy.[3]

In addition to the economic importance of the Indian Ocean, China also looked to the region for military and national security purposes. The People's Liberation Army Navy (PLAN) could not fully extend a comprehensive defensive military "umbrella" over its vulnerable long distance SLOCs in the IOR. Specifically, PLAN was acutely concerned that the Strait of Malacca bottleneck, guarded and monitored by the Singapore logistic hub and by deployed elements of the Indian Navy and the U.S. Fifth and Seventh Fleets, evinced an ever-present threat to its freedom of navigation through the strait. China was worried about the tangential threats posed by piracy in the IOR (i.e., in the Strait of Malacca and elsewhere). Therefore, PLAN deployed naval assets on patrol in the Arabian Sea to negate Somali piracy.

PLAN was equally concerned that the Strait of Hormuz bottleneck constituted a threat to its oil and gas imports, being open to interdiction by Western navies—including British and French naval assets, the U.S. Fifth Fleet headquartered in Bahrain, and the Islamic Republic of Iran Navy. Although the Iranian Navy was mostly limited as a green-water navy (apart from *Kilo*-class submarines), its multiple offshore patrol vessels were antiship ballistic missile capable.[4] In the past, Iran had threatened to close the Strait of Hormuz and continued to obstruct U.S. naval patrols in the Arabian Gulf. For instance, tensions were rekindled in the gulf with the arrest and detainment of 10 U.S. sailors by the Iranian Revolutionary Guard Corps (IRGC) in January 2016. The sailors were imprisoned on Farsi Island (a mid-gulf island outpost) and released the next day.[5] A January website article stated that "Iran released the two U.S. Navy vessels and their crew members after the IRGC determined that they had breached Iranian territorial waters 'unintentionally' on January 12."[6] When questioned, "Maj. Gen. Hassan Firouzabadi said the detainment and release of the two U.S. Navy vessels 'demonstrated the awareness and precision of the Iranian armed forces regarding American movements in the region. It taught them how vulnerable they are against the Islamic Republic's mighty forces.' "[7] In the same vein, but of lesser concern was the Bab el-Mandab Strait bottleneck, which had smaller trade volumes (estimated at 8 percent), but led China to consider constructing its first overseas military base at nearby Djibouti. Overall, these issues meant that Chinese officials feared incursions that would lead to a lack of control over its transportation routes and access to resources. They stated publically that powerful Western navies could interdict or blockade oil and gas supplies, raw materials, and essential bulk commodity shipments to its mainland ports. For these reasons, China's leaders believed in the long term that, as a country, China must take stringent measures to exercise greater control and dominance of the IOR to safeguard its economic and national security interests.

Consequently, China was taking all possible measures to overcome its logistical supply chain nightmare. Key considerations included infrastructure develop-

ments in countries littoral to the IOR; creation of the ambitious China–Pakistan Economic Corridor (CPEC) as an integral component of China's One Belt, One Road (OBOR) strategic initiative; continuing strategic investments in host nations; and long-term adoption of the so-called "String of Pearls" (SOP) maritime stratagem as perceived by the U.S. government for the past decade. PLAN clearly demonstrated the urgency of these measures by improving its blue-water navy capability, extending its airfields, deploying its military assets, and by constructing new military bases astride SLOCs in the IOR and South China Sea (map 2).

From China's point of view, all these measures were transparently stated as purely defensive in nature. President Xi Jinping consistently stated an important denial that the People's Republic of China (PRC) would ever seek hegemony in the IOR. From time to time, Beijing did issue blanket denials that it was seeking regional hegemony. Such denials became commonplace in past and present Chinese diplomatic discourse. Former Chairman Mao Zedong (1949–59) frequently issued similar denials. These denials were and are intended to mask China's hegemonic ambitions. For example, in a speech on 3 September 2015, President Xi vowed that "China will never seek hegemony or expansion," but China's actions have belied these statements.[8] Disinformation has been a part of Chinese statecraft for millennia. As early as the fifth century BC, the Chinese strategist Sun Tzu advised, "When seeking power, make it appear that you are not doing so," and it seemed Chinese leaders continued this tradition into the present.[9]

Thus, many Western nations remained largely suspicious of China's true defensive or offensive intentions. While it was difficult to navigate the changing geopolitical stances, the following influential nations had at some point expressed concern about China's activities, including the United States, India, Japan, and various North Atlantic Treaty Organization (NATO) powers. Moreover, officials from states considered smaller world players—such as Oman and some of the Association of Southeast Asian Nations (ASEAN) countries, especially Taiwan, South Korea, Australia, and New Zealand—exhibited increasing geopolitical resistance to what was seen as Chinese military expansion and a desire for maritime hegemony in both China's declared Near Seas and the IOR. Of these nations, India was a major actor in the IOR, and its government, led by Prime Minister Shri Narendra Modi, was mistrustful of Chinese intentions. India had limited influence over China's relationships with Pakistan, Afghanistan, Sri Lanka, and Myanmar. International Studies scholar Auriol Weigold believed India was strategically embraced and encircled by China, which created concerns.[10]

Again, the escalating Sino-Indian strategic maritime competition had been closely examined by FDI Senior Analyst Lindsay Hughes and demonstrated that policy makers should keep an eye on the relationship between China and India as it plays out in the IOR.[11] Hughes stated in his paper:

Map 2. South China Sea

Map courtesy of NordNordWest, adapted by MCUP.

> To protect their growing economies, China and India have scrutinised their sea-borne trade routes by enhancing their naval prowess, thus simultaneously enhancing their sea power. However, China's and India's enhancement of their respective navies causes each other concern, making each suspicious of the other's intention. Thus, they further strengthen their navies, leading to a cycle of enhanced naval power and growing suspicion.[12]

Hughes went on to claim that the desire to extend influence was an outcome of economic growth that every developing power endured. He contended that developing states seek to defend their trade routes, especially the maritime trade routes that form the bulk of their trade, because it was this very trade that

sustained their economic and, therefore, their overall growth. He asserted the only way these states could protect their maritime trade routes was to develop their naval prowess. This development, however, caused other states to become suspicious about the reasons for the original state's naval growth, leading them, in turn, to develop their own navies. From an economic perspective, therefore, the desire to extend a state's influence was motivated in the main by a desire to further increase the state's trade and commerce and its market share as demonstrated by China. As his paper demonstrated, however, trade and commerce did not constitute the ultimate motivator for extending China's influence into the Middle East and beyond it.

From a String of Pearls to Maritime Roads

The SOP maritime concept was first mooted in 2005 in a classified report submitted to the Pentagon by the consulting firm Booz Allen Hamilton, a Washington, DC, area think tank. In the past 10 years, there had been many skeptics unconvinced the concept was or is still viable, but new evidence and interpretations lend credence to the idea. The basic premise was that China will try to expand its naval presence by building civilian maritime infrastructure along the Indian Ocean periphery. The concept also refered to the network of Chinese military and commercial facilities and relationships along its SLOCs, which extended from the Port Sudan to the Chinese mainland. Each port or base became one of the "pearls" extending a connected set of posts "strung" through the IOR from China. The U.S. Department of Defense accepted the SOP concept as a means to understand China's activities. In June 2014, Virginia Marantidou revisited the idea in a Center for Strategic and International Studies (CSIS) study and came to the conclusion that "little evidence supports Chinese naval bases along the Indian Ocean littoral, particularly as that specific arrangement may not be beneficial to China. However, these same locations could serve as useful logistics support for the Chinese Navy, meeting its need to support a blue-water navy with less political cost."[13] Thus, it was important to use this concept without strictly focusing on military activities and to consider such alternative criteria as geopolitics, logistics, economics, and protected commercial trade to analyze China's diverse and seemingly unrelated activities in a larger, possibly more dangerous context.

The PRC, in an effort to thwart Western interpretation of the military implications of the SOP concept, introduced three new initiatives with the emphasis on developing trade corridors for economic and commercial purposes. To this end, through the guise of the Chinese Academy of Social Sciences and its 2013 Blue Book called *Development Report in the Indian Ocean*, the Chinese emphasized their economic interests.[14] The Blue Book said that China has no maritime, read "military," strategy for the Indian Ocean. President Xi initiated the maritime silk road (MSR) concept later in October 2013. He introduced this idea to reinforce

the message that China sought only economic objectives in the IOR and subsequently redefined China's MSR foreign policy with another, more pressing, wider initiative called OBOR.

"One Belt, One Road" Chinese Initiative

President Xi's newest and most ambitious strategic initiative—OBOR—encompassed the 2013 Silk Road Economic Belt and MSR subinitiatives and could plant the seeds for a new geopolitical era in the IOR.[15] The OBOR initiative was launched on 28 March 2015 by China's top economic planning agency, the National Development and Reform Commission located in Beijing. As CSIS analysts Scott Kennedy and David A. Parker explained, "President Xi has made this program a centerpiece of both his foreign policy and domestic economic strategy. Initially billed as a network of regional infrastructure projects, one of the latest releases indicates that the scope of the 'Belt and Road' initiative has continued to expand and will now include promotion of enhanced policy coordination across the Asian continent, financial integration, trade liberalization, and people-to-people connectivity."[16] While Chinese officials denied the military-centric interpretation of their policy as visualized in the SOP concept, these new initiatives demonstrated the truth of the SOP ideas along with the tradition of obfuscating its true intentions for regional hegemony.

Chinese Military Incursions in the IOR and Beyond

On first sight, all the nonmilitary commercial initiatives proposed by the PRC appeared "well intentioned, good and wholesome" in the interests of generating increased trade between Western Europe, the Middle East, Africa, Asia, and Australasia. The initiatives portrayed Chinese soft-power projection and diplomacy exercised to perfection. Militarily speaking, this was merely a convenient smokescreen for China's real intentions in the IOR and South China Sea. This was more than just supposition considering recent actions by the Chinese; PLAN announced that China's first overseas military base was to be located at Djibouti on the east coast of Africa.[17] Situated close to the Bab el-Mandeb and Strait of Hormuz, the new base has significant strategic importance because PLAN will be able to exert a degree of maritime control over the world's second and third greatest bottlenecks ranked by volume of seaborne trade. Theoretically, to consolidate its strategic presence in the longer term, the Chinese government could resurrect the proposed construction project known as the Bridge of the Horns, which would result in a bridge between the coasts of Djibouti and Yemen across the Bab el-Mandeb.[18]

Similar actions had taken or were taking place in other locations as well. In the South China Sea, PLAN had already reclaimed approximately 3,000 acres on which two military bases had been built in the Spratly Islands—one on Yongshu

Reef (Fiery Cross Reef) and the other on Mischief Reef. Civilian aircraft landed at one of these airports in January 2016.[19] Additionally, Gwadar, Pakistan, initially constructed as a commercial port at the IO end of the CPEC, may one day be used by PLAN for military purposes. Thus, PLAN had constructed, or intended to construct, at least four military bases seen as new pearls in the SOP concept. This description excluded five additional military airbases proposed in the Spratly Islands and new naval bases on mainland China and at Sanya on Hainan Island.[20] The precedent was thus set for China to build more overseas bases.

Local politics in areas where China had been in action also added possible pearls to China's national security necklace. In theory, a change of regime to a more pro-Chinese government in Malaysia could possibly see "favored" Strait of Malacca ports and infrastructure converted to become additional PLAN military outposts to complement Djibouti and Gwadar in the IOR. China had secured a 99-year lease through the state-owned Shandong Landbridge Group to operate Port of Darwin, Australia, which was peripheral to the IOR. PLAN deployed naval assets to the IOR and Australasian waters, including surface warships and submarines, and was building a second aircraft carrier. Moreover, China agreed to supply eight submarines under soft terms to Pakistan costing around $5 billion.[21] This would effectively double the size of the Pakistan Navy, thus posing a greater threat to India, which conveniently played into China's national security agenda. Mathieu Duchatel, head of the China and Global Security Project at the Stockholm International Peace Research Institute, was quoted as saying the following:

> With progress in its defence industry and strong government support for research and development, China has become a major player in weapons system. . . . The success in the deals with Pakistan will make it easier for China to secure markets in the countries in which China has strong defence relationship, as it means that the weapon systems are already tested. China was the third-largest arms exporter in 2012–13 but has since fallen to fifth place, behind Britain, France, Russia, and the United States, according to the institute's research. But it remains the main supplier for Pakistan, delivering half of the country's arms from 2010–14.[22]

By selling more arms to Pakistan, PLAN engendered a new arms race with India in the IOR particularly in terms of naval assets, base building, and missile deployments. China had invested close to $120 billion in selected IOR countries during 2005–16 and planned to invest a further $46 billion and $10 billion in Pakistan and Malaysia, respectively, by 2020. The total investment projected to 2020 was a mind boggling $176 billion. It appeared to be the largest Chinese

cross-border investment in global offshore assets anywhere in the world, *ceteris paribus*. Similar investments in Africa, the United States, and Western Europe may not eclipse the projected expenditure in the IOR. Financially speaking, given the magnitude of the above figures, China clearly demonstrated geopolitical, strategic, and economic IOR (and global) hegemonic intent, quite apart from expanding military intentions. In the short term, a world recession may slow down the rate of investment and ameliorate the levels of Chinese investment. Financial advisor George Soros asserted that China was leading the world into the third leg of the global financial crisis.[23]

China's Economic Interest in the IOR

China's Oil Thirst

China's need for crude oil had grown during the last decade, which explained its overt and covert activities in the IOR. As of 2011, China imported approximately 60 percent of its oil from the Middle East, up from 40 percent in 2005, and its demand continued to increase. At the time of this writing, China continued to buy large quantities of crude oil. Sinopec through its marketing company, Unipec, booked the Belgian TI-class *Europe*, an Ultra Large Crude Carrier (ULCC) with a storage capacity of 3.2 million barrels. The world's largest oil tanker by tonnage, the tanker was used for floating storage off Singapore.[24] In 2016, taking optimal advantage of lower world oil prices, China was likely to double its oil imports, overtaking America as the world's largest net oil importer.[25] China, fed by abundant Middle East, Central Asian, and Russian oil, would soon have the world's largest strategic reserve of oil, potentially surpassing that of the United States. The implication manifested itself: China would have military advantage in hydrocarbons reserve.

While China's economy was dependent on many imported resources, oil was a particularly strong motivator for the expansion of its defensive perimeter. The U.S. Energy Information Agency (EIA)

> forecasts that China's oil consumption will continue growing through 2016 at a moderate pace to approximately 11.3 million bbl/d [barrels per day]. China's oil consumption growth is forecast in IEO2014 [International Energy Outlook] to rise by about 2.6% annually through 2040, reaching 13.1 million bbl/d in 2020, 16.9 million bbl/d in 2030, and 20.0 million bbl/d in 2040. EIA forecasts that China's oil consumption will exceed that of the United States by 2034.[26]

In 2014, China imported 51 percent of its crude oil requirements from six Middle East countries, namely Saudi Arabia (16 percent), Oman (10 percent), Iraq

(9 percent), Iran (9 percent), United Arab Emirates (4 percent), and Kuwait (3 percent).[27] Currently, China was negotiating with Iran to increase its crude oil imports of Iranian oil now that the embargo has been lifted. Likewise, using the same extrapolation methodology and source, China imported 17 percent of its crude oil requirements from three African countries: Angola (13 percent), Congo (2 percent), and South Sudan (2 percent). These additional crude imports transited the IOR. China's oil imports from the Middle East were projected to grow to 54 percent of total oil imports by 2035.[28] It was likely that if China imports significant crude from Iran in the future, higher estimates may be obtained. Statistical variations in projections manifested depending on the sources and method of calculation. Moreover, it was anticipated that China may lead a world increase in demand for oil tankers of the Very Large Crude Carrier (VLCC) and ULCC varieties as its energy needs rose in the next decade. As of 2014, "China already owns 70 VLCCs out of a total global VLCC fleet of 633 units, or about 11% of the world's working super tankers," as analyst James Bourne indicated.[29] He added, "Chinese firms currently have about 27 new tankers on order at shipyards, or about one-third of the current global order book."[30] The VLCC and ULCC tankers would soon provide 80 percent of China's oil and 65 percent of India's, fuel desperately needed for the two countries' rapidly growing economies. Japan, South Korea, and ASEAN member nationstates were almost totally dependent on energy supplies shipped through the Indian Ocean.

Why China Needs More and More Oil

This section was not intended to reiterate the above discussion but to provide some explanation as to why China is buying so much oil and gas. The PRC's aggressive policy to buy crude oil and gas supplies and to invest in oil infrastructure development was so that it can compete in the global consumer market.[31] Chinese policymakers supported the production of consumer and manufactured goods on a massive scale for internal and external demand. China's 1.401 billion consumer market was the world's largest with much demand for Western goods and increased standard of living.[32] Economic expansion was paramount. As more Chinese citizens toured overseas countries and often experienced affluent living standards and conditions, tales of economic well-being in the West will filtered back to mainland China. Consequently, those in China who might consider themselves the "have-nots" would compare themselves to the "haves" in the West, which could lead to some interesting actions by the Chinese who want to catch up in terms of their standards of living. This would drive the emerging consumer economy. The above premise was derived from past general research work, interviews with Chinese migrants in Australia, and as a result of several recent visits to China.

An August 2009 report released by management consultants McKinsey &

Company titled *If You've Got It, Spend It: Unleashing the Chinese Consumer* outlined the challenges facing the Chinese government. The authors argued that China could again raise private consumption above 50 percent of GDP. If successful, this would "enrich the global economy with $1.9 trillion a year in net new consumption."[33] China's private domestic consumption in 2009 was estimated at 37 percent of GDP. Thus, China's economic expansion had placed it on a collision course with global competitors in the market for scarce resources, including critical oil and gas supplies. The PRC accounted for nearly 40 percent of the increase in global oil consumption between 2004 and 2007. In a short period, China evolved from a position as a net oil exporter in 1992 to the world's second largest net oil importer by May 2015. In 2016, China was likely to become the world's largest net oil importer.[34]

Beyond the internal demand, China wanted to continue exporting large volumes of consumer goods and services worldwide to retain its advantageous dominant position as the world's leading exporter.[35] Products exported included electronic equipment; machines, engines, and pumps; furniture, lighting, and signs; knitted, crocheted, and general clothing; medical and technical equipment; plastics; and miscellaneous goods.[36] Westerners now possessed a significant number of Chinese manufactured goods and the "Made in China" label was ubiquitous. China had penetrated every market in the West, including the emerging driver-economies of Brazil, India, and a resurgent Russia. The PRC wished to accelerate its growth as a part of a self-equilibrium economic model. Thus, China had a "unique symbiotic relationship" with much of the West, particularly with the United States, one of its largest markets. China's trade surplus in 2015 was projected by Australia New Zealand Bank analysts to attain a massive $600 billion, more than doubling 2008 figures.[37] Hence, it was clear that China would continue to import increasing amounts of oil to pursue its industrial growth, despite the difficulties faced in getting supplies to its ports.

Oil Supply Route to China

En route to China, oil tankers must take an indirect route through the Indian Ocean and South China Seas through islands and various straits. Stretching from the Arabian Gulf and the coast of East Africa on one side to the Malay Archipelago and the shores of Australia on the other, the vastness of the Indian Ocean consists of an area of more than 45 million square kilometers. The 30-odd nations that constitute the ocean's littoral region contained one-third of the world's population. This region was central to China policy even though it seemed so distant to Westerners. To better understand this perspective, Geoffrey Kemp inverted the world map in his *Limited Contingency Study* of 1977.[38] This was to clarify the proximity of Russian military bases to oil supply routes in the Indian Ocean and around the Cape of Good Hope. A South Korean propaganda video similar-

ly demonstrated and used an inverted map for strategic, military purposes.[39] Thus, it need not be a Eurocentric world. If China was positioned at the center of the world (azimuthal projection) and the world map was again inverted (i.e., south-up map), it was easy to see the world the way PLAN military strategists did, including how vital the Indian Ocean and China's Near Seas were to mainland China.

From their view, the vital sea lanes for the transport of crude oil provided an expeditious route for tankers on their way to China's ports. Upon exit from the Strait of Hormuz, the main oil supply route traversed through the Arabian Sea, rounds Dondra Head (Sri Lanka), crossed the Indian Ocean, entered the Strait of Malacca, bypassed Singapore, and entered the South China Sea and the disputed waters claimed by China as part of its "Sacred Territory."[40] The route then threaded its way past the Spratly Islands, Johnson Reef, Macclesfield Bank, and Paracel Islands to Zhanjiang (opposite Hainan Island) and Guangzhou (Canton) to Hong Kong, Xiamen, and Fuzhou; continued on through the Taiwan Strait to the East China Sea, calling at Ningbo, Hangzhou, and Shanghai; and then swung northward to the Yellow Sea, to ultimately deliver the crude oil to Qingdao, Dalian, and Tianjin.[41] The greatest geographical impediment to expedient oil supply to China was the Strait of Malacca. An estimated 50,000 cargo vessels transited the region each year. In fact, the EIA described it as a "world oil chokepoint" moving approximately 15 million barrels of oil through the strait each day despite the narrowness of the route.

Andrew S. Erickson and Gabriel B Collins claimed that "Chinese experts . . . believe that the United States can sever China's seaborne energy supplies at will and in a crisis might well choose to do so."[42] In particular, some of these experts expected that America "has the capability to cut off Chinese oil imports and could severely cripple China by blocking its energy supplies."[43] Pablo Bustelo had also identified Chinese concerns as to the ongoing viability of sustained oil supply to China, while President Xi had not publically announced any Chinese fears pertinent to the bottleneck Strait of Malacca.[44] If anything, he avoided the subject unlike his predecessor, former president Hu Jintao (2003–13), who declared in November 2003 that " 'certain major powers' were bent on controlling the strait, and called for the adoption of new strategies to mitigate the perceived vulnerability."[45] In his statement, Jintao implied that China faces a "Malacca dilemma"—the vulnerability to disruption of its oil supply lines from the Middle East and Africa. Antoine Bondaz asserted,

> As a rising power, China faces a "rise dilemma" (*juéqǐ kùnjìng*). According to power transition theory (and what has been termed the "Thucydides' trap"), rising powers like China elicit opposition from their [neighbors] as well as dominant powers like the United States, increasing tensions and the likelihood of war. Assuming

> that conflict between rising and dominant powers is not inevitable, China's dilemma is to avoid a direct political and military confrontation with the United States in which it would be the main loser and to prevent its neighbors from balancing its rise.[46]

Past and present Chinese foreign policy evidenced that China had always sought to protect its energy security using the following preemptive methodologies: (1) by desired domination of its Near Seas (including the energy rich SLOCs in the South and East China Seas); (2) by diversifying its sources of oil and gas on a global basis (thus avoiding some seaborne shipments); (3) by invoking elements of the SOP concept, MSR, OBOR, CPEC, Malacca Gateway and other strategic initiatives; (4) by constructing the world's largest mercantile marine; and (5) by building a protective blue-water navy and an air defense protective umbrella incorporating Air Defense Identification Zone declarations. It was thus given that President Xi had de facto endorsed the salient features of Chinese foreign policy earmarked above, which implied that he was circumventing the Malacca dilemma by all other means possible.

Although investments in new pipelines via the planned CPEC initiative—across Central Asia (Turkmenistan–Afghanistan–Pakistan–India Pipeline), across Myanmar, and from Russia and Central Asia—could collectively reduce China's dependence on the Strait of Malacca as a major supply route, oil/gas VLCC/ULCC tanker volume shipments remained far more cost-effective in terms of transport economics.[47] Research was merited, if not already undertaken by the oil majors, using linear programming software.[48] Comparison could be made between the unit tonnage oil/gas cost per shipment vessel by sea with the alternative cost for tonnage equivalent throughput by oil pipeline to a storage destination. For example, theoretically, how many pipelines would equate to one VLCC shipment, taking near equivalent long distances into consideration? New technical innovations in multiple pipeline technology and pumping stations had been instigated by Saudi Aramco in Saudi Arabia. It might not be possible, however, to adopt a valid model to prove the algorithmic mathematics are correct.

The fact that China was prepared to continue and plan for infrastructure investments in oil/gas pipelines, amounting to "open check book" billions of dollars despite the adverse transport economics outlined above, demonstrated that the Chinese Communist government was predominantly concerned about the bottleneck Strait of Malacca and the potential threat from interdiction by the Indian, American, and other Western navies, ipso facto.

Pearls on China's String

It now remains to give closer attention to the pearls and "fortresses" in the Indian Ocean. It was also prudent to discuss present and future deployments of Chinese

warships in the Gulf of Oman, Arabian Sea, Bay of Bengal, and the wider extent of the Indian Ocean. This article was primarily concerned with the Indian Ocean, but the SOP maritime concept also extended beyond this to the South China, East China, and Yellow Seas.[49]

Gwadar, Pakistan

The revitalized port of Gwadar was a mere 200 nautical miles from the mouth of the Arabian Gulf. Gwadar, in particular, was listed as an essential constituent of the original SOP concept pertaining to the IOR. In past years, Beijing had helped Pakistan to construct a massive deepwater port and potential naval base. Port improvements and dredging had been undertaken and were now largely completed. China had provided 80 percent of Gwadar port's $248 million initial development cost. More specifically, China provided $198 million of the development cost in the form of official development assistance, while the balance of $50 million was paid by the Pakistan government. It was reported on 22 January 2016 that Chinese and Pakistani officials had agreed to work on a master plan to turn Gwadar into a major economic hub.[50]

China–Pakistan Economic Corridor

Recent Chinese activity in Gwadar connected past attempts to future hopes for the region. China was also building an innovative and costly economic corridor connecting Gwadar to Kashi (Kashgar) in China's western Xinjiang Uyghur Autonomous Region "via roads, railways and pipelines to transport oil and gas. It would act as a bridge for China's planned MSR meant to link more than 20 countries as part of a trans-Eurasian project."[51] Gwadar would also provide economical access to the sea for cargo generated in the northern and southern parts of Pakistan and neighboring states, while Pakistan offered the shortest route to Central Asia via land. President Xi announced his commitment to the CPEC during his state visit to Pakistan in April 2015. It was a crucial component of the Chinese president's OBOR, sometimes called China's Marshall Plan. This had become an indispensable element of discussions about China's foreign policy and one of the Chinese president's most emblematic policy initiatives. CPEC only formed one component of the total OBOR concept that involved some 65 countries, 4.4 billion people, and a massive investment of at least $1.37 trillion spent during the next 10–15 years.[52] CPEC was a proposed land bridge between the maritime road linking the Chinese mainland to Southeast Asia, India, Africa, and Western Europe with the belt overland route linking China to central Asia, Russia, and Eastern Europe.[53]

CPEC, as with other OBOR components, was to be funded by three new financial institutions: the Silk Road Fund, Asian Infrastructure Investment Bank, and New Development Bank.[54] The preexisting, well-established, and rival Asia

Development Bank (ADB) estimated that Asia needed $8 trillion to fund infrastructure construction for the 10 years prior to 2020.[55] This estimate taken over a shorter timescale was eight times larger than that originally foreseen by President Xi in September 2013 when the OBOR initiative was first announced at Nazarbayev University in a state visit to Kazakhstan. The completion cost for the OBOR initiative will not be known until at least 2020.[56] In 2013, mainland China's outbound direct investment rose 14 percent to a record $123 billion. Former All Pakistan Shipping Association Chairman Aasim Siddiqui stated several times that "once developed, the proposed corridor would cut the conventional 19,000-mile Sino-Europe shipping route by thousands of miles. Rendering PCEC to be of 'immense importance' for the economy of Pakistan."[57]

China's development of SLOCs through Pakistan, then, was significant, and China would therefore cut 10,000 miles from the conventional Sino-Europe SLOC. Transport costs, including oil and gas shipments, for all forms of mercantile trade might well be reduced by more than 50 percent. As a part of this, Gwadar lies at the confluence of not just local offshore drilling pipelines, but also of the sea and land routes that would move oil to Central Asia, India, China, and Japan in the twenty-first century. It would become a new "Venice" for the oil trade: a modern replacement for the silk trade. Put succinctly, Pakistan wanted to become China's newest superhighway to Europe. And considering recent actions, China did too.[58]

The infrastructure development of Gwadar marked China's new strategic presence on the Indian Ocean. The Gwadar port, referred to by U.S. analysts as the "Chinese Gibraltar," represented an initial total of $1.87 billion in Chinese investment plus another estimated $46 billion for all phases in the years to come. In addition to the port and naval facilities, China had financed an airport planned to be Pakistan's largest and had plans to refurbish an oil refinery designed to produce 60,000 barrels per day from offshore drilling. A new Chinese-funded superhighway, built for mercantile purposes would connect Gwadar to Karachi. It was implicit in the plans that the new superhighway could also be used by the military for strategic purposes.

Despite the present euphoria, a qualifying statement was advanced by a highly placed Chinese official at a press gathering in Ürümqi, the provincial capital of the Xinjiang Uyghur Autonomous Region in western China. The unnamed official stated "that a study based on a 3,000 km direct rail link from Gwadar to Kashgar has been initiated despite a 'hostile environment and complicated geographical conditions'."[59] The chief minister of Khyber-Pakhtunkhawa, Pervez Khattak, told a similar gathering that "Gilgit-Baltistan, Khyber-Pakhtunkhawa, Punjab, Sindh and Balochistan are all being linked as part of the economic corridor."[60] The enormity of the Gwadar Project and associated CPEC raised acute concerns from India and Western nations.

Several Indian officials expressed reservations, including former Indian Army Lieutenant General Raj Kadyan and India's defense minister who stated that "Pakistan's decision to hand over strategic Gwadar port to China is a matter of 'serious concern' for India."[61] Kadyan was responding to a media query about handing over the Gwadar port in Pakistan and related Indian vulnerability. Strategically, Gwadar port would give China access to the Arabian Gulf and would provide for future development, such as a naval base. To counter this move, Indian leaders wanted to develop Iran's Chabahar port, a few miles away from Gwadar. The Chabahar port would open a route to Afghanistan while circumventing Pakistan. Thus, there was much evidence for the argument that the MSR and OBOR initiatives served as screens for China's hegemonic goals in the region.

Hambantota, Sri Lanka

Again, in Sri Lanka, Chinese aid and commercial investments were increased markedly while the government of President Mahinda Rajapaksa (2005–15) was in power. The $1.16 billion Chinese-funded Hambantota port development project near Dondra Head in the southern part of Sri Lanka would potentially set up a naval military base to rival that of the United Kingdom's Diego Garcia military base in the Chagos Archipelago islands, which was currently leased to the U.S. Navy. Hambantota was a strategically vital gateway for securing access to SLOCs in the Indian Ocean. The new port was only six nautical miles from major SLOCs between the Bay of Bengal and Arabian Sea.

When completed, Hambantota would be more than three times the size of Colombo Harbor, Sri Lanka. The port would be able to accommodate a new generation of megaships and was to include four terminals (12 berths), bunkering and refueling facilities, a liquefied natural gas refinery, aviation fuel storage facilities, and dry docks. The port would be able to handle VLCCs, ULCCs, smaller oil tankers, and mercantile shipping as a halfway respite stop on their way to China. Other Chinese-funded projects in Sri Lanka included new port infrastructure at Galle; the new international airport; the Norochcholai Lakvijaya Power Plant project ($855 million); the Colombo-Katunayake Expressway ($248 million); and the National Performing Arts Theatre ($21 million). In recent years, Chinese aid to Sri Lanka had grown fivefold.[62] In-depth research indicated there had been problems with some of these Chinese funded projects. The international airport proved to be a "white elephant," Norochcholai Lakvijaya Power Plant had been beset with shutdown failures, and the Galle new port infrastructure was not yet completed. There was abundant evidence of corruption within the previous, now deposed, Mahinda Rajapaksa regime.[63]

Saliya Senanayake, formerly of Chartered Institute of Logistics and Transport in London, was quoted as saying that

> India is about five to six years behind Sri Lanka when it comes to port infrastructure. The SLPA [Sri Lanka Ports Authority] is pouring millions of dollars into infrastructure around the island and says it is on course to increase container handling capacity by 1.6 million containers to 6.4 million by April [2014]. It hopes to have a container capacity of 10 million by 2020, while revenue is forecast to triple to one billion dollars by 2020.[64]

According to Priyath Wickrama, of the Sri Lanka Ports Authority, "The new port will boost the country's annual cargo handling capacity from 6 million containers to some 23 million."[65] It remains to be seen if Chinese investment in Sri Lanka would be sustained and if current Chinese funded development projects would be completed. If a complete blockage was applied, then Chinese warships would simply divert to Gwadar.[66] Notwithstanding, Hambantota had the potential to become an island fortress analogous to that of Hainan Island, guarding Chinese oil supply movements through the South China Sea. The implications of military positioning under the guise of economic growth could be seen in Sri Lanka, where the new president allowed Chinese submarines to dock in Colombo and possibly in Hambantota Port in the future. In the meantime, Sri Lankans were relying on Chinese investment for purportedly commercial reasons.[67]

Malacca Gateway Project

China announced it intends to invest $10 billion in the Malacca Gateway project situated near Melaka, Malaysia, with a total land area of 246 hectares. The project would consist of a deep-sea port and ocean park and was expected to be completed in 2025. The work was to be largely undertaken by KAJ Development Sdn Bhd in joint venture with other entities.[68] Malaysian Transport Minister Liow Tiong Lai pointed to this: "China is recognised for its top 10 seaports in the world and Malaysia can anticipate its very own top-notch seaport with the expertise and fiscal commitment from China in unveiling a high-value harbour here."[69] According to the article, Liow was on record for discussing the agreement between his federal government and China about the Chinese initiative to develop the project, including a deep-sea port and ocean park. Thus, Malaysia was implicitly and explicitly backing President Xi's OBOR vision.[70]

Chinese institutional investors, including state-owned corporations, were involved in the Malacca Gateway project. They included entrepreneurs from Guangdong Province and Qiagen Development Limited on mainland China. Dignitaries participating in research and planning for the project included Yue Jin Rate (Sanya City Development Corporation on Hainan Island), Huang Huikang (Qiagen Development), Zhu Xiaodan (Guangdong Governor), Datuk Wong (Hong Kong), and many others.[71] Chinese companies were participating in a number of other

infrastructure developments in the Strait of Malacca. One of these was at Kuala Kedah. The proposed Kedah Integrated Fishery Terminal was planned to become an international fisheries center, especially for tuna in Southeast Asia. This terminal would be a joint venture between Kedah state-based development company and a Chinese-based company to funnel MYR1 billion (Malaysian Ringgits) into the project. The planners were targeting one million tons annually of fish landings.[72]

The project above may just be the beginning since there were 21 Malaysian ports in the Strait of Malacca.[73] Among these, the MMC Corporation Berhad operated four ports that handled 22 million 20-foot equivalent units (TEUs) in 2014.[74] Tanjung Pelepas was the eighteenth largest port in the world by volume of TEU shipments.[75] It was not known how much Chinese investment had percolated into other Malaysian ports in the Strait of Malacca. Certainly the ports handling significant TEU tonnages were very much in the eyes of potential Chinese investors. While not the focus of this article, further research was merited. Infrastructure developments in the Strait of Malacca Strait were attracting global investors.

Political Instability in Malaysia

Chinese investment in Malaysia was a topic of global concern beyond Southeast Asia because Malaysia's unstable political situation could put the country in a position for a takeover, commercially if not politically.[76] Sol W. Sanders stated, "Southeast Asia's multi-ethnic player, Malaysia, with its carefully balanced Malay majority but dynamic Chinese and Indian minorities, is in crisis. A lack of resolution could not only jeopardize the country's 30 million people but destabilize the region, especially neighboring Singapore with its Malay minority within an overseas Chinese majority, Indonesia, and Thailand."[77] The veracity of this statement was apparent when considering the high level of governmental corruption at all bureaucratic levels within Malaysia. The growing financial and political scandals were adversely impacting Malaysia's police and legal systems. Sanders explained that "A full-fledged insurgency among the minority Malay-speaking population in southern Thailand has ties to Malaysian orthodox Muslims. Indonesian Islamic terrorists, with deep roots in some areas of the country going back to pre-independence, have attacked Western targets."[78]

Nonetheless, the bilateral relationship between China and Malaysia remained strong. In 1974, Malaysia became the first country in ASEAN to establish diplomatic relations with China, and since then, the two nations continued to work together. Both governments relied on a long diplomatic tradition and regarded the relationship as mutually beneficial and based on economic ties. In 2014, bilateral trade reached $106 billion, and for six years prior to that Malaysia had been China's largest trading partner in ASEAN. Leaders from the two countries pledged to try to increase trade volume to $160 billion by 2017.[79]

Recently, Malaysians echoed some concerns in the media about China's military activities in the South China Sea. In a speech delivered to a party congress in Kota Kinabalu, the capital of the Malaysian state of Sabah, Deputy Prime Minister Ahmad Zahid bin Hamidi took aim at Beijing's questionable historical claims in the South China Sea as well as its construction of facilities 3,218 kilometers from the Chinese mainland and just 155 kilometers from Sabah.[80] In spite of these misgivings, Prime Minister Najib Razak was still insistent on trying to preserve a good overall relationship with China. Clearly, Malaysia needed to court commercial investment, but while it did so, some Malaysians were watching, as others should, to determine what it will mean in the long run.

Chinese-Funded Developments Located Elsewhere in the IOR

In September 2014, China's President Xi secured Maldivian support for his purported MSR as he began a South Asian tour. In the newly signed accord, Maldivian President Abdulla Yameen Abdul Gayoom also secured Chinese support for a bridge project to connect central Malé Island and nearby Hulhulé Island on which the international airport is located.[81] Rajat Pandit, a *Times of India* journalist, asserted that "with China poised to establish a full-fledged embassy at Maldives, strategically located southwest of India astride major sea lanes in IOR, officials say Beijing has stepped up its 'lobbying' to bag a couple or more of crucial development projects in the 1,190-island archipelago."[82] The so-called MSR was a deliberate Chinese strategy to alleviate Indian and American fears by rebranding the SOP concept.[83] As author William Yale noted for readers of the *Diplomat,* China was promoting the idea of the MSR as a part of the Silk Road Economic Belt initiative and using the OBOR slogan to obscure its territorial designs. Yale stated it plainly: "The 21st Century Maritime Silk Road is multi-pronged: it is intended to serve diplomatic, economic, and strategic purposes."[84]

Defense analysts still perceived the MSR as a smokescreen to hide the inevitable infrastructure projects, designated economic zones, the Air Defense Identification Zone, and logistical system of linked pearls (i.e., fortified ports) already prevalent within the SOP concept. It was difficult to assess the value of Chinese investments in the Maldives in view of the rivalry between India and China, as well as a lack of informed sources. Moreover, China won a $500 million contract in September 2014 to upgrade and expand Malé International Airport.

More remotely in the mid-Indian Ocean in the Seychelles, China established trade links and investments as part of a clever sister-city agreement between Victoria (capital city) and Qingdao on mainland China. The Seychelles News Agency reported on the "trade and investment opportunities available between Seychelles and Qingdao, a major port city of China's eastern province of Shan-

dong, have been widely discussed between entrepreneurs from both countries."[85] The Chinese government wished to position the Seychelles as a trade hub to Africa consistent with its MSR initiatives. Even so, the military implications were self-evident. China had successfully set up useful sister-city agreements worldwide, including in Australasia, as just another means to project soft power. Chinese investments in the Seychelles, Madagascar, and Mauritius were estimated at $6.00 million (pledged), $29 million, and $1.15 billion, respectively.

China had also capitalized on a 1992 agreement with Myanmar for the construction of ports at the Small and Great Coco Islands (on the eastern side of the Bay of Bengal/Andaman Sea) in return for the modernization of Myanmar's navy. As Darshana M. Baruah noted, "Kyauckpyu is a small port town in Myanmar and possibly Beijing's answer to its 'Malacca Dilemma.' The Chinese presence in Myanmar and the Bay of Bengal is too close for comfort for policymakers in New Delhi. However, undeterred by Indian concerns, China has continued to invest in Myanmar, resulting in two gas and oil pipelines ferrying Chinese energy imports straight from the Indian Ocean without crossing the Strait of Malacca."[86] Thus, she continued, "the gas and oil pipelines help solve China's 'Malacca Dilemma,' increasing its energy security tremendously. While the pipelines have great economic benefits for Myanmar as well, the underlying strategic dimension of the project cannot be overstated."[87] Myanmar could be viewed as a stopover on China's MSR, or a pearl on its strand of hegemony.

In addition, Chinese firms had constructed or modernized ports at Sittwe, Kyauckpyu, and Mergui, and at Hainggyi Island. Some Western analysts claimed that the Chinese military also operated reconnaissance and electronic intelligence stations on several islands belonging to Myanmar, though both Indian and American intelligence officials said there was no evidence to support that claim. The eastern seaboards of Bangladesh and Myanmar (as far south as the Coco Islands) appeared to be covered militarily and subject to Chinese geopolitical intentions. It was not known to what extent military resources were involved or would be involved in these projects. Total Chinese investment in Myanmar was estimated at $6.06 billion from 2005 to 2015.

Chittagong, Bangladesh, also benefited from Chinese-funded projects. The regional head of the Bangladesh National Party, Amir Khasru Mahmud Chowdhury, believed that "the Chinese are developing a real strategy over the next 30 years."[88] In addition, Raisul Haq Bahar of the *Chittagong Daily Star* asserted that "China is supporting us through their big projects."[89] Investments included a new container terminal with five berths, a 950-meter, four-lane bridge, and subsidized loans for a water treatment facility, a private power plant, and a nearby international airport.[90] While these were substantial developments, they were certainly being played up for the benefit of China. For example, "China is building

a spectacular deep-sea harbor in the island of Sonadia for an estimated cost of $5 billion. There is also a tunnel under the Chittagong River, a China-Bangladesh highway via Burma (Myanmar), and the project of a new industrial park."[91]

To add to this, retired Indian Army Brigadier Arun Sahgal described China's investments as "calibrated inroads" into the Bay of Bengal.[92] China was examining the feasibility of constructing a $21 billion canal across the Kra Isthmus in Thailand.[93] This new canal would allow tankers and other commercial vessels to bypass the chokepoint Strait of Malacca. The canal project, if implemented, would give China port facilities, warehouses, military installations, and other infrastructure in Thailand capable of further enhancing Chinese influence in the Andaman Sea and the Gulf of Thailand.

The Chinese were looking at the IOR broadly, considering activities on any island or in any nation that may extend China's influence in the region. On the periphery of the IOR, China successfully made some inroads into Australia. The Shandong Landbridge Group was a Chinese holding company operating ports as well as storage and processing facilities in Australia's Northern Territory. Much to the displeasure of the U.S. government, the group secured a 99-year lease to operate the Port of Darwin.[94] A number of military analysts in the United States wondered about an eventual Chinese naval base in the Persian Gulf. As the *Iran Times* reported, "The frigate *Maanshan* and the supply ship *Qiandaohu* sailed through the Strait of Hormuz last week [2010] and docked at Abu Dhabi for an official visit to the United Arab Emirates. . . . There was speculation that China might be approaching the UAE for some kind of basing rights."[95] In 2014, Chinese and Iranian forces continued this trend by running joint naval exercises in the gulf. As Keith Johnson wrote from the "Observation Deck" of *Foreign Policy,* "The United States may not have to confront a Chinese carrier-strike group in the Persian Gulf just yet, but it still needs to prepare for cohabitation or collision—or both."[96]

The Chinese encirclement of the Indian Ocean using the SOP concept as a blueprint was yet to be fully realized and could be portentous for many decades to come as seen with President Xi's new initiatives. Military analysts in the West expressed concerns. The phrase "Power, One Pearl at a Time" had been coined and was understood by many as a tightening of the virtual necklace. Chinese naval strategy and military philosophy in the Indian Ocean context may be seen by some analysts as a virtuous regional hegemony, that was, a calculated bid to reach ultimate maritime supremacy in the future. This extreme viewpoint, however, could be refuted. For the reasons stated below, it would be impossible for China to apply hegemony in the IOR in the near future for there was far too much competition. The situation could easily change by 2030 or even earlier depending on the progress of infrastructure development and military expansion.

At the present time, at least, Chinese naval strategy largely comprised a de-

fensive mode to deter Western/allied attempts to interdict the supply of oil and vital strategic minerals via SLOCs to mainland China. But this could change especially if China decided to adopt an offensive mode beyond the present OBOR soft-power projected initiatives.

Chinese Investments in the Indian Ocean Littoral Nations

This article was not intended to provide accurate assessments of past or planned investments in all nations littoral to the Indian Ocean relative to the SOP concept. The following estimates for the period from 2005 to 2015 may be taken as a guide, however.[97] The investments totalled $119.91 billion as shown in table 1.

As stated previously, anticipated Chinese expenditure in developing CPEC would amount to between $30 billion and $40 billion. Some economists estimated that CPEC would cost as much as $46 billion.[98] This enormous cost, almost tripling past investments in Pakistan, would be incurred over several decades, and no completion date had been stipulated. Potentially, when including the completed CPEC, Chinese investment in Pakistan would approach a staggering estimated $67 billion—one of China's largest overseas investments. As a consequence, Pakistan would surely retain its prime position in the rank order of public limited company investments in the IOR littoral countries.

Malaysia also deserved special mention. The recently announced Malacca Gateway project was conservatively estimated to cost about $10 billion. When

Table 1. Select Chinese infrastructure investments in the Indian Ocean Region

Country	Investment (billion US$)	Rank
Pakistan	20.56	1
Malaysia	19.88	2
Iran	17.83	3
India	14.70	4
Sri Lanka	10.78	5
Singapore	10.55	6
Mozambique	7.72	7
Bangladesh	6.90	8
Myanmar	6.06	9
Djibouti	1.78	10
Yemen	1.71	11
Mauritius	1.15	12
Madagascar	0.29	13

Source: American Enterprise Institute, "China Global Investment Tracker," http://www.aei.org/china-global-investment-tracker/.

this proposed cost was taken into account, Chinese past and planned investment costs in Malaysia would increase to approximately $30 billion. Malaysia and Pakistan represented strategic nodes on the MSR; Malaysia particularly because of the bottleneck Strait of Malacca and Pakistan because it afforded opportunity for a new land bridge to western China. Hence, the combined past and proposed Chinese investments in the two countries amounted to approximately $107 billion. This figure was greater by around $14 billion than past Chinese investment in the United States. It was not known what new investments China was planning for America.

By contrast, past Chinese investments in Western Europe were close to $122 billion.[99] From this cursory analysis, it may be asserted that China's global investments were almost equally split three ways by approximately $100 billion each in the IOR, Europe, and the United States. The analysis did not include Africa. The China Global Investment Tracker puts total Chinese foreign direct investment in Africa at $61 billion in 2013.[100] The actual figure, if known, may be much closer to, and possibly greater than, $100 billion. This should give interested parties pause to consider if all of this investment was related purely to commercial development or if there were strategic, national security rationales mixed with the economic justifications for IOR development. The present economic slowdown in China might delay the above planned projects as would a world recession, but this did not detract from the import of already spent and promised funds, which could position China as one of the world's biggest cross-border investors.

Deployment of Chinese Warships

When considering the purpose of Chinese spending, other actions spoke to the possibility of funding IOR projects for development beyond just economic purposes, such as the deployment of Chinese warships and the building of ships for China's blue-water navy. Franz-Stefan Gady reported on the Chinese Ministry of National Defense's announcement on 29 January 2015 that China indeed would be stepping up its activities in the IOR. Senior Colonel Yang Yujun "downplay[ed] Chinese naval activities in the region, characterizing them as normal, and emphasizing that 'there is no need to read too much into them.' "[101] These and other similar activities fell well within China's waishi diplomatic policy, which included a projection of a position on the world stage to allay Western suspicions by playing down the impute of official statements relative to increasing aggressiveness, expansionism, and continuing militarism.[102] This concerned Indian officials as sightings of submarine forces become more frequent. Military analysts in India stated that the deployment of Chinese nuclear submarines would initiate a naval arms race. As of mid-2015, reports indicated that the Indian Navy was "determined to control the Indian Ocean Region."[103] And, other countries had seen more than just submarines. China dispatched a flotilla to the Persian Gulf in

2008, including a Type 052C Luyang II-class guided-missile destroyer as a part of an international Somali counterpiracy campaign. As of 2015, Ridzwan Rahmat reported for the IHS *Jane's Defence Weekly* that "the PLAN is deploying the 19th rotation of its naval escort fleet to the counter-piracy campaign."[104] While China could show goodwill participating in these antipiracy efforts, it was also a chance for the Chinese to demonstrate strength in the region.

Quite apart from the Chinese deployments to the western Indian Ocean, Chinese warships steamed into the eastern Indian Ocean somewhere between Christmas Island and Indonesia in 2014. The small flotilla comprised an advanced amphibious landing craft, *Changbaishan*, and two escort destroyers, *Wuhan* and *Haikou*. The flotilla was tasked with counterpiracy, search and rescue, and damage control drills. The *Changbaishan* was China's largest landing craft at 20,000 tons capable of transporting a marine battalion, 15–20 armored vehicles, a hovercraft, and two helicopters.[105]

China's sale of eight modified Type 41 Yuan-class diesel-electric submarines on very soft terms to Pakistan reinforced New Delhi's view that China had aggressive plans to neutralize India in its own backyard. The *Diplomat*'s Benjamin David Baker reported that "these boats will provide Islamabad with much-needed Anti-Access/Area Denial (A2/AD) capabilities against the Indian Navy in case of war."[106] This dilatory ploy would make Pakistan powerful enough to move India's attention away from China. Moreover, Beijing would have the ability to concentrate for the short term on events in the South China Sea. These events could also explain why New Delhi planned to place S-400 Triumf antimissile systems to its west and only two in its eastern region.[107]

The Possibility of Chinese Aircraft Carriers in the IOR

Traditionally, PLAN was originally configured for coastal defense and the invasion of Taiwan. Looking at the strategic situation from a purely military perspective, however, it was evident PLAN, in the last seven years, continued and was continuing to rapidly expand its South Sea fleet. It now had oceanic ambitions beyond its Near Seas. PLAN already had an operational aircraft carrier as of January 2015. The aircraft carrier *Liaoning* was based in the port of Qingdao in Shandong Province on mainland China. The original *Admiral Kuznetsov* Soviet-class multirole aircraft carrier began life as the uncompleted *Varyag* in the Ukraine, was abandoned when the Soviet Union collapsed, and later sold for $20 million to a Hong Kong developer. Subsequently, the ship was towed to a Dalian shipyard in northeastern China, refurbished, renamed, and commissioned by PLAN in September 2012. Flight tests were undertaken with the Shenyang J-15 Flying Shark carrier-borne fighter jet.[108] It was questionable whether this carrier would ever be assigned to patrols in the IOR. Certainly, it appears not in the immediate short term. Nonetheless, the possibility must not be discounted. Much depended on

the infrastructure in place in such faraway ports as Gwadar and Hambantota.[109]

In January 2014, it emerged that China was allegedly building a second aircraft carrier. This news had been cautiously accepted by naval intelligence experts. Wang Min, a Chinese Communist Party secretary, stated that construction of the carrier's design was completely different from that of the refurbished *Liaoning* described above. At that point, the new carrier was purportedly under construction at the Dalian shipyard and would take six years to complete.[110] It was not known when the second carrier was destined to be commissioned by PLAN, but as of January 2016, Defense Minister Yang Yujun confirmed China's persistence that the new carrier be designed and built indigenously.[111] Indeed, as Franz-Stefan Grady reported in January 2015, China might already be in the process of creating a fourth fleet, based at Hainan Island in the South China Sea. This fleet would comprise two carrier battle groups deemed to be operational by 2020. It could be argued that as these carrier battle groups would be extremely vulnerable to U.S. naval superiority in the Western Pacific, and thus their intended patrol areas might be de facto in the IOR. Here the two groups would exercise more of a psychological impact as well as protecting China's SLOCs. But even in peacetime, the presence of these groups in China's Near Seas and Indian Ocean would increase the chance of further undesirable confrontations, skirmishes, and incidents at sea. Yet, in the diplomatic tradition of *waishi*, Chinese officials in the Ministry of National Defense continued to deny claims about building warships beyond what they have admitted to publicly.[112]

Some pundits asserted that carriers were likely here to stay as the United States worked to replace its aging fleet with the new *Gerald R. Ford* class carriers and China built up a fleet of its own.[113] Other navy analysts were not so certain and believed the era of aircraft carriers might be over.[114] Clearly, the Chinese and the American governments had not given up on these maritime "dinosaurs," and they might even become targets for long-range antiship missiles or attack subs. Only time will tell if these actions by both governments would lead to an arms race to counteract each other's power or if China would gain hegemony in the IOR without incident.[115]

Chinese-Western Aircraft Carrier Ratio

To determine relative naval power, we could use ratios to determine superiority. Generally, analysts were concerned with battle group superiority that considered, in the case of aircraft carriers, both the carriers and extensive escorts. Thus, nations with carrier battle groups had superiority over those who could only deploy individual carriers without large numbers of supportive ships and personnel. At the time of writing this article, India was the only littoral nation that could deploy two carriers, forming at least one carrier battle group in the IOR.[116] Fortunately, the U.S. Navy already demonstrated it could deploy up to three carrier battle

groups as necessary in the IOR, but this was about to change.[117] As power shifts in the region, other countries were sending ships. In January 2015, the French sent the 42,000-ton *Charles de Gaulle* (R 91) from Europe to the Indian Ocean for exercises with the intention of possibly aiding other Eastern Mediterranean nations in the fight against the Islamic State in Iraq and the Levant.[118] This would make up for any U.S. reduction in carrier deployment in terms of the Chinese–Western aircraft carrier ratio. Overall, as the Chinese pursued commerce and pirates, Western powers could justify their presence similarly.

In the past, the U.S. Navy deployed up to three carriers in the Arabian Gulf and Arabian Sea region.[119] Allied navies also deployed warships, but few if any carriers. Hence, the current ratio could be calculated as follows: two Indian carriers, one from France, and two U.S. carrier battle groups amounting to five in total. PLAN could possibly deploy only one carrier at present; however, this figure was by no means certain. Thus, the ratio presently stood at 1:5 in favor of pro-Western navies. China was rethinking how a future war might play out, considering submarines and cruise missiles as key investments.

The SOP Concept: China's "Ports Wish List"

To summarize, China's SOP concept today consisted of the following ports that were being or could readily be used and accessed by PLAN: Djibouti, Hambantota, Gwadar, Chittagong (Bangladesh), and Marao (Maldives). Ports that PLAN would like to use but the territory concerned might not voluntarily allow, or that U.S. and Western navies might resist include Darwin (Australia); Kyauckpyu (Myanmar); Singapore; Penang, Northport, and Tanjung Pelepas (Malaysia); Aden (Yemen); Bandar Abbas (Iran); Berbera (Somalia); and Tanjong Priak (Indonesia). In the wish list of secondary ports, Singapore would be the most important addition to the SOP concept. Approximately 80 percent of China's imported energy came through the Strait of Malacca. Singapore was currently home to U.S. littoral combat ships and, in the event of trouble, would be awash with U.S. Marines, as was the case during the Vietnam War.

As David Brewster noted in the *Interpreter*, "China confirmed it was in talks with Djibouti to construct its first overseas military base," on 26 November 2015, and "this represents a major symbolic and practical step in China's emergence as a global military power."[120] In essence, the Chinese wanted the option to respond to multiple scenarios. Brewster pointed to the fact that China would implement a policy in the near future that would likely focus on "military operations other than war" in the IOR.[121] China would be able to react quickly to any contingency concerning the sustainability of oil and gas shipments to China from the Middle East.[122] This new development alone reinforced the validity of the SOP concept and the idea that the MSR had become a smokescreen for China's true intentions because China allayed Western suspicions by using the waishi policy. Brewster

added that while the "Chinese analysts use the term *bùjǐ zhàn* (literally 'depot' or 'supply station') to describe China's needs in the Indian Ocean," nothing could be further from the truth.[123] For any war machine to conduct campaigns at vast distances from the motherland, infrastructure and prepositioning of materiel must first be in place. This was a fundamental logistical requirement.

Looking to the Future in the IOR

Apart from financial constraints, the sustainability of the MSR as an integral component of China's OBOR initiative could only be ensured by a number of factors: (1) improved infrastructure and services to enhance international trade; (2) continuously improved productivity levels to accommodate trade growth; (3) consolidated trade cargoes at preferred, strategic ports; (4) ports to harness multimodel logistics to link to hinterland economic corridors; and (5) strategic alliances with leadership trading partners using state-of-the-art information technology, marketing, and business administration.

Multiple Western and Pacific Rim nations—including, the United States, United Kingdom, France, Germany, and other Western European countries as well as Pakistan, India, ASEAN member countries, Taiwan, China, South Korea, Japan, and Australasia—were all heavily dependent upon sustained oil and gas supplies sourced from the Arabian Gulf and from elsewhere in the Middle East. None of these countries, especially China as the world's second largest net oil importer, could afford disruptive interdiction in the Strait of Hormuz, Strait of Malacca, or elsewhere in the IOR. By seeking maritime hegemony, China could least afford to entertain disruption to its SLOCs. If in the future China was able to import adequate alternative oil and gas supplies from Central Asia or from Russia as a viable substitute for Middle East sourced oil and gas, then the "Great Game/Big Oil" would take on another dimension. China would be able to exert total offensive hegemony in the IOR without fear of punishment to its own economy. The United States, now reaping the benefits of new domestic shale oil discoveries, was less dependent upon Middle East oil and gas shipments; however, America would continue to exercise prominent naval power, emergency rapid response, and strategic and military initiatives in the IOR largely to protect countries littoral to the IO, together with the interests of Western powers still largely dependent upon Middle East oil and gas supplies.

The role of the aircraft carrier would dramatically change in years to come. This prescient observation by military analysts merited a mention here. First, there was the unanswered question as to the susceptibility of carriers to antiship ballistic missiles.[124] Second, the future of manned front-line strike fighter aircraft might be limited. The Lockheed Martin F-35C Lightning II, according to U.S. Secretary of the Navy Raymond E. Mabus, "should be, and almost certainly will be, the last manned strike fighter aircraft the Department of the Navy will ever buy or fly."[125]

It was not known if the development of remotely piloted aircraft or unmanned aerial vehicle capabilities would eventually replace carrier-borne conventional manned aircraft.[126] Perhaps one day we might see "swarm-configurable" hostile drones emitting from a modified carrier like angry bees from a hive.[127] Will swarms of invasive Chinese, Indian, and Pakistani drones launched from a multiplicity of platforms pervade the IOR?

China might indeed be seeking hegemony in the IOR as so many analysts believed. China's String of Pearls might certainly be its true national security strategy, which should not be obscured by waishi diplomacy and such initiatives as the maritime silk road.

Notes

Sections of this article came from a special report published previously by Future Directions International (FDI), an independent, not-for-profit research institute. See Capt David L. O. Hayward, *China in the Indian Ocean: A Case of Uncharted Waters* (Perth, Western Australia: FDI, 2010). The author was given permission to reproduce portions of the text; however, relevant facts have been updated to reflect post-2011 realities and events. The author thanks the MCU Press acquisitions and editorial staff; MajGen John Hartley, Australian Army (Ret); Lindsay Hughes; Alan Baker; Patricia Hayward, and the anonymous reviewers for their thoughtful comments and suggestions during the early drafts of this article. The analysis and opinions expressed here are those of the author and do not represent the assessment of FDI, MCU Press, or any other agency.

1. China's "Near Seas" include the Bohai (Bo Hai), Yellow (Huang Hai), East China (Dong Hai), and South China (Nan Hai) Seas.
2. World Bank, "Data: GDP at Market Prices (Current US$)," 19 February 2016, http://data.worldbank.org/indicator/NY.GDP.MKTP.CD.
3. Ibid.
4. Green-water navies are made up of smaller ships and generally patrol ocean littorals, whereas blue-water navies use battleships and carriers for the more offensive missions at sea. See Robert C. Rubel, "Talking about Sea Control," *Naval War College Review* 63, no. 4 (Autumn 2010): 44–46, http://www.dtic.mil/dtic/tr/fulltext/u2/a536641.pdf. Iran has indicated in the past that it may one day construct an indigenous aircraft carrier. This may be a fallacious argument as Iran presently has neither the expertise nor the requisite financial resources to construct a blue-water navy. Nima Adelkhah, "The Impossible Dream: Tehran Rethinks Its Commitment to an Iranian-Built Aircraft Carrier," *Terrorism Monitor* 9, no. 45 (9 December 2011): 5–6, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=38768&no_cache=1#.VpYxiBV94dU.
5. Spencer Ackerman, Saeed Kamali Dehghan, and Sabrian Siddiqui, "Iran Demands Apology after Detaining U.S. Navy Boat Crews for 'Violating' Gulf Waters," *Guardian*, 13 January 2016, http://www.theguardian.com/world/2016/jan/12/iran-detains-two-us-navy-ships-persian-gulf.
6. Mehrdad Moarefian et al., "Iran News Round Up January 13, 2016," AEI Iran Tracker, 13 January 2016, http://www.irantracker.org/iran-news-round-january-13-2016.
7. Ibid.
8. "Full Text: Xi Jinping in Military Parade Speech Vows China Will 'Never Seek Hegemony, Expansion'," *South China Morning Post* (Hong Kong), 3 September 2015, http://www.scmp.com/news/china/policies-politics/article/1854943/full-text-xi-jinping-military-parade-speech-vows-china.
9. Steven W. Mosher, "Does the PRC Have a Grand Strategy of Hegemony?," Air University, http://www.au.af.mil/AU/awc/awcgate/congress/mos021406.pdf.
10. Auriol Weigold, *Embrace and Encircle? China's Approaches to India and Their Effect* (Dalkeith,

Australia: FDI, 2015), http://futuredirections.org.au/wp-content/uploads/2016/01/Embrace_and_Encircle_-_Chinas_approaches_to_India_-_final.pdf.

11. Lindsay Hughes, *Examining the Sino-Indian Maritime Competition, Part 1* (Dalkeith, Australia: FDI, 2013), http://futuredirections.org.au/wp-content/uploads/2013/12/FDI_Strategic_Analysis_Paper_-_09_December_2013.pdf; *Examining the Sino-Indian Maritime Competition: Seapower, Part 2* (Dalkeith, Australia: FDI, 2014), http://futuredirections.org.au/wp-content/uploads/2014/01/Examining_the_Sino-Indian_Maritime_Competition_Part_2_-_Seapower.pdf; *Examining the Sino-Indian Maritime Competition: China Goes to Sea, Part 3* (Dalkeith, Australia: FDI, 2014), http://futuredirections.org.au/wp-content/uploads/2014/01/Examining_the_Sino-Indian_Maritime_Competition_Part_3_-_China_goes_to_sea.pdf; and *Examining the Sino-Indian Maritime Competition: India's Maritime Strategy, Part 4* (Dalkeith, Australia: FDI, 2014), http://futuredirections.org.au/wp-content/uploads/2014/01/Examining_the_Sino-Indian_Maritime_Competition_Part_4_-_Indias_Maritime_Strategy.pdf.
12. Hughes, *Examining the Sino-Indian Maritime Competition, Part 1,* 1.
13. Virginia Marantidou, "Revisiting China's 'String of Pearls' Strategy," *Issues & Insights* 14, no. 7 (June 2014), http://csis.org/publication/issues-insights-vol-14-no-7-revisiting-chinas-string-pearls-strategy.
14. Abhijit Singh, "China's new 'Blue-Book' for the Indian Ocean," *Daily Mirror Business,* 26 June 2013, http://www.dailymirror.lk/31520/chinas-new-blue-book-for-the-indian-ocean.
15. "The 'Silk Road Economic Belt' and '21st Century Maritime Silk Road' are initiatives first introduced by Xi in the fall of 2013 during visits to Kazakhstan and Indonesia, respectively. They are expected to feature prominently in China's 13th Five-Year Plan, which will run from 2016 to 2020 and guide national investment strategy throughout that period." See Scott Kennedy and David A. Parker, "Building China's 'One Belt, One Road'," Center for Strategic and International Studies (CSIS), 3 April 2015, http://csis.org/publication/building-chinas-one-belt-one-road.
16. Ibid.
17. Philip Wen, "China Plans a Military Base in Djibouti," *Sydney Morning Herald* (Australia), 27 November 2015, http://www.smh.com.au/world/china-plans-a-military-base-in-djibouti-20151126-gl9c45.html.
18. "The Red Sea: Can It Really Be Bridged?," *Economist*, 31 July 2008, http://www.economist.com/node/11849068.
19. Kristine Kwok and Zhuang Pinghui, "Chinese Military Aircraft Likely to Land at New Airport in Disputed Area of South China Sea in Coming Months, Says Ex-PLA Officer," *South China Morning Post* (Hong Kong), 8 January 2016, http://www.scmp.com/news/china/diplomacy-defence/article/1899036/chinese-military-aircraft-likely-land-new-airport.
20. Additional military airbases are proposed for Subi, Hughes, Gaven, Johnson South, and Cuarteron reefs in the Spratly Islands. For an example, see Victor Robert Lee, "South China Sea: China's Unprecedented Spratlys Building Program," *Diplomat*, 25 April 2015, http://thediplomat.com/2015/04/south-china-sea-chinas-unprecedented-spratlys-building-program/.
21. Usman Ansari, "Pakistan, China Finalize 8-Sub Construction Plan," *Defense News,* 11 October 2015, http://www.defensenews.com/story/defense/naval/submarines/2015/10/11/pakistan-china-finalize-8-sub-construction-plan/73634218/.
22. Angela Meng and Minnie Chan, "Beijing Eyes Bigger Arms Exports after Pakistan Deal, Experts Say," *South China Morning Post* (Hong Kong), 26 April 2015, http://www.scmp.com/news/china/diplomacy-defence/article/1776522/beijing-eyes-bigger-arms-exports-experts-say.
23. Greg Earl, "Blackstone Chief Plays Down China Market Turmoil," *Financial Review,* 13 January 2016.
24. David Sheppard and Ron Bousso, "With Oil Under $100, China Trader Books World's Largest Ship to Store Crude," Reuters, http://www.reuters.com/article/us-unipec-ulcc-storage-idUSKBN0H401J20140909. Also see "Update 1-China June Crude Oil Imports Up 27 pct on Year in Challenge to U.S. for Top Spot," Reuters, 13 July 2015, http://

www.reuters.com/article/china-crude-imports-idUSL3N0ZN2MJ20150713#s3IaoY1O1cHKIoRP.97.

25. Kalyan Kumar, "China to Double Strategic Oil Purchases in 2016," *International Business Times*, 8 December 2015, http://www.ibtimes.com.au/china-double-strategic-oil-purchases-2016-1490464.
26. U.S. Energy Information Administration (EIA), "China: International Energy and Data Analysis," 14 May 2015, https://www.eia.gov/beta/international/analysis.cfm?iso=CHN. Also see David Robinson, *China's Growing Energy Demand: Some International Implications*, Oxford Institute for Energy Studies, 17 October 2013, http://www.oxfordenergy.org/wpcms/wp-content/uploads/2013/12/Chinas-growing-energy-demand.pdf.
27. EIA, "China: International Energy."
28. Erica S. Downs, "China-Middle East Energy Relations," Brookings Institution, 6 June 2013, http://www.brookings.edu/research/testimony/2013/06/06-china-middle-east-energy-downs; and International Energy and Organisation for Economic Co-operation and Development (OECD) and International Energy Agency (IEA), *World Energy Outlook 2012* (Paris: OECD/IEA, 2012), 78–80, http://www.iea.org/publications/freepublications/publication/WEO2012_free.pdf.
29. James Bourne, "Petrodollars: China Builds Up Its Oil Tanker Fleet," *The Barrel* (blog), *Platts McGraw Hill Financial*, 18 August 2014, http://blogs.platts.com/2014/08/18/china-oil-tankers/.
30. Ibid.
31. David L. O. Hayward, "China's Oil Supply Dependence," *Journal of Energy Security* (June 2009), http://ensec.org/index.php?option=com_content&view=article&id=197:chinas-oil-supply-dependence&catid=96:content&Itemid=345.
32. "China Population," Worldometers, http://www.worldometers.info/world-population/china-population/.
33. Jonathan Woetzel et al., *If You've Got It, Spend It: Unleashing the Chinese Consumer* (McKinsey Global Institute, 2009), http://www.mckinsey.com/~/media/McKinsey/Global%20Themes/China/If%20youve%20got%20it%20spend%20it%20Unleashing%20the%20Chinese%20consumer/MGI_Unleashing_Chinese_Consumer_full_report.ashx.
34. Ibid. Also see EIA, "China: International Energy."
35. "China ranked first in exports with an export value of about US$2.3 trillion in 2014." See Statista, "Top 20 Export Countries Worldwide in 2014," http://www.statista.com/statistics/264623/leading-export-countries-worldwide/.
36. The Chinese government is actively moving away from manufacturing small goods such as textiles and furnishings, outsourcing these industries to Bangladesh, Cambodia, and Vietnam, for example.
37. Ben Bland, "China Imports Slide Fuels Record Trade Surplus," *Financial Times*, 13 October 2015, http://www.ft.com/intl/cms/s/0/06cb7bbc-7161-11e5-9b9e-690fdae72044.html#axzz3zgihNaYY.
38. The ongoing race between China and the United States for military control of the Indian Ocean, Singapore, and the Strait of Malacca may underwrite any such PRC contrived copycat contingency study. See Geoffrey Kemp, "The New Strategic Map," *Survival* 19, no. 2 (1977): 50–59, doi:10.1080/00396337708441666.
39. South Korea used the South-up map orientation for decades, proving they are above North Korea. See "군가: 멸공의 횃불 (Martial Music: Myeongdong Torch)," YouTube video, 3:09, posted by "이효관," 30 July 2010, https://youtu.be/QyCOtYprTCs?t=2m28s. There are many other inverted (south-up) world maps both ancient and modern. For example, (1) Nicolas Desliens compiled an upside down map in 1566 that can be seen at the Bibliotheque Nationale in Paris, France; and (2) McArthur's Universal Corrective Map of the World was the first modern south-up map published in Australia in 1979. It is not known if Chinese military forces use inverted maps, but this is very likely as South Korea does use south-up maps for enhanced military perspective.
40. China's "Sacred Territory" is an enduring concept prevalent among the Chinese public before and after World War II. It relates to Chinese claims of sovereignty over disputed

island groups in the South China and East China Seas, including Taiwan. These claims are based upon a complicated mix of legal and historical grounds. See Jian Zhang, "China's South China Sea Policy: Evolution, Claims, and Challenges," in *The South China Sea Maritime Dispute: Political, Legal and Regional Perspectives,* ed. Leszek Buszynski and Christopher B. Roberts (New York: Routledge, 2015), 69.

41. Entry ports and oil infrastructure facilities can be further defined by access to www.portguide.com. Lloyd's Register Fairplay Ltd. published a *Tanker Berth Guide* that is available to subscribers.
42. Andrew S. Erickson and Gabriel B. Collins, "China's Oil Security Pipe Dream: The Reality, and Strategic Consequences, of Seaborne Imports," *Naval War College Review* 63, no. 2 (Spring 2010), http://www.andrewerickson.com/wp-content/uploads/2010/03/China-Pipeline-Sealane_NWCR_2010-Spring.pdf.
43. Erickson and Collins "China's Oil Security Pipe Dream" highlights the fact that "Numerous Chinese articles and discussions with Chinese interlocutors from all these communities underscore this point." For complete analysis, see Andrew Erickson and Gabe Collins, "Beijing's Energy Security Strategy: The Significance of a Chinese State-Owned Tanker Fleet," *Orbis* 51, no. 4 (Fall 2007): 665–84, doi:10.1016/j.orbis.2007.08.009. Also refer to 李小军 (Li Xiaojun), "论海权对中国石油安 全的影响" (On the Influence of Sea Power upon China's Oil Security), 国际论坛 (*International Forum*) 6, no. 4 (July 2004): 18, http://en.cnki.com.cn/Article_en/CJFDTOTAL-GJLT200404003.htm and other academic papers.
44. Pablo Bustelo, *China and the Geopolitics of Oil in the Asian Pacific Region*, Working Paper 38/2005 (Madrid: Elcano Royal Institute, 2005), http://www.realinstitutoelcano.org/documentos/226/Bustelo226.pdf. This new pipeline was completed in August 2014.
45. Ian Storey, "China's 'Malacca Dilemma'," *China Brief* 6, no. 8 (2006), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=31575&no_cache=1#.VsxYy8eof8s; and Sunny Mewati, "How Can China Protect Itself against the Blockade of Malacca Strait by a Carrier Task Force?," Quora, 13 September 2014, https://www.quora.com/How-can-China-protect-itself-against-the-blockade-of-Malacca-Strait-by-a-carrier-task-force.
46. Antoine Bondaz, "Solving the 'Rise' Dilemma: How the Chinese Silk Road Initiative Could Challenge the United States," *International Relations and Security Network* (blog), 8 May 2015, http://isnblog.ethz.ch/international-relations/solving-the-rise-dilemma-how-the-chinese-silk-road-initiative-could-challenge-the-united-states.
47. For more on future China-U.S. relations, see Kent Moors, *The Great Game: The Coming Face Off for Global Supremacy* (Baltimore: Money Map Press, 2014), 42–46.
48. Oil major BP uses multiple iterative calculations to discover the least costs for operating its oil tanker fleet worldwide.
49. In particular, Hainan Island (Hainan Dao) is perceived as the "fortress" dominating the South China Sea and filling a power vacuum left after the abandonment of the U.S. Subic Bay Naval Base, Philippines, and return of UK-administered Hong Kong to China.
50. Shahbaz Rana, "China to Provide Rs410m for Gwadar Port Feasibility Study," *Express Tribune* (Karachi), 22 January 2016, http://tribune.com.pk/story/1032426/china-to-provide-rs410m-for-gwadar-port-feasibility-study/.
51. "China Gets 40-Year Management Rights on Gwadar Port, Access to Arabian Sea," *Express Tribune* (Karachi), 15 April 2015, http://tribune.com.pk/story/870183/china-gets-40-year-management-rights-on-gwadar-port-access-to-arabian-sea/.
52. Lisa Murray, "China's Economic Vision Expands with a New Version of the Old Silk Road," *Financial Review*, 29 December 2015.
53. Ibid. Murray explains the confusing distinction between the "belt" (i.e., ancient overland route followed by the Silk Road first opened in around 3000 BC) and the "road" interpreted as the younger maritime route transiting China's Near Seas, Strait of Malacca, IOR, Suez Canal, and Mediterranean to Western Europe.
54. The three financial institutions have been set up to support its development, which have met some resistance in the West given they provide alternatives to the World Bank, IMF, and ADB. For more information on the Silk Road Fund, Asian Infrastructure Invest-

ment Bank, and New Development Bank, see Francis Cheung and Alexious Lee, "A Brilliant Plan: One Belt, One Road," Credit Lyonnais Securities Asia, https://www.clsa.com/special/onebeltoneroad/#header.

55. Ibid.
56. Summer Zhen, "China's 'One Belt One Road' Investment to Reach US$200 Billion in Three Years," *South China Morning Post* (Hong Kong), 28 October 2015, http://www.scmp.com/business/global-economy/article/1872858/one-belt-one-road-investment-reach-us200b-three-years.
57. Ismal Dilawar, "Plan to Link Gwadar Port to Western China Finalised," *Pakistan Today,* 25 November 2014, http://www.pakistantoday.com.pk/2014/11/25/business/plan-to-link-gwadar-port-to-western-china-finalised/. Also see Parvaiz Ishfaq Rana, "PCEC Will Cater for Europe's Needs Too," *Dawn* (Karachi), 25 November 2014, http://www.dawn.com/news/1146698.
58. Kamran Haider, "Pakistan Wants to Become China's Newest Superhighway to Europe," *Bloomberg Business*, 31 March 2015, http://www.bloomberg.com/news/articles/2015-04-01/pakistan-s-sharif-seeks-energy-deals-during-china-visit.
59. "Pak-China Corridor," *Dawn* (Karachi), 5 July 2014, http://www.dawn.com/news/1117079. Also see "Is China-Pakistan 'Silk Road' a Game-Changer?," BBC News, 22 April 2015, http://www.bbc.com/news/world-asia-32400091; Andrew Stevens, "Pakistan Lands $46 Billion Investment from China," CNN Money, 20 April 2015, http://money.cnn.com/2015/04/20/news/economy/pakistan-china-aid-infrastucture/; "RAW at Frontline to Sabotage Economic Corridor, China Warns Pakistan," *Express Tribune* (Karachi), 22 May 2015, http://tribune.com.pk/story/890650/raw-at-frontline-to-sabotage-economic-corridor-china-warns-pakistan/; and "中国当局将在乌鲁木齐实行宵禁1/2 2009年07月07日 Uigures Xinjiang's Bloody (Chinese Authorities Imposed a Curfew 1–2 July 2009)," Hmong video, 8:50, posted by "Nokiashilo," 7 July 2009, http://www.hmoobtube.com/watch?v=Qp7UkQY8l3c.
60. Asim Hussain, "Gwadar Port to Become Operational in May," *Daily Mail News*, 6 February 2015, http://dailymailnews.com/2015/02/06/gwadar-port-to-become-operational-in-may/; and Akhilesh Pillalamarri, "The China-Pakistan Economic Corridor Is Easier Said than Done," *The Pulse* (blog), *Diplomat,* 24 April 2015, http://thediplomat.com/2015/04/the-china-pakistan-economic-corridor-is-easier-said-than-done/.
61. "Pakistan's Gwadar Port Run by China 'Matter of Concern' for India," *Economic Times* (India), 6 February 2013.
62. "Coal-Fired Plants Elsewhere," Power Plants Around the World, 30 January 2016, http://industcards.com/st-coal-elsewhere.htm. The Colombo-Katunayake Expressway was completed and opened to the public 27 October 2013. See Tudor Wijenayake, "Colombo–Katunayake Expressway: From Rs. 5.5 Billion to Rs. 50 Billion," *Daily FT* (Sri Lanka), 12 February 2016, http://www.ft.lk/2013/10/25/colombo-katunayake-expressway-from-rs-5-5-billion-to-rs-50-billion/. The National Performing Arts Theatre officially opened 15 December 2011. See "Colombo, National Performing Arts Theatre, Completed," Skyscrapercity (forum), http://www.skyscrapercity.com/showthread.php?t=1104129; and "China to Help Build Sri Lanka National Performing Arts Theater," *Xinhua*, 11 November 2005, http://china.aiddata.org/projects/33281?iframe=y.
63. Elsa Buchanan, "Sri Lanka's New Government to Investigate Mahinda Rajapaska Corruption Allegations," *International Business Times*, 16 January 2015, http://www.ibtimes.co.uk/sri-lankas-new-government-investigate-mahinda-rajapaksa-corruption-allegations-1483812.
64. *World Maritime News,* "Sri Lanka: Colombo South Harbour Opens Today," Sri Lanka News Elephant House (forum), 5 August 2013, http://www.lankanewspapers.com/news/2013/8/84175_space.html.
65. Rish, "Emerging Giants India, China Jostle for Influence over Vital Indian Ocean Shipping Lanes," DefenceTalk (forum), 14 June 2008, no. 1268, http://www.defencetalk.com/forums/navy-maritime/indian-navy-news-discussion-3959-85/.
66. Zhao Gancheng, director of South Asia Studies at the Shanghai Institute for International Studies, is quoted as saying the following: "The Gwadar port will also guarantee

China's naval ships' maintenance and supply in the Indian Ocean. . . . The move is widely seen as crucial for China, especially as it is unlikely that Sri Lanka will open its ports to Chinese naval ships." See Lui Sha and Chen Heying, "Gwadar Set to be Regional Hub as Port Readies Launch," *Global Times* (Beijing), 15 April 2015, http://www.globaltimes.cn/content/916884.shtml.

67. Ankit Panda, "China's Sri Lankan Port Ambitions Persist," *Diplomat*, 27 July 2015, http://thediplomat.com/2015/07/chinas-sri-lankan-port-ambitions-persist/; and Debasish Roy Chowdhury, "Sri Lanka Looks to China to Buoy Sinking Port," *South China Morning Post* (Hong Kong), 11 October 2015, http://www.scmp.com/business/global-economy/article/1866287/sri-lanka-looks-china-buoy-sinking-port.
68. Dato' Sri Che Khalib Mohamad Noh, *Role of Malaysian Ports and Chinese Ports in Realizing Maritime Silk Road Initiative* (Kuala Lumpur: MMC Corporation Berhad, 2015). Page 309 of the report lists the top 30 largest shareholders. More than 70 percent of issued capital is held by two entities (private companies): Seaport Terminal Johore Sdn. Bhd (51.76 percent) and Amanahraya Trustees Berhad-Skim Amanah Saham Bumiputera (20.28 percent). Between these two entities, shares amount to approximately 1.5 and 0.6 billion shares, respectively. It is not known how many of these shares are held by Chinese investors. See MMC Corporation Berhad, *Growth Momentum: 2014 Annual Report* (Kuala Lumpur: MMC Corporation Berhad, 2015), www.mmc.com.my/pdf/MMC_AR_2014_cover_to_page109.pdf.
69. R. S. N. Murali, "RM43bil Investment in Malacca Gateway a Boost to Malaysia, says Liow," *Star Online*, 8 November 2015, http://www.thestar.com.my/news/nation/2015/11/08/china-to-spur-growth-of-ports-rm43bil-investment-in-malacca-gateway-a-boost-to-malaysia-says-liow/.
70. Ibid.; and *Star Online*, "Kedah to Emerge as International Fisheries Centre," 13 May 2015, http://m.thestar.com.my/story.aspx?hl=Kedah+to+emerge+as+international+fisheries+centre&sec=business&id={5B6CADBA-4764-42D2-94D8-1470D19D16BC}.
71. Malacca Emperor Beijing and Hong Kong (MEBHK), "首相推介礼 (Prime Minister Launching Ceremony), MEBHK, 30 January 2016, http://melakagateway.my/新闻多媒体-press-media/图片集-photos/; and "剪报 (newspaper clipping), MEBHK, 20–22 September 2015, http://melakagateway.my/新闻多媒体-press-media/c3/.
72. *Star Online*, "Kedah to Emerge as International Fisheries Centre."
73. "Strait of Malacca Ports," Ports.com, 30 January 2015, http://ports.com/sea/strait-of-malacca/.
74. TEU is a term that points to a ship's cargo carrying capacity based on the standard 20-foot shipping container. See MMC Corporation Berhad, *Growth Momentum*.
75. Ibid.
76. Joshua Kurlantzick, "Is China 'Losing' Southeast Asia?," *The Buzz* (blog), *National Interest*, 13 October 2015, http://nationalinterest.org/blog/the-buzz/china-losing-southeast-asia-14064; Joshua Kurlantzick, "Malaysia's Economy Faces Severe Strain," *Diplomat*, 29 August 2015, http://thediplomat.com/2015/08/malaysias-economy-faces-severe-strain/; Joshua Kurlantzick, "Malaysia's Economy Faces Severe Strain," *Asia Unbound* (blog), Council on Foreign Relations, 26 August 2015, http://blogs.cfr.org/asia/2015/08/26/malaysias-economy-faces-severe-strain/; Datuk Ramesh Chander and Bridget Welsh, "Solving Malaysia's Economic Crisis," New Mandala, 19 October 2015 http://asiapacific.anu.edu.au/newmandala/2015/10/19/solving-malaysias-economic-crisis/; and Florence Chong, "Financial, Human Capital in Flight from Malaysia," *Asia Today International*, 19 May 2015, http://asiatoday.com.au/content/financial-human-capital-flight-malaysia. For background reading on all Asia Pacific countries, see Ministry of Foreign Affairs (MFA) of Japan, *Diplomatic Blue Book 1990* (Tokyo: MFA of Japan, 1990), chapter 3, http://www.mofa.go.jp/policy/other/bluebook/1990/1990-3-1.htm.
77. Sol W. Sanders, "Malaysia: Over the Edge?," American Center for Democracy, 28 December 2015, http://acdemocracy.org/malaysia-over-the-edge/?utm_source=Malaysia%3A+Over+the+Edge%3F&utm_campaign=Malaysia%3A+over+the+edge%3F&utm_medium=email.
78. Ibid.

79. Ernest Z. Bower and Phuong Nguyen, "Will China–Malaysia Relations Remain a Model for Asia?," *cogitAsia* (blog), Center for Strategic and International Studies, 18 February 2015, http://cogitasia.com/will-china-malaysia-relations-remain-a-model-for-asia/.
80. Prashanth Parameswaran, "Malaysia Slams China's South China Sea Encroachments," *Diplomat*, 17 November 2015, http://thediplomat.com/2015/11/malaysia-slams-chinas-south-china-sea-encroachments/.
81. Daniel Kostecka, "Hambantota, Chittagong, and the Maldives—Unlikely Pearls for the Chinese Navy," *China Brief* 10, no. 23 (2010): 8–11, http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=37196#.Vr4SKceof8t; Cmde Sujeet Samaddar (Indian Navy, Ret), *Minerals, Markets, and Maritime Strategy* (New Delhi: VIJ Books, 2011); and Rajat Pandit, "China's Stepped Up Moves in Maldives Worry India," *Times of India*, 10 October 2011, http://timesofindia.indiatimes.com/india/Chinas-stepped-up-moves-in-Maldives-worry-India/articleshow/10294868.cms.
82. Pandit, "China's Stepped Up Moves."
83. Brahma Chellaney, "China Reinvents 'String of Pearls' as Maritime Silk Road," *Nikkie Asian Review*, 29 April 2015, http://chellaney.net/2015/05/01/china-reinvents-string-of-pearls-as-maritime-silk-road/.
84. William Yale, "China's Maritime Silk Road Gamble," *Diplomat*, 22 April 2015, http://thediplomat.com/2015/04/chinas-maritime-silk-road-gamble/.
85. Sharon Uranie, "Promoting Trade and Investment between Seychelles and China: Opportunities Discussed with Qingdao Companies," Seychelles News Agency, 13 May 2015, http://www.seychellesnewsagency.com/articles/2928/Promoting+trade+and+investment+between+Seychelles+and+China+opportunities+discussed+with+Qingdao+companies.
86. Darshana M. Baruah, "The Small Islands Holding the Key to the Indian Ocean," *Diplomat*, 24 February 2015, http://thediplomat.com/2015/02/the-small-islands-holding-the-key-to-the-indian-ocean/.
87. Ibid.; "India engages China in a dialogue—because China needs to keep its oil supply lines under Chinese control." See Manoj Joshi, "The Bigger Picture: India Is Just Another Stop on China's Silk Route," *Daily Mail India*, 19 February 2014, http://www.dailymail.co.uk/indiahome/indianews/article-2563192/THE-BIGGER-PICTURE-India-just-stop-Chinas-silk-route.html#ixzz2ttVsdVhc.
88. Vanessa Dougnac, "China's 'String of Pearls' Strategy to Secure the Ports of South Asia," *Island* Online, 14 January 2013, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=70433.
89. Raisul Haq Bahar, editor in chief of the *Chittagong Daily Star*, wrote that "they have the know-how, the people, the money, and the technical investments. . . . They [China] are selling their country, their products and services. While the Westerners are busy attending fancy dinner parties in Dacca, the Chinese are working. They will soon be the world's first economy and a country like Bangladesh cannot ignore that." See Dougnac, "China's 'String of Pearls' Strategy."
90. Ibid.
91. Ibid.
92. Ananth Krishnan, "China Offers to Develop Chittagong Port," *Hindu* (Chennai), 15 March 2010, http://www.thehindu.com/news/international/china-offers-to-develop-chittagong-port/article245961.ece.
93. Jonathan Lim, "The Canal that Will Sink S'pore's Maritime-Trade Dominance Is One Step Closer to Fruition," Mothership.SG, 18 May 2015, http://mothership.sg/2015/05/the-canal-that-will-sink-spores-maritime-trade-dominance-is-one-step-closer-to-fruition/.
94. "Industrial Conglomerates: Company Overview of Shandong Landbridge Group," *Bloomberg Business*, 15 December 2015, http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=33920707; Lisa Murray, "Chinese State-Owned Newspaper Confirms Landbridge's Military Ties," *Financial Review*, 17 November 2015; and Helen Davidson, "Chinese Company Secures 99-Year Lease of Darwin Port in $506m Deal," *Guardian* (Melborne), 13 October 2015, http://www.theguardian.com/australia

-news/2015/oct/13/chinese-company-secures-99-year-lease-of-darwin-port-in-506m-deal.

95. "China Warships in Persian Gulf," *Iran Times* (Washington, DC), 1 April 2010, http://iran-times.com/china-warships-in-persian-gulf/.
96. Keith Johnson, "China Is the New Power Broker in the Persian Gulf," *Foreign Policy,* 26 March 2015, http://foreignpolicy.com/2015/03/26/chinas-thirst-oil-foreign-policy-middle-east-persian-gulf/.
97. Figures extrapolated from data compiled by the American Enterprise Institute (AEI) and The Heritage Foundation, "China Global Investment Tracker," 4 May 2015, http://www.aei.org/china-global-investment-tracker/. By contrast, Chinese investments in the United States ($81.12 billion) and Australia ($65.94 billion) indicate investments are spread worldwide.
98. Omar Alam, "China–Pakistan Economic Corridor: Towards a New 'Heartland'?," *London School of Economics and Political Science* (blog), 16 November 2015, http://blogs.lse.ac.uk/southasia/2015/11/16/china-pakistan-economic-corridor-towards-a-new-heartland/.
99. Extrapolated figures for 21 countries in Western Europe (excluding Greece and Turkey) for 2005–16 from data compiled by AEI and the Heritage Foundation, "China Global Investment Tracker," 6 January 2016.
100. Miria Pigato and Wenxia Tang, *China and Africa: Expanding Economic Ties in an Evolving Global Context* (Washington, DC: World Bank, 2015), http://www.worldbank.org/content/dam/Worldbank/Event/Africa/Investing%20in%20Africa%20Forum/2015/investing-in-africa-forum-china-and-africa-expanding-economic-ties-in-an-evolving-global-context.pdf.
101. Franz-Stefan Gady, "China's Navy to Send More Ships to the Indian Ocean," *Diplomat*, 31 January 2015, http://thediplomat.com/2015/01/chinas-navy-to-send-more-ships-to-the-indian-ocean/.
102. For more information on this topic, see Anne-Marie Brady, *Making the Foreign Serve China: Managing Foreigners in the People's Republic* (Lanham, MD: Rowman & Littlefield, 2003).
103. Manu Pubby, "As Sightings of Chinese Submarines Become Frequent, Navy Steps Up Guard in Indian Ocean Region," *Economic Times,* 8 August 2015, http://economictimes.indiatimes.com/news/defence/as-sightings-of-chinese-submarines-become-frequent-navy-steps-up-guard-in-indian-ocean-region/articleshow/48397646.cms; David Tweed and N. C. Bipindra, "Submarine Killers: India's $61 Billion Warning to China," *Bloomberg Business,* 28 July 2015, http://www.bloomberg.com/news/articles/2015-07-28/submarine-killers-showcase-india-s-61-billion-warning-to-china; and P. K. Ghosh, "Game Changers? Chinese Submarines in the Indian Ocean," *Diplomat,* 6 July 2015, http://thediplomat.com/2015/07/game-changers-chinese-submarines-in-the-indian-ocean/.
104. Ridzwan Rahmat, "PLAN to Deploy Range of Warships in Indian Ocean, Says China's Defence Ministry," World Affairs Council, 29 January 2015, http://worldaffairsroc.org/news.cfm?story=499&school=0. Also see, Mehran Kamrava, ed., *The International Politics of the Persian Gulf* (New York: Syracuse University Press, 2011), 225.
105. U.S.–China Economic and Security Review Commission (USCC), *China's Navy Extends Its Combat Reach to the Indian Ocean* (Washington, DC: USCC, 2014), http://origin.www.uscc.gov/sites/default/files/Research/Staff%20Report_China's%20Navy%20Extends%20its%20Combat%20Reach%20to%20the%20Indian%20Ocean.pdf.
106. Benjamin David Baker, "Revealed: Why China Is Selling Submarines to Pakistan," *Diplomat,* 28 September 2015, http://thediplomat.com/2015/09/revealed-why-china-is-selling-submarines-to-pakistan/.
107. Franz-Stefan Gady, "India Cleared Purchase of Russian S-400 Missile Defense System," *Diplomat,* 21 December 2015, http://thediplomat.com/2015/12/india-cleared-purchase-of-russian-s-400-missile-defense-system/.
108. Sandeep Unnithan, "The INS Vikramaditya's China Connection," *India Today,* 15 November 2015, http://indiatoday.intoday.in/story/the-ins-vikramadityas-china-connection/1

/325050.html; and Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, 2015), http://news.usni.org/wp-content/uploads/2015/08/RL33153_4.pdf.

109. Andrew S. Erickson, "China's Main Mission: South China Sea, Not Syria," *National Interest*, 5 October 2015, http://nationalinterest.org/feature/chinas-main-mission-south-china-sea-not-syria-14012; Minnie Chan, "Chinese Aircraft Carrier Liaoning Takes Up Role in South China Sea," *South China Morning Post* (Hong Kong), 30 November 2013, http://www.scmp.com/news/china/article/1368597/chinese-aircraft-carrier-liaoning-takes-role-south-china-sea; and Press Trust of India, "China to Deploy Range of Naval Ships in Indian Ocean," *Economic Times,* 29 January 2015, http://articles.economictimes.indiatimes.com/2015-01-29/news/58586257_1_escort-missions-naval-ships-indian-ocean.

110. Wendell Minnick, "China Building Its First Chinese Designed Aircraft Carrier—'It Means that the PLA and the Party Are Serious About Operating Carrier Battle Groups'," *Navy Times*, 27 January 2014.

111. "Aircraft Carrier Project Phase 2—New Construction," Global Security.org, 14 January 2016, http://www.globalsecurity.org/military/world/china/cv-phase-2.htm; Shannon Tiezzi, "Of Course China Is Building More Aircraft Carriers," *Diplomat*, 3 February 2015, http://thediplomat.com/2015/02/of-course-china-is-building-more-aircraft-carriers/; and Jethro Mullen and Shen Lu, "China Says It's Building New Homegrown Aircraft Carrier," CNN News, 1 January 2016, http://www.cnn.com/2015/12/31/asia/china-new-aircraft-carrier/.

112. Wendell Minnick, "Experts: Chinese '4th Fleet' Appears Unlikely," *Defense News,* 6 February 2015, http://www.defensenews.com/story/defense/naval/navy/2015/02/06/taiwan/22913337/; Franz-Stefan Gady, "China's Ghost Fleet in the Indian Ocean," *Diplomat,* 7 February 2015, http://thediplomat.com/2015/02/chinas-ghost-fleet-in-the-indian-ocean/; and Sam LaGrone, "China's First Domestic Aircraft Carrier Almost Certainly under Construction," *U.S. Naval Institute (USNI) News*, 30 September 2015, http://news.usni.org/2015/09/30/chinas-first-domestic-aircraft-carrier-almost-certainly-under-construction.

113. Walter Hickey and Robert Johnson, "These Are the 20 Aircraft Carriers in Service Today," *Business Insider,* 9 August 2012, http://www.businessinsider.com/the-20-in-service-aircraft-carriers-patrolling-the-world-today-2012-8; and Jeremy Bender, "This Is America's New $13 Billion Warship," *Business Insider*, 22 June 2015, http://www.businessinsider.com/this-is-the-us-new-13-billion-warship-2015-6.

114. "The Carrier Debate: From 1922 to Now," *USNI News,* 27 June 2013, http://news.usni.org/2013/06/27/the-carrier-debate-from-1922-to-now; David W. Wise, "The U.S. Navy's Big Mistake—Building Tons of Supercarriers," *War is Boring* (blog), 27 May 2015, https://medium.com/war-is-boring/the-u-s-navy-s-big-mistake-building-tons-of-supercarriers-79cb42029b8#.wa43kk1fl; and Joseph Trevithick, "This Could 'Sink' the U.S. Navy's New Aircraft Carriers (And It's Not China)," *The Buzz* (blog), *National Interest*, 3 October 2015, http://nationalinterest.org/blog/the-buzz/could-sink-the-us-navys-new-aircraft-carriers-it's-not-china-14007.

115. "Report: Chinese Develop Special 'Kill Weapon' to Destroy U.S. Aircraft Carriers," U.S. Naval Institute, 31 March 2009, http://www.usni.org/news-and-features/chinese-kill-weapon; and Peter Hartcher, "U.S. Panic at China's New Ship Killer," *Sydney Morning Herald*, 29 September 2009, http://www.smh.com.au/federal-politics/political-opinion/us-panic-at-chinas-new-ship-killer-20090928-g95b.html.

116. David Cenciotti, "Photo of India's New Aircraft Carrier Battle Group. Better Than China's?," *The Aviationist* (blog), 6 January 2014, http://theaviationist.com/2014/01/06/indian-navy-aircraft-carriers/.

117. Due to budgetary constraints, it is projected that the U.S. Navy will have to cut the number of battle-ready carriers in half. See David Axe, "The Navy Is Dropping Down to Just Two Deployed Carriers," *War is Boring* (blog), 24 January 2014, https://medium.com/war-is-boring/the-navy-is-dropping-down-to-just-two-deployed-carriers

-fb63ed05551a#.llzs6tgno. Other authors point to maintenance issues. See Megan Eckstein, "Navy: Half the Carrier Fleet Tied Up in Maintenance, Other 5 Strained to Meet Demands," *USNI News*, 4 November 2015, http://news.usni.org/2015/11/04/navy-half-the-carrier-fleet-tied-up-in-maintenance-other-5-strained-to-meet-demands.

118. Sam LaGrone, "French Carrier to Deploy to Indian Ocean, Could Join ISIS Fight," *USNI News*, 7 January 2015, http://news.usni.org/2015/01/07/french-carrier-deploy-indian-ocean-join-isis-fight; and "Trends Containing 'The French Aircraft Carrier Charles de Gaulle," Trendolizer, http://syria.trendolizer.com/trend/The%20French%20aircraft%20carrier%20Charles%20de%20Gaulle.

119. Thomas Erdbrink, "Iran Prepares Bill to Bar Foreign Warships from Persian Gulf," *Washington Post*, 4 January 2012, https://www.washingtonpost.com/world/middle_east/iran-prepares-bill-to-bar-foreign-warships-from-persian-gulf/2012/01/04/gIQAhlWYaP_print.html; and Phil Stewart, "U.S. Military Moves Carriers, Denies Iran Link," Reuters, 11 January 2012, http://www.reuters.com/article/us-usa-iran-military-idUSTRE80A29L20120112. Also see David Blair, "Britain, U.S. and France Send Warships through Strait of Hormuz," *Telegraph* (London), 23 January 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9031392/Britain-US-and-France-send-warships-through-Strait-of-Hormuz.html; Jeremy Herb, "Iran Restarts Threats over Closing Strait of Hormuz," *The Hill* (Washington, DC), 16 July 2012, http://thehill.com/policy/defense/238061-iran-restarts-threats-over-closing-straight-of-hormuz; Kenneth Katzman et al., *Iran's Threat to the Strait of Hormuz* (Washington, DC: Congressional Research Service, 2012), https://www.fas.org/sgp/crs/mideast/R42335.pdf; *Good News,* "Closing the Strait of Hormuz: A Serious Iranian Threat," *Beyond Today*, 1 May 2012, http://www.ucg.org/the-good-news/closing-the-strait-of-hormuz-a-serious-iranian-threat; "Iran Renews Hormuz Closure Threats," Reuters, 16 July 2012, http://www.reuters.com/article/us-iran-hormuz-idUSBRE86E0CN20120716; "Iran Ramps Up Warning to U.S. over Strait of Hormuz," *Telegraph* (London), 5 January 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8992227/Iran-ramps-up-warning-to-US-over-Strait-of-Hormuz.html.

120. David Brewster, "China's First Overseas Military Base in Dijibouti Likely to Be a Taste of Things to Come," *Interpreter*, 2 December 2015, http://www.lowyinterpreter.org/post/2015/12/02/Chinas-first-overseas-military-base-in-Djibouti-likely-to-be-a-taste-of-things-to-come.aspx.

121. Ibid.

122. China is taking the example from present day rapid reaction forces maintained by NATO and the U.S. DOD (USCENTCOM). The origins of the former Rapid Deployment Joint Task Force may be traced back to Presidential Directive (PD) 18 on national strategy, which was issued by President Jimmy Carter in 1977.

123. Brewster, "China's First Overseas Military Base."

124. Defence Videos, "Defending US Aircraft Carriers Against DF-21 'Carrier-Killer' Missiles," YouTube video, 0:45, 13 November 2013, https://www.youtube.com/watch?v=owpdX7RZqYA.

125. Meghann Myers, "SECNAV: F-35C Should Be Navy's Last Manned Strike Jet," *Navy Times*, 16 April 2015, http://www.navytimes.com/story/military/2015/04/16/navy-secretary-ray-mabus-joint-strike-fighter-f-35-unmanned/25832745/.

126. The Micro Air Vehicle (MAC) called the "WASP" by the military is in the forefront of UAV development.

127. Manu Pubby, "Government Approves $400-Million Plan to Procure Armed Heron TP Drones from Israel," *Economic Times*, 11 September 2015, http://economictimes.indiatimes.com/news/defence/government-approves-400-million-plan-to-procure-armed-heron-tp-drones-from-israel/articleshow/48906195.cms; and "Pakistan Successfully Tests First Indigenous Armed Drone: ISPR," *Express Tribune* (Karachi), 13 March 2015, http://tribune.com.pk/story/852698/pakistan-successfully-test-fires-first-indigenous-drone-ispr/.

Can Refugees Be National Security Assets?
Afghan American Contributions to U.S. National Defense since 1978

John Baden

Abstract. This article examines historical contributions of U.S. Afghans to U.S. foreign policy, especially since 11 September 2001. Since then, U.S. Afghans have served as interpreters, analysts, language instructors, and cultural advisors for the U.S. government and military. Most Afghans came to the United States since 1978, after war broke out in Afghanistan and created one of the world's worst refugee crises. This history suggests that if done properly, refugee policy can be both humane and add to the country's defense.

Keywords: Afghan Americans, Afghan immigrants, Afghan refugees, refugees, refugee crisis, special immigrant visas, SIV, U.S. interpreters, Marine interpreters, Cold War, War in Afghanistan, U.S. Marine Corps, immigrant history, Afghan American studies, Afghan American history

Since the summer of 2015, the United States has struggled with its response to the broader Middle East refugee crisis, a predicament exacerbated by the polarized political climate of the 2016 presidential election. What has often been lost on both sides of the debate, however, is that refugees of Islamic-world heritage have made innumerable contributions to U.S. national security. The linguistic skill and cultural acumen of Islamic-world refugees have played critical roles facilitating diplomacy and countering threats to the United States. These efforts extend back to the Cold War era but have been especially vital since

John Baden, a history doctoral candidate at Case Western Reserve University, is currently writing a dissertation that examines immigrant communities' roles in U.S. foreign relations. It focuses on Afghans in the United States and their relations and interactions with Afghanistan since 1978.

MCU Journal vol. 7, no. 1
Spring 2016
www.mcu.usmc.mil/mcu_press
DOI:10.21140/mcuj.2016070104

the Global War on Terrorism began in 2001. Thus, refugee policy should not be based on security concerns versus humanitarian objectives. If done properly, refugee policy can be humane and add to the country's defense.

U.S. Afghan communities' histories exemplify the importance of refugees to the United States' defense and foreign policy. Afghans first arrived in the United States in large numbers during the 1980s, largely as refugees from war and political persecution by government authorities. Some Afghan immigrants contributed to U.S. efforts to counter the Soviet-backed Afghan government, but most had to focus on rebuilding their lives during that decade. As Afghans who relocated to the United States adjusted to their new lives, many were economically successful. After the events of 11 September 2001, Afghans in the United States have served as interpreters, analysts, language instructors, and cultural advisors. Others used the economic and social capital they accumulated in the United States to aid the reconstruction of Afghanistan.

The process of granting refugee status has long been politicized. Although policy makers found admissions useful to foreign policy objectives, such policies have historically been unpopular among the general public.[1] Prior to the passage of the 1965 Immigration and Nationality Act, immigration quotas largely restricted immigration from areas outside of northwestern Europe. Therefore, exceptions had to be made for refugees to be admitted to the United States. As a result, modern refugee policy was generally limited and crafted largely for the benefit of U.S. foreign policy objectives during the Cold War.[2] Refugee visas were generally given out on an ad hoc basis after crises in Communist-controlled countries. This allowed the United States to essentially save face after being accused of abandoning countries such as Hungary after the thwarted revolution in 1956 and South Vietnam after the fall of Saigon in 1975. The Refugee Act of 1980 somewhat standardized the process and criteria for requesting asylum. This act along with the 1965 Immigration and Nationality Act allowed people from all over the world to immigrate to the United States. Despite the acts, refugee admissions remained heavily politicized, and American presidents still set refugee limits from a country and could admit additional people from conflict zones that were not granted asylum.[3]

Equally valuable to U.S. foreign policy, refugee visas facilitated the entry of thousands of anti-Communists with the valuable linguistic skills needed to carry out the U.S. Cold War mission as well as those who were defectors from U.S. adversaries. Demonstrating the importance of refugee admissions to Cold War foreign policy, the Central Intelligence Agency's original charter allowed its director, the attorney general, and the head of the Immigration and Naturalization Service (INS) to override immigration laws to allow as many as a hundred people of his or her choosing to permanently relocate to the United States each year in the "interest of national security" or "the national intelligence mission."[4]

This Cold War history of government action to circumvent immigration limits for refugees demonstrates that humanitarianism was not the only reason refugees were given asylum in the United States: the U.S. government recognized the importance of refugees and felt it was in the national interest to allow for an allotment of refugees. It was in this late–Cold War atmosphere that Afghans first came to the United States in large numbers.

This exodus out of Afghanistan began in 1978 after a coup installed a Marxist-Leninist government. Rebellions broke out against the new Afghan government, and the Soviet Union deployed its army in 1979 to ensure that the government, there remained a Soviet-allied, Marxist-Leninist one. The years following the coup and subsequent Soviet intervention were violent and destabilizing. Employees of previous regimes, intellectuals, and notable public figures were particularly vulnerable to the mass arrests and executions perpetrated by the Soviet-backed government. As a result, millions fled to neighboring Pakistan and Iran. In 1980, President James E. "Jimmy" Carter granted extended voluntary departure for Afghan refugees, making it easier for them to come to America. By 1990, 28,444 Afghans made their way to the United States.[5]

The Afghan refugee crisis soon became a global news story that was a public relations disaster for the Soviet Union's international image. Although many U.S. officials appear to have felt genuine sympathy for the refugees, they also recognized the political importance of the refugee crisis for their efforts to discredit the Soviet Union. In 1982, President Ronald W. Reagan declared 21 March (Persian New Year) as Afghanistan Day. After the president signed the proclamation, an Afghan student in the United States took the stage telling the audience that she had "witnessed the killing of my friends . . . and we [Afghans] will continue our war," before giving Reagan an Afghan flag.[6] During his speech, Reagan cast the Afghan struggle in the broader Cold War context: "The Afghans, like the Poles, wish nothing more, as you've just been so eloquently told, than to live their lives in peace, to practice their religion in freedom, and to exercise their right to self-determination."[7] A number of newspaper editors around the world then published the image of the president hugging the Afghan student.[8]

Ronald Reagan was not the only one in the U.S. government who recognized the symbolic importance of Afghan refugees to the U.S. Cold War mission. On 5 December 1985, the Associated Press reported that "more than 70 members of Congress, citing the U.S. image as 'a refuge for the oppressed,' urged the Reagan administration yesterday to grant political asylum to 33 Afghans detained by immigration authorities in New York."[9] The congressmen noted that "when a small number of the individuals who have fought the Soviet occupation show up on our shores, we treat them with contempt by jailing them for an indefinite period of time."[10] In a similar situation, Democratic Congressman Fortney H. Stark Jr., who represented the Oakland suburbs, home to the nation's largest

Afghan population, wrote on behalf of Afghan refugees facing deportation for not having proper visas.[11] Writing to White House Congressional Liaison Kenneth M. Duberstein, Congressman Stark advocated for the refugees by going around the INS. He wrote, "I am sending this directly to you rather than making inquiries at INS, since I suspect that INS is processing according to the rulebook—but the net effect may not be in accordance with the President's view."[12] The congressman continued, "I hope you can take a look at this file [which contained newspaper clippings and nongovernmental organization (NGO) appeals] to see whether INS shouldn't be less zealous in this case."[13] Additionally, in a request apparently unrelated to Stark's, a writer only identified by the name "Steve" asked officials at the Office of Policy Development to "please take a look" at the case of the Afghans in California facing deportation. In this internal White House memo, Steve recommended to the office's William Barr that "we should find out if INS is still taking a hard line against Afghan refugees, and help out if possible."[14] It appears unlikely that the White House did intervene, but the Afghans did win the right to stay in the United States.[15] Although White House intervention probably did not materialize, the case demonstrates that high-level members of the U.S. government recognized the importance of refugee policy to their broader Cold War objections.

It is difficult to discern how most U.S. Afghans felt about the politicization of their situation, although nearly all Afghan Americans who published memoirs and oral histories spoke negatively about the Communist-inspired, nominally Afghan government.[16] Resentment of the Afghan government and its Soviet allies led to the desire of a number of Afghan immigrants to support the U.S. Cold War mission, regardless of whether they took active roles. The work provided income, a chance to contribute to the United States, and a means to subvert the Marxist-Leninist regime in Afghanistan.

Shukria Raad was one person who took the United States up on its offer to contribute her skills for its benefit and became a key figure in the Voice of America (VOA) Dari language broadcasting service. She left Afghanistan in December 1979 because the Communists took over her employer's operation, Radio Afghanistan.[17] By 1982, she was broadcasting in Dari to Afghanistan on VOA, trying to counter the Soviet-backed accounts of the news.[18] Another Afghan who fled to the United States after the invasion, Spozhmai Maiwandi was perhaps the central figure in VOA's Pashto service into the early 2000s.

After the Soviet-backed government in Afghanistan collapsed in 1992, Afghanistan fell off the radar of most U.S. policy makers. As the country disintegrated into civil war, it was also more difficult for Afghans in America to travel to their home country, rally behind a common political cause, or imagine a permanent return. A number of Afghans in the United States, however, did manage to establish a number of nongovernment organizations to perform charitable work

during the decade. Although the population of people of Afghan descent born in the United States rose from 28,444 to 45,195 during the 1990s, many Afghans in the United States became more disconnected from Afghanistan's politics and changes.[19]

Then on 11 September 2001, Afghan Americans' relationship with Afghanistan dramatically changed. Suddenly, the country, which had become virtually inaccessible and had its news buried in U.S. newspapers, was front and center. The nonstop media coverage of the attacks and al-Qaeda perpetrators with Afghanistan connections forced Americans—Afghan or otherwise—to face the presence of this place that before had seemed so remote. Like every community, there have been debates and differing views on the proper U.S. response to these events. Many chose to directly support the United States or to help rebuild Afghanistan and have made invaluable contributions to those efforts.

Dr. Obaid Younossi of the Rand Corporation was at work across from the Pentagon on 9/11. That morning, he witnessed hijacked American Airlines Flight 73 fly over his office window just before it crashed into the Pentagon. After returning home, Younossi sensed a change within himself. Afghanistan was a country he had left long ago and had emotionally detached from. Now, Afghanistan was suddenly on the front page of newspapers, with places mentioned that he had known growing up.[20] Younossi recalled being overcome with emotion, trying to be a "good American" while also empathizing with Afghans facing troubling times. He wanted to help. Younossi decided the best route for himself and his family was to look for Afghanistan assignments within the Rand Corporation. He worked on projects involving security and reforming the Afghan National Army, and this work took him to Afghanistan multiple times from 2005 to 2011.

Like Younossi, many Afghan Americans shared a similar desire to help after 9/11. The United States was now at war with the Taliban and al-Qaeda insurgents in Afghanistan and needed people with linguistic and cultural knowledge to facilitate U.S. efforts in the country. For example, the Leader Development and Education for Sustained Peace Program delivered programs for the U.S. military by contracting Afghan American experts to give talks to officers about Afghan culture, politics, and history before deployment.[21] Afghan Americans employed at San Diego State University's Afghanistan Language and Culture Program also produced online cultural and political lessons for the U.S. Marine Corps. To prepare Marines, other Afghans participated in role-playing exercises in mock Afghan villages at infantry immersion trainer locations, such as Camp Pendleton in California. Such training settings helped prepare U.S. personnel to handle situations in Afghanistan by providing them with cultural awareness to minimize unnecessary conflict with local Afghans.[22]

Afghan Americans have been especially valuable as linguists and interpreters. Most of the United States' interpreters in Afghanistan were non-U.S. residents

living in the region. Jobs that required secret or top secret clearance, however, had to be filled by U.S. citizens.[23] According to a spokesperson for Mission Essential Personnel, the contractor employing the predominant share of linguists for the United States in Afghanistan, 1,080 of their 6,896 linguists were from the United States in October 2012.[24] It appears that nearly all of these positions were filled by Afghan Americans or other Americans of Islamic-world heritage. Moreover, Afghan Americans and other immigrants from Islamic majority countries have played a key role in building the military's language capabilities by serving as language instructors, either directly teaching military personnel at institutions like the Defense Language Institute in Monterey, California, or teaching language courses classes attended by students with ROTC Global Officers.[25]

Their work was vital to the U.S. mission when few other people in the United States were qualified. In 2010, the U.S. government was in such dire need of qualified applicants that defense contractors sponsored an Afghan American soccer tournament in the Washington, DC, area to advertise their job openings. The soccer field's fences were heavily adorned with large advertisements informing attendees that they could earn "$210K a year" as linguists.[26] One defense company even went as far as handing out 500 T-shirts that read in Pashtu, "If you can read this, we might have a job for you." Meanwhile, that year's television advertisements directed at Afghan Americans urged qualified individuals to serve with the U.S. agencies in Afghanistan, "For America, For Afghanistan, For Me."[27]

Fahim Fazli took the call to service seriously. After watching television one night, he saw an advertisement to be a linguist and wondered, "With my gift for languages, might there be something extra I could do for America—beyond just paying taxes? Could I simultaneously help both my new country and my old?"[28] He had come to the United States from Afghanistan during that country's refugee crisis in the 1980s.[29] When his family became separated during the Afghan–Soviet War of the 1980s, he fled with his father and brothers to Pakistan. There the U.S. embassy and its Marine Corps guards helped locate his mother who had fled to the United States. With additional help from a Christian charity, Fazli was reunited with his family in the United States in 1985 at the age of 18. For the next two decades, Fazli worked various jobs before finding success as an actor. Ironically, Fazli almost exclusively played terrorists in films and on television. By 2009, his acting career had picked up, but he felt it was his time to give back to his adopted country as well as helping his country of birth. He signed up to be an interpreter for the U.S. military. After completing preliminary training at Fort Benning in Georgia, Fazli volunteered to join the U.S. Marines Corps as an interpreter despite knowing that this branch was the most likely to face combat.[30] Fazli served as an interpreter for 3d Battalion, 4th Marine Regiment, in Helmand Province from October 2009 to July 2010. Recognizing his value, Captain Ryan Benson wrote of Fazli's service, "Fahim operated alongside the Marines of India Company facing

the same dangers and hardships they faced. . . . He has become a brother not just to me, but to each of the Marines under my charge."[31]

U.S. Afghan women have also served as interpreters in specially trained female engagement teams (FET). These military units have often been the only U.S. personnel interacting with Afghan women due to cultural prohibitions against Afghan women talking to men.[32] As a result, they have been vital for both tracking insurgents and facilitating local development projects. Afghan American women have been among the few to qualify for such work because of the scarcity of Pashtu speakers in America and U.S. residency requirements. Nadia Sultan was one interpreter for a U.S. Army FET. As recounted by author Gayle Tzemach Lemmon, Sultan "was energized by the idea that she could make good money doing a job she believed in while also serving the nation that had given refuge to her own family when it was too dangerous to stay in Kandahar."[33] Sultan worked in Afghanistan from summer of 2009 to 2011 at Bagram Air Base before transferring to an FET.[34] In 2011, Sultan was seriously wounded in an IED explosion that killed her FET leader and two servicemembers.

Outside of U.S. government employment, Afghan Americans have been crucial to building educational institutions in Afghanistan and helping with the country's reconstruction. Afghan Americans founded NGOs such as Afghan Friends Network, the Children of War, Help the Afghan Children, and the Khaled Hosseini Foundation; established schools; and sponsored education for Afghans. Other organizations, such as Afghans 4 Tomorrow and Society of Afghan Engineers, have focused on health, infrastructure, agriculture, training, and building standards, as well as education.[35] Since Afghanistan's government has limited capacity to help its citizens, nonprofits funded and ran by members of the Afghan diaspora have played a critical role supporting the country's infrastructure and educational system. These contributions promote an independent and stabile Afghanistan that can stand on its own.

Humaira Ghilzai, who had been director of international marketing at Sun Microsystem's software division and Oracle, was one Afghan American who cofounded a nonprofit organization after 9/11. She recalled her disconnection from her Afghan identity prior to the tragic events of that day explaining that "from the time I went to college until 9/11 happened I had no direct connection with the Afghan community, Afghan people, Afghanistan. I really did not know what was going on there. . . . The Russians left, the Mujahideen came, the Taliban took over and I was oblivious to all."[36] When Ghilzai gave her name after the 9/11 attacks, people would ask where she was from, and with that said, her "carefully built . . . nice American persona" suddenly collapsed. Her father pushed her to try and help Afghanistan since the country was once again accessible, and survivor's guilt affected her deeply. She now refers to herself as a "born-again Afghan."[37] After becoming involved in small projects, she cofounded the Afghan Friends

Network. Since 2002, the Afghan Friends Network has provided funding for the education of hundreds of Afghans in Ghazni Province as well as scholarships incentivizing students to attend college in Afghanistan. Afghan Friends Network's educational curriculum includes a gender equality program taught to 500 girls, 250 boys, and 80 women by religious leaders.[38] Only about 17 percent of Afghan women and 31 percent of Afghans overall are literate. The Afghan Friends Network and similar organizations make valuable contributions to education and gender equality—two of the most promising avenues for expanding opportunity to Afghans.[39]

Despite significant contributions from refugee communities, such as those of the Afghans, the fear of terrorist infiltration has made many people uneasy about allowing refugees from Islamic-majority countries into the United States. Terrorism is indeed a significant international problem, and safeguards will need to be implemented in the United States to prevent admitting extremists with violent ambitions from around the world. Yet most people do not understand how rare these attacks have been, and the role Muslims and refugees from the Islamic world have played in preventing them. It is true that a small number of people in the United States from Islamic-majority countries have committed acts of terror against the United States. Two Afghan Americans, in fact, were arrested for plotting to attack New York's subway system.[40] The 2015 attack in San Bernardino, California, was inspired by the Islamic State of Iraq and the Levant (ISIL) terrorist organization, but the attackers were not Afghan. Such acts are inexcusable, but perspective on violence and mass killing is needed. Attacks from international terrorist organizations, such as al-Qaeda and ISIL, gather much of the media's focus, but are extremely rare thanks in no small part to Muslim American communities.

After 11 September 2001, there were approximately 147,000 murders in the United States from 2002 to 2010, but only 33 deaths came as a result of Muslim American acts of terrorism.[41] The role of anti-Muslim xenophobia becomes more apparent considering that two white shooters acting independently in Tucson, Arizona (2011), and in Sandy Hook, Connecticut (2012), took nearly the same number of lives in their two acts alone. Sadly, the 2015 San Bernardino shootings added to this tally of deaths by Muslim American terrorists, but it took place alongside numerous other mass shootings in that year that were perpetrated by white, often nonreligious-based, shooters. In fact, it appears that since 9/11, more deaths have been attributed to U.S. Far-Right–wing terrorism than Muslim American terrorism.[42]

People of all religious affiliations and ethnic groups in the United States perpetrate violence, and it appears that only a small portion of it comes from Islamic-world refugees. These statistics are similar to the data on attacks in Europe, which show that jihadist-affiliated terrorist groups garner the most attention

but account for minor contributions to the overall violence, even after the tragic 2015 attacks on Paris. From 2001 to 2014, only two attacks by Islamic-extremist affiliated terrorist organizations in Western Europe killed more than 10 people.[43] Homicide statistics are still difficult to obtain for 2015, but in 2012 there were a combined 2,989 homicides in Austria, Belgium, France, Germany, Italy, Spain, the Netherlands, and the United Kingdom. Out of these, only 17 people died from terrorist attacks (not just Islamist-extremist affiliated ones) in the entire European Union.[44] Although the 2015 Paris attacks were horrific, the continent's worst mass killing that year came when a white Germanwings company copilot crashed an airliner, apparently deliberately, into the Alps with 150 passengers onboard.[45]

Some critics have claimed that Muslims are reluctant to condemn terrorism, but in reality nearly every major U.S. Muslim organization has condemned terrorism in general and such groups as ISIL and al-Qaeda specifically.[46] While it is true that a minority of people living in Muslim-majority countries have indicated in polls that terrorism can be justified in some cases, the results have varied considerably and have seldom been compared to views from non-Muslim countries. A 2009–10 Gallup poll indicates that respondents from countries that are Organisation of Islamic Cooperation members were slightly less likely to support violence against civilians than respondents from other countries. For example, 22 percent of Americans and 15 percent of Canadians believe that "individual [implying nonmilitary] attacks on civilians are sometimes justified," while 18 percent of respondents from Organisation of Islamic Cooperation countries expressed this view.[47] These findings substantiate the results of an earlier poll conducted by the University of Maryland in 2006.[48] Whereas respondents from Muslim-majority countries, such as Indonesia, Pakistan, and Nigeria, had lower numbers polled and lower acceptance of attacks against civilians.[49]

Terrorist attacks perpetuated by U.S. Muslims in the United States have been rare, and the U.S. Muslim community has been vital to keeping these numbers low. For cases in which data exists, officials cite Muslim Americans as the source of 40 percent of all initial tips disrupting terror plots attempted by Muslim Americans in the United States from 12 September 2001 to 2010.[50] If national security is used as a justification for immigrant and refugee exclusion, security concerns should also be a reason for allowing more immigrants and refugees from the Islamic world to immigrate to the United States. Moreover, international terrorists can attempt to enter the country through temporary tourist, student, or work visas regardless of U.S. immigrant and refugee policies. Recent experiences suggest, however, that Muslim Americans, as well as refugees from Muslim-majority countries, can be among the most effective at combatting terrorism.

Allowing refugees from the Islamic world into the United States has taken on a special importance recently because of U.S. involvement in Afghanistan and Iraq. As U.S. troops have withdrawn, local personnel working for the United

States have been left vulnerable to reprisals by insurgents. As in past conflicts, such as those in Vietnam and Cuba, many U.S. policy makers and veterans believe that leaving U.S. allies vulnerable to reprisal threatens American honor and international credibility. Despite congressional legislation providing special immigrant visas for personnel who completed their work in good standing, the process has been mired in bureaucratic missteps and red tape. The *Washington Post* reported that, in 2012, the State Department awarded "just 32 visas for more than 5,700 Afghan applications."[51] Although improvements have been made to the Special Immigrant Visa (SIV) program, thousands of former U.S. employees remain stranded in Afghanistan.[52] Inaction could adversely affect the United States' ability to hire personnel to perform vital work and convince Afghans that they have their best interests in mind.

Former interpreter Sami Khazikani's experience highlights the dangers former U.S. personnel have faced in recent years. He had been forced to leave Afghanistan after his in-laws learned of his service to the U.S. Marines and received death threats. Khazikani had applied for a SIV from the United States, but still had not received it; the visa appeared to be stuck in the application process. He and his family fled to Turkey and, after being told to leave by officials, then sailed to Greece. During the journey, his boat nearly sank in the Mediterranean while other nearby boats succumbed to the sea. After arriving in Greece, Khazikani and his wife and daughter lived on the streets of Athens before trekking on foot to the Hungarian border. As of this writing, Khazikani is living in a German refugee camp with his wife and daughter.[53] Unfortunately, Khazikani is not alone in his predicament. In 2014, approximately 6,000 Afghans were stuck in the SIV application process, and visa advocates argue that in 2015 thousands of former U.S. personnel, such as Sami Khazikani, were attempting to make it into Europe as refugees.[54]

Many Americans have shown their support for former interpreters and refugees, and U.S. veterans have been at the forefront of these efforts.[55] After seeing coverage of the developing refugee crisis in September 2015, former Marine Sergeant Aaron E. Fleming personally contacted the interpreter with whom he worked, the aforementioned Sami Khazikani. Fleming learned through social media that Khazikani and his family were refugees in Greece. Fleming took action and formed a team to launch an online fundraising campaign to help his former interpreter. One of those who helped Fleming raise funds for Khazikani, Gunnery Sergeant Emir Hadzic, was once a Muslim refugee from Bosnia who served in Afghanistan alongside Khazikani. Hadzic had joined the Marines "hoping to pay my debt to America," when the United States began sending peacekeepers to Bosnia and made a long-term commitment after 9/11.[56]

In 2013, Afghanistan veteran Matthew Zeller learned that his former interpreter, Mohammad Janis Shinwari, was receiving death threats in Afghanistan and

was unable to escape the country. After waiting two years, Shinwari received a U.S. visa, but the U.S. government revoked it shortly thereafter.[57] Shinwari had saved Zeller's life twice in Afghanistan, and Zeller felt he owed Shinwari. Zeller lobbied the State Department and Congress on Shinwari's behalf. Due in part to Zeller's efforts, Shinwari had his visa reinstated and moved to the United States with his family. Once in America, Shinwari and Zeller founded No One Left Behind, an organization that helps former interpreters in Afghanistan and Iraq resettle in the United States.[58] The efforts of former servicemembers and nonprofits suggest that the U.S. government's approach to its former Afghan interpreters is severely lacking. Qualified interpreters have already served the United States and could continue to do so on American soil.

Since the 1980s, Afghan refugees were given the chance to rebuild their lives in the United States, and many have made significant contributions to securing their adopted home. Today, millions of displaced people from such locations as Syria, Libya, Iran, and Pakistan long for the ability to pursue economic opportunity and live in the relative safety that life in the United States can provide. The U.S. government is neither going to take in every refugee nor is every refugee admitted into the United States going to agree with all U.S. foreign policy. Any significant number of refugee admissions, however, goes a long way to assure the world of U.S. intentions and values. Refugees' successes in the United States counter extremists' hostile portrayals of America and offer a positive example of the country's best values of inclusion and opportunity. As the United States has witnessed in Afghanistan, distant refugee and "failed state" crises of today may unfortunately become the U.S. battlefields of tomorrow. If that is the case, the United States will need people who understand the cultures and dialects of the region. It would be unwise to solely admit refugees on the expectation of service for U.S. security. Yet, former refugees—including Obaid Younossi, Fahim Fazli, Humaira Ghilzai, Nadia Sultan, and countless others—have made the United States more innovative, skilled, and safe. Our recent history suggests that many of today's refugees will do the same.

Notes

1. For historical polls on refugee admissions, see Frank Newport, "Historical Review: Americans' Views on Refugees Coming to U.S.," Gallup, 19 November 2015, http://www.gallup.com/opinion/polling-matters/186716/historic-review-americans-views-refugees-coming.aspx.
2. Prior to immigration restrictions enacted in the late nineteenth century and the 1920s, there was little need for a refugee policy. Nearly anyone with the resources to come the United States was allowed to immigrate. After 1924, Congress effectively restricted immigration to the United States outside of northwestern Europe. See American Immigration Council (AIC), "An Overview of U.S. Refugee Law and Policy," AIC, 18 November 2015, http://www.immigrationpolicy.org/just-facts/refugees-fact-sheet.
3. For an extensive list of historical executive actions that facilitated immigration, especially refugees, see "Executive Grants of Temporary Immigration Relief 1956–Present," AIC,

October 2014, http://www.immigrationpolicy.org/sites/default/files/docs/executive_grants_of_temporary_immigration_relief_1956-present_final.pdf. For an overview of foreign policy and domestic politics concerns regarding refugee policy, see Carl J. Bon Tempo, *Americans at the Gate: The United States and Refugees During the Cold War* (Princeton, NJ: Princeton University Press, 2008).

4. Central Intelligence Agency Act of 1949, 50 U. S. C. §7 (2012), http://www.legcounsel.house.gov/Comps/CIA49.pdf. For their part, refugees in the United States courageously served in such government agencies as the Central Intelligence Agency (CIA) throughout the Cold War, often taking on shockingly high casualty rates. The CIA's attempted Bay of Pigs Invasion to overthrow Fidel Castro's regime is the most well-remembered incident, but countless refugees perished on U.S.-supported missions throughout the world. For more on refugee involvement in CIA operations, see Tim Weiner, *Legacy of Ashes: The History of the CIA* (New York: Doubleday, 2007).
5. Campbell Gibson and Emily Lennon, "Table 3. Region and Country or Area of Birth of the Foreign-Born Population: 1960 to 1990," U.S. Census Bureau, 9 March 1999, https://www.census.gov/population/www/documentation/twps0029/tab03.html?cssp=SERP.
6. United Press, "Afghan Gets Reagan Hug," Afghan Refugees, William Barr Files, 1982–1983, Ronald Reagan Presidential Library, Simi Valley, CA.
7. Ronald Reagan, "Remarks on Signing the Afghanistan Day Proclamation" (speech, White House, Washington, DC, 10 March 1982), American Presidency Project, http://www.presidency.ucsb.edu/ws/?pid=42248.
8. United Press, "Afghan Gets Reagan Hug."
9. Associated Press, "73 House Members Ask U.S. Asylum For Afghan Refugees," *San Francisco* (CA) *Chronicle*, 5 December 1985.
10. Ibid.
11. The *San Francisco Chronicle* reported that the district Immigration and Naturalization Service involved with the case's decision "indicated that they would not be returned to Afghanistan," but rather he intended to deport the individuals in question to another country. See Randy Shilts, "Afghans Face Ouster Ousted by U.S.," *San Francisco Chronicle*, 18 February 1982; and Congressman Fortney H. Stark Jr. to assistant to the President for congressional liaison Kenneth M. Duberstein, newspaper article, ID #079793, IM 079433-080097, WHORM: Immigration, box 7, Ronald Reagan Presidential Library.
12. Stark to Duberstein, 24 May 1982, ID #079793, IM 079433-080097, WHORM: Immigration, box 7, Ronald Reagan Presidential Library; "Steve" to William Barr, 31 May 1982, folder "Afghan Refugees (OA 9094)," William Barr Files, Ronald Reagan Presidential Library; and Bill Soiffer, "Judge Disregards Fake Visas: Afghan Refugees Can Stay," *San Francisco* (CA) *Chronicle,* 11 August 1982.
13. Ibid.
14. "Steve," to William Barr.
15. A response to Congressman Stark written by Alan C. Nelson, Immigration and Naturalization Services commissioner, offers no indication that the White House would intervene and only clarifies that "consistent with Administration policy, no Afghans are being returned to Afghanistan, given the conditions in that country," but that some could be returned to a "third country." Additionally, the statement reiterates that fake passports were used to enter the United States. See Alan C. Nelson to Congressman Fortney H. Stark Jr., 20 July 1982, ID #079793, IM 079433-080097, WHORM: Immigration, Ronald Reagan Presidential Library; and Soiffer, "Judge Disregards Fake Visas."
16. Examples of criticism of Soviet-backed government include Fahim Fazli, *Fahim Speaks: A Warrior-Actor's Odyssey from Afghanistan to Hollywood and Back*, with Michael Moffett (North Hills, CA: Warriors Publishing Group, 2013); Saima Wahab, *In My Father's Country: An Afghan Woman Defies Her Fate* (New York: Crown Publishers, 2012); Maryam Qudrat Aseel, *Torn Between Two Cultures: An Afghan-American Woman Speaks Out* (Herndon, VA: Capital Books, 2003); and Suraya Sadeed, *Forbidden Lessons in a Kabul Guesthouse: The True Story of a Woman Who Risked Everything to Bring Hope to Afghanistan*, with Damien Lewis, (New York: Hyperion, 2011).
17. Frank Ahrens, "Crackling Signals," *Washington Post*, 10 November 2001, https://www

.washingtonpost.com/archive/lifestyle/2001/11/10/crackling-signals/123cf76f-8b02-4168-ab50-a302db4dbe05/.

18. Analyzing the effectiveness of Cold War VOA broadcasts is outside the scope of this article. Obviously, progovernment forces in Afghanistan made attempts to jam the broadcasts, which often made it difficult for the United States to broadcast into Afghanistan. Still, VOA broadcasts were heard in Afghanistan, and Spozhmai Maiwandi reported receiving listener mail from people in Afghanistan. She listened to a VOA Dari broadcast the night before fleeing Kabul, Afghanistan. Spozhmai Maiwandi, interview by Mae McKernan and Shaista Wahab, 8 September 1983, Afghan Oral History Project, audiocassette, University Library, University of Nebraska at Omaha.
19. U.S. Census Bureau, "Table FBP-1. Profile of Selected Demographic and Social Characteristics: 2000, People Born in Afghanistan," http://www.census.gov/population/cen2000/stp-159/STP-159-afghanistan.pdf.
20. Obaid Younossi, telephone interview with the author, September 2015.
21. Robert Tomasovic, telephone interview with the author, September 2015.
22. Tony Perry, "Mock Afghan Village at Camp Pendleton Aims to Prepare Troops for Combat," *L.A. Now* (blog), *Los Angeles Times*, 16 November 2010, http://latimesblogs.latimes.com/lanow/2010/11/my-entry.html; and Carl Nasman, "Marines Get Crash Course in Afghan Culture in California Model Village," PBS NewsHour, 6 March 2012, http://www.pbs.org/newshour/bb/military-jan-june12-afghanvillage_03-06/.
23. Steve Wartenberg, "The Language of War," *Columbus* (OH) *Dispatch*, 8 November 2009, http://www.dispatch.com/content/stories/business/2009/11/08/Mission_Essential.ART_ART_11-08-09_D1_FCFIUBU.html.
24. Mission Essential Personnel's prominent role in providing linguists for the United States in Afghanistan can be seen in the fact that, as of January 2013, the office of the Deputy Assistant Secretary of Defense (Program Support) reported there were only 5,796 translator/interpreters in Afghanistan employed by U.S. Central Command (CENTCOM). Compare this with Mission Essential Personnel spokesman citing that 6,896 linguists worked on behalf of the U.S. government in October 2012. See Jesse Ellison, "As War Nears an End, Our Afghan Translators Are Being Left Behind," *Daily Beast*, 21 October 2012, http://www.thedailybeast.com/articles/2012/10/21/as-war-nears-an-end-our-afghan-translators-are-being-left-behind.html; and Office of the Deputy Assistant Secretary of Defense (DASD), *Contractor Support of U.S. Operations in the USCENTCOM Area of Responsibility to include Iraq and Afghanistan* (Washington, DC: DASD, 2013), http://www.acq.osd.mil/log/ps/.CENTCOM_reports.html/5A_Jan2013.doc.
25. While there are no widely available statistics for the percentage of foreign-born employees at such institutes as the Defense Language Institution, its website states that "applicants must have near native language proficiency in all skills." This suggests that one would probably be a native or heritage speaker of the language to receive the job. For information on the ROTC Global Officers program, see "FAQs," Project Go, http://www.rotcprojectgo.org/faqs.
26. Kevin Sieff, "At Afghan Cup in Virginia, Recruiters Offer Big Money for Interpreters," *Washington Post*, 11 July 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/10/AR2010071002922.html.
27. Ibid.
28. Fazli, *Fahim Speaks*, 114.
29. Ibid., 48–50.
30. Ibid., 114–16.
31. Capt Ryan P. Benson, "From Formal Evaluation of Fahim Fazli by Captain Ryan Benson, USMC," in Fazli, *Fahim Speaks*.
32. Sgt Christopher McCullough, "Female Engagement Teams: Who They Are and Why They Do It," U.S. Army, 2 October 2012, http://www.army.mil/article/88366/; Hope Hodge Seck, "Marine Corps Revives Female Engagement Team Mission," *Marine Corps Times*, 5 August 2015, http://www.marinecorpstimes.com/story/military/2015/08/05/marine-corps-revives-female-engagement-team-mission/30796519/; Regional Command Southwest Press Room (RC[SW]), "Female Engagement Team (USMC)," RC(SW), https://

regionalcommandsouthwest.wordpress.com/about/female-engagement-team-usmc/; and Gayle Tzemach Lemmon, *Ashley's War: The Untold Story of a Team of Women Soldiers on the Special Ops Battlefield* (New York: HarperCollins, 2015).

33. Tzemach Lemmon, *Ashley's War*, 172.
34. Ibid., 175.
35. For a discussion of these organizations and Afghan American remittances, see Shah Mahmoud Hanifi, "Material and Social Remittances to Afghanistan," in *Converting Migration Drains into Gains: Harnessing the Resources of Overseas Professionals*, ed. C. Wescott and J. Brinkerhoff (Manila, Philippines: Asian Development Bank, 2006).
36. Humaira Ghilzai, interview with the author, October 2015.
37. Ibid.
38. Afghan Friends Network (AFN), "Gender Equality Program" AFN, http://www.afghanfriends.net/gender-equality/; and Humaira Ghilzai, interview with the author.
39. Fisnik Abrashi, "Illiteracy Undermines Afghan Army," *Army Times*, 14 September 2009.
40. Tina Susman, "Bosnian Immigrant Gets Life Sentence in Plot to Blow up N.Y. Subways," *Los Angeles Times*, 16 November 2012, http://articles.latimes.com/2012/nov/16/nation/la-na-nn-ny-subway-plot-20121116.
41. Note that this statistic includes "murder and nonnegligent manslaughter." See FBI, "Table 1. Crime in the United States," https://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl01.xls; and Charles Kurzman, *Muslim-American Terrorism Since 9/11: An Accounting* (Chapel Hill, NC: Triangle Center on Terrorism and Homeland Security, 2011), http://kurzman.unc.edu/files/2011/06/Kurzman_Muslim-American_Terrorism_Since_911_An_Accounting.pdf.
42. Arie Perlinger categorized the "violent far right" as comprised by "a racist/white supremacy movement, an anti-federalist movement and a fundamentalist movement." See Arie Perliger, *Challengers from the Sidelines: Understanding America's Violent Far-Right* (West Point, NY: Combating Terrorism Center, U.S. Military Academy, 2012), 100, https://www.ctc.usma.edu/posts/challengers-from-the-sidelines-understanding-americas-violent-far-right; Charles Kurzman and David Schanzer, *Law Enforcement Assessment of the Violent Extremism Threat* (Chapel Hill, NC: Triangle Center on Terrorism and Homeland Security, 2015), https://sites.duke.edu/tcths/files/2013/06/Kurzman_Schanzer_Law_Enforcement_Assessment_of_the_Violent_Extremist_Threat_final.pdf.
43. "Daily Chart: Terror Attacks," *Economist* (London), 15 January 2015, http://www.economist.com/blogs/graphicdetail/2015/01/daily-chart-8.
44. See Eurostat, "Homicides Recorded by the Police, 2002–12," 3 June 2014, http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Homicides_recorded_by_the_police,_2002%E2%80%9312_YB14.png; and Europol, "Rise in Terrorist Attacks in Europe in 2012," 25 April 2013, https://www.europol.europa.eu/content/rise-terrorist-attacks-europe-2012.
45. "Germanwings Crash: Co-Pilot Lubitz 'Practised Rapid Descent'," BBC News, 6 May 2015, http://www.bbc.com/news/world-europe-32604552.
46. For pieces dealing with Muslim condemnation of terrorism, see Zafar Siddiqui, "American Muslim Organizations Condemn ISIS Terrorism," *Star Tribune* (Minneapolis, MN) (blog), 4 September 2014, http://www.startribune.com/american-muslim-organizations-condemn-isis-terrorism/273886931/; Sarah Parvini, "U.S. Muslims Ask Why Their Religion's Condemnation of Violence Often Goes Unheard," *Los Angeles Times*, 9 May 2015, http://www.latimes.com/nation/la-na-muslim-condemnation-20150509-story.html; and "Arab States Condemn 'Terrorist' Paris Attacks," *Al Arabiya*, 14 November 2015, http://ara.tv/bv6fx.
47. Abu Dhabi Gallup Center, "Views of Violence," Gallup, http://www.gallup.com/poll/157067/views-violence.aspx.
48. Kenneth Ballen, "The Myth of Muslim Support for Terror," *Christian Science Monitor*, 23 February 2007, http://www.csmonitor.com/2007/0223/p09s01-coop.html.
49. Ibid.
50. Kurzman, *Muslim-American Terrorism Since 9/11*.
51. Thomas Gibbons-Neff, "Afghan Interpreter Visa Program Expanded in a Rare Bipar-

tisan Vote," *Washington Post*, 1 August 2014, https://www.washingtonpost.com/news/checkpoint/wp/2014/08/01/afghan-interpreter-visa-program-expanded-in-a-rare-bipartisan-vote/.

52. Ibid.
53. Perry Chiaramonte, "'Don't Let Me Down:' Afghan Who Risked Life Helping U.S. Marines Dodges Death in European Refugee Wave," Fox News, 23 November 2015, http://www.foxnews.com/world/2015/11/23/dont-let-me-down-afghan-who-risked-life-helping-us-marines-dodges-death-in/; Aaron E. Fleming, "My Afghan Battle Partner Deserves a U.S. Visa," *Washington Post*, 27 November 2015, https://www.washingtonpost.com/opinions/my-afghan-battle-partner-deserves-a-us-visa/2015/11/27/98b00ab6-912d-11e5-a2d6-f57908580b1f_story.html; James LaPorta, "Afghan Interpreter Flees the Graveyard of Empires," *Jacksonville* (NC) *Daily News*, 26 November 2015, http://www.jdnews.com/article/20151126/NEWS/151129355/?Start=1; James LaPorta, "Former Afghan Interpreter Recalls Journey to Germany Following Death Threats," *Jacksonville* (NC) *Daily News*, 27 November 2015, http://www.jdnews.com/article/20151127/NEWS/151129250/0/SEARCH/?Start=1; Bill McMorris, "One Translator's Story," *Washington Free Beacon* (Arlington, VA), 10 September 2015, http://freebeacon.com/culture/one-translators-story/; and Bill McMorris, "Imperiled Marine Interpreter Reaches Austria," *Washington Free Beacon* (Arlington, VA), 14 September 2015, http://freebeacon.com/culture/imperiled-marine-interpreter-reaches-austria/.
54. Gibbons-Neff, "Afghan Interpreter Visa Program"; and Chiaramonte, "Don't Let Me Down."
55. Several online news sources have reported similar efforts by veterans on behalf of their former interpreters in addition to cases mentioned in this article. See for example, Jude Joffe-Block "Veterans in Phoenix Help Afghan Interpreter Settle into a New Life," Fronteras, 24 November 2015, http://www.fronterasdesk.org/content/10169/veterans-phoenix-help-afghan-interpreter-settle-new-life; and Paul Purpura, "With Help of a Local Marine, Afghan Interpreter Who Guided U.S. Troops Achieves Dream of Making It to America," *New Orleans* (LA) *Advocate*, 28 November 2015, http://www.theneworleansadvocate.com/news/14077483-32/with-help-of-a-local. For an example of articles written by former servicemen, see Michael Breen, "Congress Must Help Those Who Served with the U.S. Military," *The Hill* (blog), 17 September 2014, http://thehill.com/blogs/congress-blog/homeland-security/217914-congress-must-help-those-who-served-with-the-us; and Fleming, "My Afghan Battle Partner."
56. Bill McMorris, "Bosnian Marine Working to Bring Refugee Interpreter Home," *Washington Free Beacon* (Arlington, VA), 21 September 2005, http://freebeacon.com/issues/bosnian-marine-working-to-bring-refugee-interpreter-home/; Chiaramonte, "Don't Let Me Down"; Fleming, "My Afghan Battle Partner"; and LaPorta, "Afghan Interpreter Flees."
57. Ernesto Londoño, "State Department's Revocation of Visa Dashes Hopes of Afghan Interpreter," *Washington Post*, 24 September 2013, https://www.washingtonpost.com/world/national-security/state-departments-revocation-of-visa-dashes-hopes-of-afghan-interpreter/2013/09/24/33e7b5ae-254e-11e3-b75d-5b7f66349852_story.html.
58. Joe Gould, "Advocates: U.S. Has 'Moral Responsibility' to Fix Interpreter Visa Blunder," *Military Times*, 10 November 2013, http://www.militarytimes.com/story/military/archives/2013/11/10/advocates-u-s-has-moral-responsibility-to-fix-interpreter-visa/78543546/.

The Intelligence Dilemma in History, Fact, and Fiction

Robert J. Kodosky

The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal. By David E. Hoffman. New York: Doubleday, 2015. Pp. 336.

The Hidden Hand: A Brief History of the CIA. By Richard H. Immerman. Chichester, UK: Wiley Blackwell, 2014. Pp. 264.

The Rise and Fall of Intelligence: An International Security History. By Michael Warner. Washington, DC: Georgetown University Press, 2014. Pp. 424.

Edward J. Snowden's revelation in 2013 about the secret operations of the U.S. National Security Administration (NSA) raised a familiar question: is it possible to reconcile America's ideals with its national security needs? As Communism concerned Americans for much of the twentieth century, terrorism does today. Americans value the protection of their individual liberties. Then as now, Americans look to policy makers for protection against enemies but also against government secrecy. For the intelligence community using the latest surveillance technology, the often palpable tension resulting from the conflicting needs of secrecy and transparency is evident in the works from David E. Hoffman, Richard H. Immerman, and Michael Warner that trace the evolution of intelligence and espionage over time. While terrorism concerns Americans, privacy does also. Americans at once want the government to protect them from terrorists and surveillance.[1] Intelligence gathering and the use of surveillance are not new, yet they deserve special attention considering the technology available for internal surveillance and espionage. These authors speak to the importance of these activities and how they evolved over time.

Robert J. Kodosky, PhD, is an associate professor in the history department at West Chester University and the author of *Psychological Operations American Style: The Joint United States Public Affairs Office, Vietnam and Beyond* (2007).

"Before there was history," writes Warner, a historian for the Department of Defense, "there were spies" (p. 11). His book *The Rise and Fall of Intelligence: An International Security History* begins with a survey of spy craft in the ancient world. There, as he chronicles, spy versus spy sufficed. Espionage only became *intelligence* out of necessity. During the nineteenth century, competing political ideologies and industrialization rendered the environments where nation-states operated, both locally and globally, unprecedentedly complex. Governments and militaries sought to "gather and concentrate information by all available means" (p. 35). The craft of spying transformed into a profession essential for survival. As a result, President Harry S. Truman signed the National Security Act in 1947, which dismantled the Office of Strategic Services (OSS) of the World War II era and birthed the Central Intelligence Agency (CIA), an intelligence-gathering agency, to meet the needs of the United States during the Cold War.

By the end of the twentieth century, however, as proclaimed by political scientist Francis Fukuyama, history itself was ending.[2] Western liberalism, challenged by Communism for nearly a century, emerged from the Cold War as triumphant. Intelligence fared less well. The very factors that had enabled its ascent—new technology and conflicting ideologies—suddenly conspired to undermine it. The Age of Information opened up an Era of Surveillance. The line "blurred between watchers and watched, and "scrutiny," as Warner observes, "flows in all directions" (p. 333). Officials at the CIA came to acknowledge this reality in the midst of the Global War on Terrorism. They understood that maintaining detention facilities for captured terrorists contained inherent risks that included the "likelihood of exposure" that would "grow over time" and "inflame public opinion."[3]

That said, perhaps none are more qualified than Richard Immerman to scrutinize the history of the CIA. Besides his many scholarly contributions, Immerman served as assistant deputy director of National Intelligence for Analytic Integrity and Standards and Analytic Ombudsman for the Office of the Director of National Intelligence. Immerman's perspective is unique and complements well that of Michael Warner, a former historian for the CIA and the Office of the Director of National Intelligence.

Immerman and Warner track the evolution of the intelligence profession. They demonstrate it becoming increasingly complex, multidirectional, and militarized while David Hoffman, a former Moscow correspondent for the *Washington Post*, conducts a sweep that is far less grand but no less thorough. Through *The Billion Dollar Spy*, Hoffman scours Cold War Moscow to locate the tale of a particular time and place. Yet, he does so much more. He amplifies the lesson contained in both *The Hidden Hand* and *The Rise and Fall of Intelligence*. No matter the technological advance, as Hoffman observes, human source intelligence stands as "indispensable to national security" (p. 254).

The increased connection between intelligence and national security is rendered explicit by Warner in *The Rise and Fall of Intelligence*. Warner thoughtfully chronicles the factors that enabled the rise and fall of intelligence as monopolized by nation-states. The rise stemmed from necessity. Nineteenth and twentieth-century technologies shrank the globe even as industrial and ideological competition threatened to tear it apart. Western governments, especially their militaries and police, set aside previous aversions to spying and began to professionalize espionage as a means of ensuring stability. World War I, a conflict unprecedented in scope, gave rise to intelligence gathering while, as Warner persuasively argues in a chapter entitled "As Good as It Gets," World War II served as the peak of government activities. Old-fashioned espionage continued to play an important role, but European and American government agencies embraced science while enabling Allied intelligence to prove decisive in defeating the Axis powers.

The ensuing Cold War, an ideological competition framed by the United States and the Soviet Union, manifested issues for intelligence that remain unresolved. Technology grew more accessible. Nation-states no longer monopolized the tools of surveillance. Moreover, as intelligence became increasingly militarized, liberal nation-states faced reconciling their means with their ideals. The Cold War's conclusion and the Global War on Terrorism's onset served to aggravate these tensions.

As Americans are now conflicted about issues of privacy versus safety, tensions about intelligence gathering within a liberal political milieu have spilled over into popular culture as seen in the acclaimed television series *Homeland* (2011–present). In the 5 October 2014 episode, the show's protagonist, Carrie Mathison, a CIA agent played by Claire Danes, receives the nickname of "The Drone Queen" from her colleagues. Despite her success in previous operations, Mathison authorizes a bomb strike based on unverified reports. Taliban leader Haissam Haqqani (Numan Acar) is apparently killed. So too are 40 members of his family attending a wedding. The entire operation is captured on video by a survivor's iPhone and uploaded to YouTube. The video goes viral. Mathison becomes enraged.

Haqqani, as it turns out, survives the attack, and Mathison wants him dead. Her supervisors, including her mentor, insist otherwise. The higher ups are willing to take Haqqani off the CIA's kill list in exchange for a pledge to stop harboring terrorists. Mathison quits the agency and joins a security firm because her ideals, unlike those of her CIA colleagues, remain uncompromised. A similar story arc of *Homeland's* "The Drone Queen" can be seen in numerous television shows and movies since Snowden's revelations were released to the public at large. See another recent example in the film adaptation of John le Carré's novel *A Most Wanted Man* (2014).

In *The Hidden Hand: A Brief History of the CIA*, Immerman uses portrayals of

the CIA from television and film such as *Homeland* and *Argo*, the 2012 Best Picture Oscar winner, to demonstrate that the CIA is as "central to America's popular culture as it is to its national security" (p. 8). The CIA's actual history, however, remains "carefully guarded" (p. 8). Immerman's book is a testament to that; the prepublication review proved less than smooth. The work's initial submission met with a delayed CIA response, which "insisted on scores of redactions" and lacked "a single word of explanation" (p. xiv). An appeal resulted in a lessened number of redactions. Still, redactions remain. According to Immerman, these made little sense because the affected material is readily available in the public domain. The effort to maintain secrecy, however, testifies to the agency's ongoing resistance to calls for greater transparency.

Such intransigence proves counterproductive. It stands as a discredit to Immerman's considerable public service. Further, it does little to gain the CIA any trust from its considerable number of critics among academics and policy makers. Most important, it violates the ideals that Americans embrace. It threatens to thwart the scrutiny essential to national security as conceptualized by liberal republican governments.

The agency's efforts at concealment serve to heighten the value of Immerman's work, *The Hidden Hand*, which clarifies the CIA's part outlined by Warner in *The Rise and Fall of Intelligence*. The agency plays the starring role and easily morphs from an agency established to "collect, analyze, and disseminate intelligence" into one that additionally serves as an "instrument for engaging in covert, frequently paramilitary operations" (p. 21). The latter mission quickly and irrevocably diverts resources and commitment from the former, which is hardly what the CIA's designers intended.

In great detail, Immerman chronicles the historical circumstances, legislative loopholes, personality clashes, organizational interests, and bureaucratic politics that carried the CIA into clandestine affairs. Resistance in this transition proved futile, even when it originated from ones such as George F. Kennan, the architect of America's policy of containment against Communism. Kennan served as a proponent for both psychological warfare and paramilitary activities, but he argued that these responsibilities belonged elsewhere, in a newly created office, for instance, with "broader mandates and capabilities" (p. 23). It is no small irony that Kennan's proposal spawned NSC 10/2, the National Security Council's seminal directive establishing the CIA's covert capability.

In the ensuing decades, the CIA embraced covert and paramilitary activities. The agency's work, under Director of Central Intelligence Allen W. Dulles, whose career with the OSS during World War II had become legendary, and with the support of President Dwight D. Eisenhower and his Secretary of State John Foster Dulles, Allen's brother, established the foundation with operations perceived as successful in Iran (1953) and Guatemala (1954).

In the 1960s and 1970s, the agency had little oversight, congressional or otherwise, and insisted its operatives simply "learn by doing" (p. 51). The CIA and its operatives exercised great freedom to undermine Communism, both at home and abroad, allowing for possibly too much institutional and individual freedom. As Immerman demonstrates, these activities become a formula for increasingly reckless behavior including an illegal program of domestic surveillance (Operation MH/Chaos) authorized by President Lyndon B. Johnson, expanded by his successor Richard M. Nixon, and run by CIA counterintelligence chief James J. Angleton.

Despite public outcry, congressional investigations, and moderate reform, CIA covert operations barely missed a beat in the 1980s. They oversaw the failed attempt to rescue American hostages in Iran (Operation Eagle Claw) and assumed a central place in United States initiatives in Latin America and in Afghanistan. *The Hidden Hand* reveals a history of successful operations that serve as exceptions to the rule of failure.

Yet, these exceptions became the tail that wags the dog. The few successes, not the many failures, constitute the operational history that CIA leaders prefer to embrace. As Immerman argues, this choice is costly to CIA credibility, national security, and American ideals. The agency operates as a discrete paramilitary organization, countering terror networks with counterterrorist pursuit teams and drones, without the oversight of the military branches. Resources spent targeting enemies are diverted from the collection, analysis, and dissemination of information.

While the evidence of the changes in American espionage and intelligence gathering, as compiled by Immerman and Warner, is copious, *The Billion Dollar Spy* renders it preponderant. The case made by its author, David Hoffman, rests on 944 pages of declassified operational files redacted by the CIA prior to their release. These files largely comprise cable traffic between CIA headquarters and the Moscow station from 1977 to 1985 and are supplemented by interviews and additional documents, including ones released in response to a Freedom of Information Act request made by Hoffman. He uses it all well.

Hoffman's tale is true, yet it reads like fiction. The setting is Soviet Moscow. For CIA officials, this location represented a place where "no one could be trusted," and therefore "there could be no spies" (p. 15). Then one emerged, or tried to at least. Adolf G. Tolkachev, a middle-age electronics engineer, approached the CIA. He went directly to Robert M. Fulton, a 20-year agency veteran and a former military intelligence officer during the Korean War. In January 1977, Tolkachev found Fulton at a gas station and initiated contact as the American waited to fill up his tank. As instructed by his superiors, Fulton did nothing. He did the same the next three times Tolkachev contacted him. Fulton's tour ended and he left Moscow. Tolkachev remained. Time after time, seven in total, for more than

a year, Tolkachev worked to strike up a relationship with the CIA. The agency finally reciprocated in March 1978. By then, the agency determined that Tolkachev worked as a designer at one of two research institutes for Soviet military radars, "especially for those deployed on fighter aircraft" (p. 53) and could possibly be trusted enough to engage.

The Billion Dollar Spy does not constitute the first telling of the Tolkachev story. *The Main Enemy*, a collaboration between former CIA officer Milton Beardon and *New York Times* reporter James Risen, did so in 2003. Four years later, the CIA released Barry G. Royden's official unclassified version of the events as "Tolkachev, A Worthy Successor to Penkovsky: An Exceptional Espionage Operation." This account, however, lacks the details that *The Billion Dollar Spy* provides, which matters because that is precisely where the devil of it all resides.

The Billion Dollar Spy reveals human source intelligence as time consuming and tedious, precarious and dangerous. Tolkachev waited 12 years to start his yearlong dance to garner the attention of the CIA. Aware that his planned activity could result in a "severe ordeal" for his family, Tolkachev first wanted his son Oleg to grow up (p. 173). Once the spying began, he met his handlers only face-to-face and requested tapes of Western rock bands for his son. His activities, of course, required careful evasion of the ever vigilant KGB, the CIA's Russian counterpart. In the end, CIA Officer Edward G. Howard was fired, betrayed the operation, and defected to Moscow. These events led to Tolkachev's execution, tragically ending an operation that, while costly and unnerving, proved invaluable for American national security. Liberty and security exact high tolls. Americans weighing the costs of privacy with national security stand to gain by becoming informed about the sacrifices made by spies and other operatives in earlier periods of U.S. history, especially during the Cold War.

The Hidden Hand, *The Rise and Fall of Intelligence*, and *The Billion Dollar Spy* constitute required reading for those interested in the history of intelligence. The authors make a forceful case. Intelligence matters. It always has. Understanding its evolution separates facts from fiction, which might not prevent the fall of intelligence for the United States, but is essential for rehabilitating intelligence agencies to serve both America's national security and ideals.

Notes

1. George Gao, "What Americans Think about NSA Surveillance, National Security, and Privacy," Pew Research Center, 29 May 2015, http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/.
2. Francis Fukuyama, "The End of History?" *National Interest*, no. 16 (Summer 1989): 3–18.
3. U.S. Senate Select Committee on Intelligence, *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, 3 April 2014, http://www.intelligence.senate.gov/sites/default/files/press/executive-summary_0.pdf.

The Terrorist's Dilemma: Managing Violent Covert Organizations. By Jacob N. Shapiro. Princeton: Princeton University Press, 2013. Pp. 335. $29.95 (hardcover); $22.95 (paperback).

Many books and articles have covered the rise and fall of terrorist groups and the people who comprise them. In the majority of these, the authors have sought an understanding of why terrorists do what they do. The psychology of the "whys" dominates mainstream media and the attention of theorists striving to produce viable counterterrorism strategies. In far too many instances, terrorist groups are elevated to a lofty and idealized level of near invulnerability. Jacob Shapiro, in *The Terrorist's Dilemma*, takes a step back from the prevailing rhetoric to pull these actors down from those romanticized positions and to demonstrate that terrorists are like any other people operating organizations in that they have management and financial issues that they must address to operate. In this work, Shapiro challenges the reader's preconceived notions that terrorists act seemingly without constraint, without funding, and without the need for accountability. In essence, the modern terrorist organization faces the same scrutiny by its stakeholders as does any corporation or military, and that this knowledge may present a fracture point that counterterrorist forces and governments may exploit to more rapidly defeat these anti-establishment groups.

Readers and students of terrorism studies may be familiar with works that cover the funding and development of terrorist organizations from preeminent scholars, such as Martha Crenshaw or Bruce Hoffman, who have devoted enormous effort into the methodologies for understanding the recruitment of terrorists. These authors have only tangentially discussed the overall management of those assets. Moreover, as Shapiro declared, "There is a natural tendency to shy away from treating terrorists as rational actors" (p. 18). This was an inherently profound statement about organizations, which were routinely referred to as evil or inhuman by the media and by politicians. Yet, despite all the research and published material concerning the psychology and methodology of terrorist organizations, governments have struggled to make palpable inroads into defeating them, and as a result, the overwhelming majority of governments have

resorted to costly and inefficient military, attritional strategies. Shapiro's primary goal then, with *The Terrorist's Dilemma*, is to assist strategists by adding a level of understanding and a new dimension to the counterterrorism battles because as he pointed out, "Ultimately, we cannot efficiently fight organizations that we do not understand" (p. 25).

The foundation of the author's analysis rests with the concept of *agency problems*. Basically, agency problems may be defined as conflict arising when people (the agents) entrusted to look after the interests of others (the principals) use that authority or power for their own benefit instead of as contracted. Agency problems, he argues, permeate terrorist organizations just as much as they do in any standard business model, and he proffers three conditions that, should they exist in a terrorist organization, will most certainly indicate the presence of agency problems within that organization. First, the need of a principal to delegate actions. Second, the inability of that principal to fully monitor the agent's actions, or the ability to punish with certainty the agent when a transgression has occurred. Third, the agent's preferences are not aligned with those of the principal.

Shapiro's analysis delves deeper into the organizational weaknesses of terrorist groups by adding two perspectives. In his theory, a principal faces the greatest challenges in managing agents with respect to *preference divergence*. Simply put, preference divergence is the *delta* between what the principal wants and what the agent wants. In game theory, the principal is always seeking the best outcome for himself, while trying to convince the agent that that agent's desires are also being met. Game theorists will recognize the practical imbalance between the two as related to a Nash Equilibrium when two players seek to find a balance between their minimum trade-offs and maximum payoffs. The author went on to elaborate that both principal and agent are concomitantly engaged in a search for balance with respect to security, which he outlined as a *security-control trade-off* and a s*ecurity-efficiency trade-off*. Shapiro gives a concise, but brief introduction to these concepts. A recommended read for those interested in a deeper understanding of these trade-offs is *From People's War to People's Rule: Insurgency, Intervention, and the Lessons of Vietnam* by Timothy J. Lomperis (1996).

Using four case studies, Shapiro then applies his criteria to comprise the meat of the book. He did not limit himself to contemporary terrorist organizations, which lends strength to his argumentation. He applies them across a 100-year timeline of terrorist activities to demonstrate the viability of his hypothesis. Theses case studies were pre-Soviet Russia, activities of the IRA during the height of its activities in Ireland, the Palestinian-Israeli conflict, and al-Qaeda in Iraq. While the case studies provided a point of departure for his analysis, the reader should be more intimately familiar with the histories of these conflicts to better appreciate his analysis.

Overall, this book is worth the read even considering the shallowness of

the case studies. Additionally, the author's discussion of game theory is a bit superficial for general readers. Yet based on the lengthy annotated bibliography of terrorists' autobiographies and the extensive presence of primary sources, this work is a usable source for scholars or other well-versed readers.

LtCol Gregory Reck, USA
Special Operations Forces Chair
Marine Corps University

First, Fast, Fearless: How to Lead Like a Navy SEAL. By Brian "Iron Ed" Hiner. New York: McGraw-Hill Professional, 2015. Pp. 304. $26.00 (hardcover).

From the blockbuster success of the films *American Sniper* and *Lone Survivor* to Navy Admiral William H. McRaven's 2014 commencement speech at the University of Texas at Austin that went viral, the Navy Sea, Air, and Land (SEAL) brand has never been more prominent or more revered in American culture. This popular appeal contradicts the general trend of American suspicion about governmental and law enforcement institutions. While the physical aspect of the SEALs' cachet is obvious (e.g., google "Navy SEALs physical fitness"), Brian "Iron Ed" Hiner's book focuses on the more critical element of the SEALs' operational excellence—leadership.

Hiner's own experience could be a case study for Navy SEAL leadership. After enlisting and progressing through the standard training program in 1993, Hiner rose to become an officer and ultimately the head of training for all SEALs. The challenge for Hiner, who recently retired as a lieutenant commander, is how to distill almost two decades of leading and helping others to become leaders into a single volume, and how, within that volume, to relate leadership in a crucible-like atmosphere, where success meant survival and failure could result in death, to the more mundane world of business.

To convey the leadership philosophy of the book's title—*First, Fast, Fearless*—Hiner outlines three core elements: *brand, brotherhood*, and *battle rhythm*. A leader, regardless of formal role or the context for leadership, develops a brand of trust by practicing key personal virtues and principles. Drawing on Robert Greenleaf's famous formulation of the servant-leader model, Hiner argues that a leader's "brand" or reputation can only be built on constant attention to taking care of team members and adhering to a clearly defined ethos. Hiner highlights this concept of a leadership branding with the example of a SEAL sniper who, as team leader, was willing to forego an easy kill from a distance because of his concern about mistakenly identifying a possible high-value target (HVT). Instead of taking a shot from a distance, he took the risk of getting his team in position to tackle the target and confirm his identity. By doing so, they discovered after DNA

testing that the captured individual was not the HVT; this courageous SEAL team leader took to heart the ethos of respecting life—even as the easier, safer choice was both available and approved under the rules of engagement.

The concept of "brotherhood" is a familiar one in both popular and academic literature on leadership and the military, and as such, Hiner defines it as a "full commitment and promise from each team member to look after each other and to put the well-being of others before themselves" (p. 111). This emphasis on the brotherhood shared by soldiers is not new and is often culturally referenced with the quote from William Shakespeare's rendition of Henry V's speech at Agincourt—"we few, we happy few, we band of brothers"—and by numerous more modern popular culture references. Hiner draws on the role of the SEALs' swim buddy system to illustrate the need for close bonds between team members. By placing the fastest swimmers with those who are struggling, the swim buddy system "accomplishes the goal of getting everyone across the finish line faster" (p. 138). In the water, the faster swimmer can set the pace and navigate, preventing the slower swimmer from zigzagging and allowing him to save time and energy. Hiner translates this concept to other situations, pointing out that we already use swim buddies under different names: "a 'partner,' an 'associate,' or a 'teammate' " (p. 141).

Hiner then argues that finding the right "battle rhythm" leads to an organization that functions more like a jazz ensemble than an orchestra with a dictatorial conductor. This so-called battle rhythm is an "organizational condition, or context, that helps individuals confront the change and VUCA [volatility, uncertainty, chaos, ambiguity] of high-stress organizations—and enables the highest levels of success" (p. 185). A leader who is attuned to this rhythm can then empower team members to act, make key decisions, and be accountable without micromanaging or stifling the creative or entrepreneurial spirit.

At its best, Hiner's book conveys leadership lessons with a combination of succinct statements of principle and vivid illustrations of those values in action during his SEAL career. For example, in the chapter on humility as a prerequisite for great leadership, he cites the SEAL tradition of allowing various training cohorts to perform skits that caricature their instructors as one way to encourage, even provoke, humility in leaders. Hiner then makes the connection between this less-formal feedback mechanism in the SEAL training process to the growing application of 360-degree performance reviews in government and private sector organizations.

These powerful passages and Hiner's fundamental points are sometimes obscured, however, by a confusing conflation of multiple leadership philosophies and limited exploration of more strategic leadership considerations. Occasionally, Hiner's invocation of various leadership theories and buzzwords makes it unclear whether the primary focus is on the "First, Fast, Fearless" theme of the title; the

SEALs' "Five Pillars" of moralist, jurist, teacher, steward, philosopher; or the "brand, brotherhood, battle rhythm" construct that shapes the core of the book.

And while this leadership framework of brand, brotherhood, and battle rhythm is powerful, Hiner misses an opportunity to examine the more strategic aspects of leadership. Early in the book, he discusses the development of a formalized ethos for the SEAL community in 2005. Moreover, he alludes to problems and some organizational tumult within the community as the impetus for this new ethos. This episode would have been a great springboard to articulate not just how to engage and complete "the mission," but also how leaders have to grapple with defining and choosing what "the mission" itself should be.

Hopefully, readers will wade through the intermittent use of leadership clichés to the more compelling principles and examples from Hiner's book; in doing so, they will find ample material to nurture and develop their own brands, brotherhoods, and battle rhythms as they become first, fast, and fearless leaders.

Evan Haglund, PhD
Department of Humanities
United States Coast Guard Academy

Momentum and the East Timor Independence Movement: The Origins of America's Debate on East Timor. By Shane Gunderson. Lanham, MD: Lexington Books, 2015. Pp. 180. $80.00 (hardback); $79.99 (e-book).

In *Momentum and the East Timor Independence Movement*, Shane Gunderson traces the evolution of a social movement (1975–99) that supported the ultimate attainment of independence for East Timor. He meticulously uncovers who the movers and shakers were within a global network of advocates centered on bringing attention to injustices perpetrated by Indonesia in the former Portuguese colony of East Timor and the international acquiescence or support for that occupation. The author examined primary documents held at the United Nations' (UNs) archives and conducted in-depth interviews with major figures in the movement to construct a historical record of rather unique events surrounding the East Timorese attainment of national self-determination and political sovereignty. He cites other primary documents from the UN Human Rights Commission, the International Commission of Inquiry of East Timor, and nongovernmental organizations like the East Timor Action Network (ETAN).

Gunderson wrote this book to explore the identities of the people who led this successful social movement and the reasons why others allowed the genocide to occur. In transforming this project from a dissertation into a monograph, however, he omitted much of the theoretical analysis and literature review. Tracing a

series of the East Timor Independence Movement's turning points in the book's 10 chapters, the author recounts such well-publicized events as Pope John Paul II's visit to Timor in 1989 and the Santa Cruz massacre of 1991. More important, the author documents Timor's political struggle to surmount domination by Portugal and Indonesia through the 1960s and 1980s, which resulted in little action save a UN acknowledgement. The unforeseen waning of the Cold War overshadowed this negative momentum and two Timorese activists, José Ramos-Horta and Bishop Carlos Belo, subsequently received the 1996 Nobel Peace Prize for their role as catalysts for UN involvement. After the 1997 Asian financial crisis and subsequent fall of Indonesian President Suharto, a 1999 referendum on East Timor's independence attracted 99 percent of eligible voters, of which 78 percent chose independence.

The book also details the significant dissident intellectuals and activists associated with the movement and their contributions. These include Arnold Kohen's major role in building relationships with the Catholic Church, Charlie Scheiner's help disseminating information on events inside Timor to a wider constituency in America, and Noam Chomsky's counsel on general strategies to deal with media and governmental institutions. Gunderson even acknowledges the importance of Cornell University students and faculty acting under the tutelage of a coterie of those mentored by famed Southeast Asian studies scholar Benedict Richard O'Gorman Anderson. Collectively, this loose network found support for the movement among nongovernmental organizations in Australia, New Zealand, and Europe and successfully lobbied for East Timor before the UN and the U.S. Congress.

While Gunderson thoroughly explains the impact of most events that shaped the pursuit of the referendum, some milestones, such as the arrest of resistance leader Kay Rala Xanana Gusmão, are not addressed. Even if Gusmão's arrest was not a setback, the event needs further explanation in the context of East Timor's mêlée. The decision by the United States and the UN to become bystanders to genocide in Rwanda in 1994 and the later commitment of President William J. "Bill" Clinton and UN Secretary-General Kofi A. Annan to intervene in human rights violations in East Timor and Kosovo in 1999 provide two additional examples of turning points that might not be given due weight in Gunderson's account. Thus, more description regarding the level of influence this movement really exerted on decision-making powers in Canberra, Washington, New York, and Jakarta would have been beneficial.

Emphasis is given to the possibility that U.S. weapons were used during the Indonesian invasion and occupation as well as the plausibility that genocide was constituted owing to the perpetrated crimes against humanity. As opposed to the modest discussion on the lack of international action on behalf of East Timor,

a more nuanced explanation of Indonesian motives and interests in possessing Timor would have contributed to a more complete understanding of the political environment. For example, Indonesia's involvement in Timor also arose from the ambitions of the military class, challenges of holding the territory together, and aspirations for national identity, some of which Benedict Anderson addressed in more detail in his classic work *Imagined Communities* (1983). Similarly, Gunderson might have broached a more contextual discussion by introducing other secessionist movements, such as those in Aceh or West Papua, if only to highlight how Timor's unique unresolved UN status contributes to the limited success of the Aceh Merdeka (Free Aceh) or Papua Merdeka (Free Papua) movements.

Gunderson tailored this monograph to those with a deep and abiding interest in East Timor, particularly its past, but not necessarily its future. Overall, the goals of the book are limited to documenting the individuals and organizations that advocated for Timor in the United States. Although Gunderson identifies the public as referees for social movements in both the introduction and conclusion, the U.S. public seemed to play a negligible role while rather politically sophisticated and academically informed activists and intellectuals pursued a lengthy lobbying effort that ultimately contributed to other political forces that pressured Indonesia to allow a referendum. Thus, the activities of Timorese supporters were largely a lobbying campaign driven by a small network of intellectuals and activists rather than a mass social movement. Despite a foreword by Ambassador Constâncio da Conceição Pinto and one chapter emphasizing the Intra-Timorese dialogue, the book's substance lacks much on the Timorese role, especially the parallel efforts of the internal social movement, clandestine operations, and public campaign. The author provides little context of the massive student protests and strikes inside Timor, even though they would be the closer corollary to Gunderson's comparison of East Timor independence to U.S. civil rights movement.

Nevertheless, *Momentum and the East Timor Independence Movement* is a worthwhile read for those interested in how East Timor remained on the international agenda for more than two decades despite the Timorese suffering from extended violence and oppression. Against the odds, the region emerged as a global concern, and through concerted efforts by multifaceted constituents, Timor became the first new state of the twenty-first century. Gunderson competently tells the story of a band of activists operating diligently toward that singular goal in a new and comprehensive way.

James DeShaw Rae, PhD
Department of Government
California State University, Sacramento

The Tail Wags the Dog: International Politics and the Middle East. By Efraim Karsh. New York: Bloomsbury, 2015. Pp. 256. $28.00 (hardback); $28.99 (e-book).

While many Americans attempt to understand the events in the Middle East from a physical and cultural distance, Professor Efraim Karsh provides scholars, foreign policy experts, and politicians a different perspective concerning global power politics and their impact on the Middle East. As a professor of political studies at Bar-Ilan University in Israel, scholarly writer, and editor, Karsh has gained a wealth of knowledge about the Middle East. In *The Tail Wags the Dog,* he conveys that external involvement in Middle Eastern affairs is "neither the primary force behind the region's political development nor the main cause of its notorious volatility" (p. 2) and reiterates his position from *Rethinking the Middle East* that "long-existing indigenous trends, passions, and patterns of behavior" (p. 52) cause Middle Eastern turmoil.

Karsh develops his arguments throughout a series of nine essays on significant aspects of the region and the involvement of such important outside players as the United States, Russia, and Britain. He presents factual case studies of what Western powers did to influence the Middle East and concludes that the great powers did not cause the turmoil, but culpable power hungry local players created the region's malaise.

Many scholars accept the conventional wisdom that European powers picked apart the Ottoman Empire over the centuries, drove it into World War I, and took control of its land. Karsh points out, however, that squabbles within the empire—such as the machinations of the Hashemites to create Iraq and Transjordan—caused the region to become divided by sowing the seeds of future violence. The contemporary Middle East emerged from a variety of forces, including the consequences of the Hashemite dream of succeeding the Ottoman Empire, the Jewish quest for a homeland, British colonial aspirations, Turkish nationalism, and Armenian and Kurdish self-determination, as well as the ambitions of such outsiders as the French, Italians, and Greeks. Middle Eastern politicians who chose to attain their objectives by subverting and manipulating the United States and the former Soviet Union added to the discord. It is thus no wonder that the Middle East is a complex topic.

Although a general understanding of Middle Eastern history makes the book easier to follow, Karsh nonetheless provides an invaluable perspective for those who seek the truth about the complicity of local players in the formation of the modern Middle East. Combine *The Tail Wags the Dog* with David Fromkin's *A Peace to End All Peace: The Fall of the Ottoman Empire and the Creation of the Modern Middle East* (2009) for opposing perspectives of the forces influencing the region's conflicts.

Some readers may view the insightful and noteworthy epilogue Karsh com-

posed for *The Tail Wags the Dog* as an attack on Islam, but others may grasp it as a critical examination of the role of Islam in fostering current violence. Karsh points out that violence and turmoil were not imported to the region by foreign imperialism; such instability has been an integral part of local culture throughout history. He further highlights Islam's inability to separate religion from politics as a significant contributing factor to the region's volatility. Notably, Islam became a great empire, it faded, and the resurgent interest in a super Islamic nation-state—the Islamic State—fuels modern violence. To achieve this unification of religion and politics through the creation of an Islamic empire, Muhammad and his followers devised the concept of jihad. Out of this duty, al-Qaeda and other terrorist organizations are attempting to restore the greatness of the ephemeral theocratic empire.

With Professor Karsh's alternate perspective to the long-held theory of foreign imperialism as the root cause of Middle East turmoil, readers will broaden their thinking to more clearly understand the issue. The epilogue of *The Tail Wags the Dog* heightens the international community's awareness that international terrorist groups who use the Islamic religion as the basis for their conquests have an irreconcilable nature and will not stop until they are defeated. With this knowledge, global leaders will be better positioned to develop an effective counterstrategy for Islamic jihadists determined to restore the caliphate—including all the lost Islamic territories—and expand the Islamic religious and political empire to other regions of the world.

LtCol R. Nicholas Palarino, USA (Ret)
Adjunct Professor
Georgetown University

A War It Was Always Going to Lose: Why Japan Attacked America in 1941. By Jeffrey Record. Lincoln, NE: Potomac Books, 2010. Pp. 184. $24.95 (hardcover).

Many readers may find it difficult to accept the idea of war as a rational conclusion to failed negotiations. How could war be rational for Japan, especially when facing the military and economic might of the United States, shielded as it was with the advantages of geographical location, land mass, natural resources, and population? Perhaps due to the natural passing of many Japanese and American veterans and civilians from that generation, there is less reflection on this predicament today than before the 1995 Japanese commemoration of the 50th anniversary of the end of World War II. Yet, the question must be considered when examining the Japanese attack on the United States.

In *A War It Was Always Going to Lose*, Jeffrey Record describes the decision

making that led to the outbreak of war and reminds readers to reconsider these important events. Record, a well-known and thoughtful writer on defense issues, teaches strategy at the U.S. Air War College. Some readers may find his digression in certain passages too opinionated, but his wealth of practical and academic experience supports them.

The author divides this book into chapters that provide a cursory view of the war's chronology from the Japanese viewpoint. Chapter 1, "Introduction: A 'Strategic Imbecility'?," challenges the various observations about Japan's irrational provocation of war with the United States, and critiques U.S. mistakes along the march to war. Three chapters—"Japanese Aggression and U.S. Policy Responses, 1937–1941," "Japanese Assumptions and Decision Making," and "Failed Deterrence"—make up the crucial presentation of historical materials in the book. The shortest chapter—"Was the Pacific War Inevitable?"—examines the evidence and concludes that "by late 1941 the clash between core Japanese and U.S. security interests (in Southeast Asia) had become irreconcilable by means short of war. Japan was bent on further aggression, and the United States was determined to resist it" (p. 116). The final chapter, "The Enduring Lessons of 1941," introduces problems relevant to today's policymakers.

Particularly helpful to understanding Japan's perspective, chapter 2 aggregates the sources of tension between Japan and the United States in the subsections of U.S. racism and immigration policies, open door policy and American moralism, U.S. nonrecognition of Manchuria, Japanese aggression in China, U.S. assistance to Chiang Kai-shek's national government, and U.S. embargoes on Japanese trade. Of further benefit, Record also discusses the consequences arising from Japan's arrogance and ignorance of the outside world, specifically noting a failure to recognize enemy attributes.

In light of all the reasons Record uses to rationalize the obvious outcome of Japan's offensive, it would have been a mystery if the two countries did not go to war. Conversely, the author also notes that we should not argue that the war was "historically determined" (p. 44) because to do so is "to claim that that Japanese and American political and military leaders had no control over events. . . . This is simply not the case. They may have misjudged and miscalculated, ignored unpleasant facts, and engaged in wishful thinking, but they consciously made decisions and those decisions had consequences, intended or otherwise" (p. 44–45).

With this in mind, Record does not examine in detail the nuances of Japanese policy making, namely that there were serious divisions not only in warfighting strategy, but also in whether to go to war at all. The author notes this division was particularly evident among the more internationally minded Japanese politicians and foreign ministry officials who believed in historic cooperation with the United Kingdom and United States. These groups faced arrest or assassination,

opposed war, pushed diplomacy, and sought to bring an early end to the war. They emerged as leaders in postwar Japan.

To bring out these nuances and other aspects of sociocultural elements influencing the war, the book would have benefited from the insight recorded in Japan's extensive collection of literature and primary documents. While specific to Japan's decisions during World War II, the lessons presented in *A War It Was Always Going to Lose* are, unfortunately, universal and timeless.

Robert D. Eldridge, PhD
School of International Public Policy
Osaka University

The Art of the Possible: Diplomatic Alternatives in the Middle East. By M. Reisman. Princeton, NJ: Princeton University Press, Princeton Legacy Library, 2015. Pp. 170. $29.95 (paperback).

> The day-to-day events transpiring in the Middle East are quickly and dramatically presented to the American public. What has been lost in the mundane montage of newsprint, radio, and television reports has been the larger view in which changing details become coherent, and in which proposed alternatives can be evaluated rationally (p. 3).

If one were to add social media to the list of media, we could be forgiven for thinking that this was written just last week. The passage was published, however, some 45 years ago. The mark of a good book is its ability to resonate over time, and Michael Reisman's work does just that in the reprint of his book originally published in 1970. While some of the references to particular events or relationships are now somewhat anachronistic, the lessons and analysis remain as relevant as ever.

In this work, Reisman gave voice to a frustration that the Middle East was mired in a cycle of violence, focusing on four major issues that were roadblocks to an environment of peace: the Sinai, Jordan and the Palestinians, the Golan Heights, and Jerusalem. He rightly notes a number of reasons that an understanding between the conflicting parties was elusive: dictatorial and demagogic Arab leaders, Israeli leaders who ignored the rights of Palestinians and seemed intent on creating new realities, and external actors who enabled bad decision making in the region and often undermined the possibility of any positive steps forward. The frustration could only grow over the intervening 45 years since a number of the roadblocks and poor leadership are still present.

We read this book now knowing that, as Reisman was writing, the Egyptian-Israeli War of Attrition (1969–70), Jordanian-Palestinian Civil War or Black September (1970–71), and the Egyptian-Syrian Yom Kippur War (1973) were events on the horizon. The Lebanese Civil War (1975–91) was not far off either. It is like watching a movie after having read the book: no matter how badly the story ends the first time, if the movie remains true to the written work, the feeling of impending doom is almost overwhelming.

Reisman's chapter on Israel, Egypt, and the Sinai represents either the groundless musings of an academic or a bold proposal to move the region out of the cycle of violence that had already become well established by 1970. While the chapter is rather anachronistic now, Reisman's ideas do bring up stereotypical "what if" thinking. What if the international community had encouraged truly bold action in light of the wars that had occurred from 1948 on? What if the superpowers could have viewed the region through a prism rather than on global and regional chessboards? Would the Sinai Development Trust have made the area a model for the larger Middle East? Would it have encouraged economic, and subsequently political, cooperation that would have led us to a truly different twenty-first century? We will never know. What the chapter may ultimately contribute to longer-term discussion is the fact that the Middle East has been the victim of a dearth of boldness when attempting to find underlying causes of and long-term solutions to conflicts, something Reisman addresses directly throughout the book.

In his discussion of the plight of the Palestinians, Reisman notes "an equitable solution to the problem of the Palestinian Arabs is not only an exigent moral demand but also a crucial requirement for increasing stability in the Middle East" (p. 44). Nothing has changed. He was prescient in fearing the establishment of Arab Bantustans. Moreover, as one views the current siege of Gaza and the breakup of the Palestinian West Bank coupled with the increased polarization and focus on identity within Israel, it is difficult not to be even more pessimistic and worry that the window of opportunity for an equitable settlement has permanently closed. Reisman is right to point out that the plight of the Palestinians is not the fault of the Israelis alone. The Egyptians and Jordanians did nothing to advance the Palestinian cause during their 19-year occupation of the Gaza Strip and West Bank. Palestinian leaders were probably unfairly expected to compromise on territorial claims through no real fault of their own, but reality had passed them by after 1948; they really had no option but to adapt, and for a while they did not.

The author also introduces the idea of carving out a space for the Druze, members of a nonmainstream faith found in parts of the Middle East. The creation of a Druze Trust Territory in the Golan Heights region is also a novel

approach, and clearly one that would have required international action. But, the real benefit of chapter 4 is the smaller nuggets, including background on the Druze and the acknowledgement even then that the Lebanese political structure could guarantee "at least one crisis per decade" (p. 64). While current events in Syria have now likely changed the equation regarding the Golan, Lebanon continues to stumble from crisis to crisis.

Both the United Nations Special Committee on Palestine and Reisman agreed on the need for some level of internationalization of Jerusalem, but again the intervening 45 years since Reisman wrote his proposal for a Jerusalem statute through the United Nations has solidified positions, especially the Israeli position. A division of authority over certain aspects of Jerusalem, such as control over holy sites, legal disputes, or even "mundane secular matters," simply will not be acceptable to either the current Israeli government or the Palestinian National Authority. The importance of the religious sites has not lessened over the decades, and the creation by Israel of facts on the Jerusalem ground (e.g., housing settlements, the barrier, and civil authority) has ensured that the city remains a flashpoint. No Israeli or Palestinian political leaders could countenance the presence of an outside authority without paying an extremely high price. Reisman's program would have been unacceptable in 1970, and positions have only hardened since. What is important about Reisman's work is the realization that, more than 40 years ago, Jerusalem would be important in the future and that an international role for resolving the conflict was imperative.

Ultimately, Reisman raised one very important point: the international community as of 1970 needed to play a cohesive and objective role in resolving these points of contention. The United States was clearly an advocate of the Israeli position after the 1967 war. The Soviets, and subsequently the Russians, had their own agenda when supporting Syrian and Egyptian leaders. When the opportunity arose to bring members of the international community together to focus on the Israeli-Palestinian conflict, the United States ensured that the Middle East Quartet—the United States, Russia, the European Union, and the United Nations—created in 2002 was simply a way to co-opt the actions of other international actors rather than combining forces to exert more pressure on the parties to the conflict and coming up with the bold programs, à la Reisman, to resolve the conflicts.

This book is a quick little read, but it is worthwhile to slow down and mull over the ideas that Reisman presents, the aspects of the regions that remain unchanged, and the fact that we may be watching the first substantive changes in the region since 1967, if not 1948. The appendix of League of Nations and United Nations documents beginning with the July 1922 Mandate for Palestine and ending with the 1967 United Nations Security Council Resolution 242 provide

useful reference materials for understanding the legal-political context as well as a reminder for how little has been settled in the intervening 90 years.

1stSgt Timothy Schorn, ARNG, JD, PhD
Associate Professor of Political Science
Director of the International Studies Program
University of South Dakota

Ballots, Bullets, and Bargains: American Foreign Policy and Presidential Elections. By Michael H. Armacost. New York: Columbia University Press, 2015. Pp. 304. $35.00 (hardcover and e-book).

Michael H. Armacost adroitly tackles an understudied topic—the interplay between our presidential electoral process and the conduct of U.S. foreign policy—using examples since 1948. He brings the eye of a Washington, DC, political insider to the analysis; he served in the State Department for more than two decades, rising to undersecretary of state, ambassador to Japan and the Philippines, and president of the Brookings Institution.

Drawing on memoirs, personal experience, and journalistic accounts, Armacost analyzes each phase of the electoral process: from the intensely partisan battles to win the party nominations, to the more centrist debate necessary for the general election, to the awkward transition phase after the November election when an incumbent president still has a few months in office, to the frenzied start-up phase for a new administration, to the looming prospect of running for reelection after only a few years in office. Armacost teases out how the particular political dynamics of each phase can affect ongoing diplomatic negotiations, the broader foreign policy agenda, and relations with other countries.

"The U.S. presidential election system was not designed for the efficient pursuit of foreign policy objectives," Armacost argues, and yet somehow the republic muddles through (p. 220). The contenders for president, more often than not, possess little substantive knowledge of foreign countries and have not thought deeply about U.S. strategic imperatives. Elections tend to be backward-looking, a referendum on the last administration's record, when incumbents oversell their achievements and contenders exaggerate current problems and build aspirational platforms better suited to marketing than political realities. Democrats running for president tend to talk tough to compensate for their party's historical stereotype as weak on national security. Republican contenders, on the other hand, if campaigning with a Democrat in the White House, tend to advocate for wholesale rejection of existing policies, an "anything but" approach (p. 202). A matter of crucial importance for the nation—the selection of vice presidential candi-

dates—"remains incredibly informal, even casual" (p. 61). In other words, the political process does not select the most experienced or knowledgeable candidates and the debates accompanying presidential elections do little to illuminate the substantive foreign policy problems the United States faces.

After the results are in, a new president-elect, often a Washington outsider who has "spent the bulk of their time for several years with people better equipped to get them elected than to help them govern," suddenly faces a steep learning curve, especially on foreign policy (p. 14). The first daunting task is staffing the top layers of the national security bureaucracy while dealing with a recalcitrant partner in Congress. Some new presidents feel pressure to act quickly to make changes in line with campaign promises, even though they do not yet have the lay of the land in terms of the strategic interests of the United States or the constraints imposed by legacies from the past administration or an understanding of the nuances of bureaucratic politics. As a result, some presidents make initial moves that they later reverse (e.g., William J. "Bill" Clinton linking China's most-favored nation trade status to its behavior on human rights), although others preside over slower and smoother launches of their foreign policy agenda (e.g., George H. W. Bush revealing the benefits of greater experience with Washington and the issues before taking office).

Just as the president is finally settling into the job less than three years after taking office, he must begin to think about the looming battle for reelection, a situation that can have both positive and negative effects on U.S. foreign policy. An incumbent president has incentives to put some controversial issues on hold (e.g., Lyndon B. Johnson downplaying the need for military intervention in Vietnam prior to the 1964 election), to make course corrections on others (e.g., Ronald Reagan taking a more conciliatory approach to the Soviet Union in a January 1984 speech), and to push for a resolution on others before facing an accounting in the general elections (e.g., Bill Clinton pushing for the Dayton Accords to settle the Bosnian conflict before the 1996 election). And, of course, as Armacost observes, a sitting president has the incentive and the resources to use his office to gain a public relations advantage during a general election as shown by Richard M. Nixon's trip to China and signing of the Strategic Arms Limitation Treaty prior to the 1972 election.

Transition periods can also affect foreign policy. Sometimes the commitments that one administration makes to another country can get lost in the process. But there are also examples when "the baton" is passed smoothly, such as when James E. "Jimmy" Carter took up the negotiations for the Panama Canal Treaty started under Gerald R. Ford or when Clinton continued the negotiations for the North American Free Trade Agreement started under George H. W. Bush. Armacost also observes how the sitting president, watching his time run out after a November election, has incentives to act quickly and shore up his legacy

(e.g., George H. W. Bush intervening in Somalia after he lost the 1992 election).

For all the turmoil and political maneuvering, remarkably, the system still somehow works, mostly: "[T]he Republic has survived quite comfortably, and the United States has compiled a creditable, albeit uneven, record of accomplishment in its engagement with the world" (p. 220). While some issues are allowed to fester without sustained attention and while there are swings from expansive commitment followed by retractions, Armacost argues that there is still a policy of continuity from administration to administration grounded in stable national interests.

Overall, Armacost's analytical method is to observe patterns using selected historical examples. For better or worse, he sidesteps the academic literature that tries to understand events, such as the effect of elections on the diversionary use of force, using quantitative analysis. Without doubt, the book offers many new and useful insights about the messiness of Washington politics and its impact on the conduct of foreign policy. In a few cases, however, readers may feel that a particular topic (e.g., the general differences between Republican and Democratic contenders or the extent of continuity between administrations) could benefit from a more systematic approach.

Shoon Murray, PhD
School of International Service
American University

Cyber Blockades. By Alison Lawlor Russell. Washington, DC: Georgetown University Press, 2014. Pp. 176. $49.95 (hardcover); $29.95 (paperback and e-book).

On 10 July 2015, the U.S. Office of Personnel Management (OPM) made the stunning announcement that the records of some 21.5 million federal workers and contractors had been stolen from OPM's computer networks. On the heels of this announcement, Director of National Intelligence James R. Clapper Jr. noted in widely publicized remarks that China was the "leading suspect" among those believed to be responsible for the theft of the records. Despite its breathtaking scope, the OPM data breach was only one of a string of high-profile federal computer network intrusions to occur in 2015. In March, the U.S. State Department had to take its entire unclassified email system offline to address a massive digital infiltration. Unconfirmed rumors circulated that the Russian government was behind this breach at the State Department. And in August—less than a month after news of the OPM records theft became public—the Pentagon announced that the Joint Chiefs of Staff's unclassified email system had also been compromised. Both Russia and China were named as possible culprits.

The OPM, State Department, and Joint Chiefs incidents fit into expanding scholarly debates about the rising importance of cybersecurity concerns in government. Alison Lawlor Russell attempts to shed further light on this subject in her 2014 book, *Cyber Blockades*.

Russell, a political scientist, seeks to explain how entire nations can be deliberately cutoff from cyberspace, and why state or nonstate actors might choose to use the tactic of blockading a nation virtually. Following a brief introduction, she sets out a number of potential acts in chapter 2 that could constitute cyber blockades. These include physical attacks on infrastructure—the literal severing of Internet cables—as well as virtual acts, such as Distributed Denial of Service (DDoS) attacks. She then turns to general descriptions of blockades, a tactic used most often in the context of traditional warfare or economic disputes.

In chapter 3, the author unpacks the many potential meanings of blockades in the contexts of sea, air, land, space, and information operations; readers may recognize these categories as essentially the same domains used by the Department of Defense in its own policy and strategy documents. The detailed historical information in chapter 3 provides an eye-opening description of the many forms that blockades can take. For example, the author's descriptions of U.S. no-fly zones created to protect Iraqi civilians in the wake of the first Gulf War illustrate that these no-fly zones were, in effect, aerial blockades. Most important, Russell constructs a five-factor theoretical framework to evaluate whether a particular act constitutes a cyber blockade.

Russell uses her theoretical framework in chapters 4 and 5 to assess two recent and prominent cases of possible cyber blockades: the 2007 DDoS attacks in Estonia and the 2008 cyberattacks that accompanied the Russian ground invasion of its neighbor Georgia. The author presents compelling evidence that both nations' experiences qualify as cyber blockades, despite important contextual differences between the two cases. In concluding the book, Russell offers a range of lessons for scholarly and policy communities. Notable among these conclusions is that the advent of cyber blockades introduces the need for unprecedented levels of public-private sector cooperation, a function of the private sector's dominance in building and maintaining information technology infrastructure.

While Russell successfully defines and provides evidence for the existence of cyber blockades as a tool to advance foreign policy agendas, the book could be strengthened by a discussion of how states may impose cyber blockades upon their own citizens, which the author terms "censorship." In fairness, Russell distinguishes between cyber blockades and state-imposed online censorship at the outset, and she is direct in pointing out that her book focuses on the former.

But the ubiquity of state-directed online censorship, as well as state-directed Internet blackouts, is hard to ignore. During the Arab Spring, Egypt's four primary Internet service providers severed their connections to the Internet. This was

likely done under direct pressure from the Egyptian government, which at the time sought to stop protestors from using social media sites to organize demonstrations against the government. Syrians, too, were cut off from the Internet for a period of 19 hours in May 2013. There is speculation that the regime of Bashar al-Assad did this deliberately to prevent Syrian opposition groups from communicating with each other as well as the outside world. And China has long been known for its "Great Firewall," a gargantuan state censorship initiative that blocks its citizens from accessing sites such as Google and Facebook while also virtually abolishing social media updates that too strongly criticize Beijing.

While *Cyber Blockades* contributes to our understanding of how global conflicts are evolving, one is left with the nagging sense that state-directed online censorship to control domestic populations—not the use of cyber blockades as tools of foreign policy—will likely prove to be the more widespread and vexatious challenge in the years ahead.

Austen D. Givens
Department of Economic Crime, Justice Studies, and Cybersecurity
Utica College

Understanding Contemporary Africa, Fifth Edition. Edited by April A. Gordon and Donald L. Gordon. Boulder, CO: Lynne Rienner, 2012. Pp. 511. $27.50 (paperback and e-book).

While you read this book review, Western personnel from government and private sectors are fully engaged across Africa in numerous activities. Doctors, lawyers, teachers, and military personnel, to name a few, are working with their African counterparts. All face the same challenge, which is to build common grounds to work effectively with partners who come from different parts of the world and have other perspectives on how to address problems. This is the reason why cultural sensitivity is paramount. In that respect, military and civilian personnel will use *Understanding Contemporary Africa* as a reference guide to enhance their knowledge of Africa to be better prepared to perform a variety of activities ranging from planning and achieving projects to building alliances and training with Africans.

Understanding Contemporary Africa offers a rich and articulated introduction to the continent. African cultural, social, political, and economic systems are well addressed throughout the easily read 511 pages. By integrating the contributions from eight other experts, the work of April and Donald Gordon encompasses topics and issues critical to Western planners and operators. The book provides an eye-opening perspective to the reality, cultures, and behaviors of African

societies in the early twenty-first century. Highlighted throughout the study are primary factors and drivers that define the functioning, behavior, and cultures of African governmental institutions, civil societies, and private sectors. With a broad scope, up-to-date information, and in-depth insight, the 13 chapters also provide military students from all Services with critical-thinking elements about the challenges they will face while participating in strategic planning conferences with African partners, assessing the warfighting functions of African forces, and conducting military education and training with African counterparts.

The rigorous cultural insight provided in the chapters on "Africa Politics" (chapter 4), "Economies of Africa" (chapter 5), and "Family and Kinship" (chapter 9) will likely be very helpful to Western militaries who are often bewildered by African norms and culture overall. These chapters may assist readers in refining their approach to patronage and corruption within many African institutions. Our African counterparts, for instance, are often prompt to remind us that the word "corruption" does not exist in any African language. Attempts of translation rather refer to the more traditional concept of reciprocity, which drives the exchange of favors between individuals when they are blood-related through family, ethnicity, and clan. "Many African systems emphasize shared 'blood' or consanguineal relations" (p. 281) that define a traditional code of reciprocity between family members and kinship. African militaries are no exception. Some individuals continue to abide by the traditional code of reciprocity even though their Western counterparts condemn it as a pattern of patronage and corruption.

The in-depth information that relates to African politics (pp. 61–113) offers readers another valuable set of keys to better understand the root causes of the overall leaning toward a centralized top-down functioning of chains of command, rigid hierarchies, and elite mentalities that seems to permeate many African organizations to include African militaries. Intended as an introduction to African politics, the chapter also provides elements that answer the question "Are Western-style democratic states possible in Africa now?" (p. 63). The editors remind readers that although "patron-client relationships permeate most African governments" (p. 80) and "efforts by African citizens to achieve further liberalization and democratization in many states had been stalled by powerful elites while, in other states, previously gained liberties were lost" (p. 100), yet "across the continent, virtually all countries have undergone political liberalization and, with rare exceptions, the single-party state has disappeared" (p. 106).

Chapter 10 navigates the field of "Women and Development." The input unveils some of the cultural roots that explain the specific approach to gender within many African militaries. Another particularly timely topic is the chapter "Religion in Africa." Indeed, chapter 11 emphasizes the influence of traditional African religions in the shaping of both Christian and Muslim ideologies and practices in Africa. The analysis of such factors as "Belief in the supreme being"

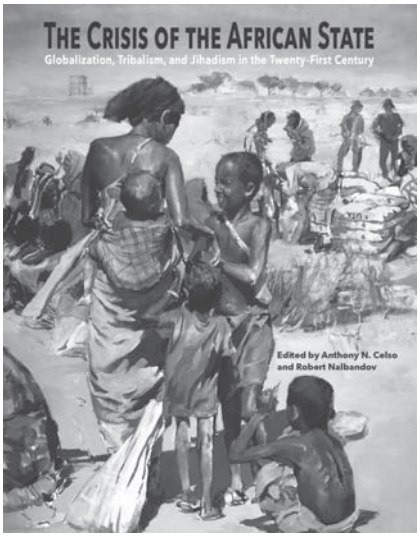
(p. 337), "Belief in divinities and spirits" (p. 338), "Belief in life after death" (p. 341), "Religious leadership and sacred places" (p. 342), and "Witchcraft and magic" (p. 343) provides an articulated and well-informed insight that encourages the reader to better understand the African perception of a variety of current security challenges. This chapter, for instance, helps readers understand the root causes of the negative initial reaction of the populations to the medical treatment set up by Western humanitarian organizations fighting the Ebola virus in West Africa in 2014. On the same note, the study highlights the reason why the majority of the African Muslim communities are opposed to the spread of the violent Islamist jihad promoted by extremist groups such as al-Qaeda in the Islamic Maghreb in the Sahel region, Boko Haram in Central Africa, and al-Shabaab in East Africa.

Another daunting question about the continent is often "Where does Africa appear to be heading?" (p. 417). Chapter 13, "Trends and Prospects" (pp. 417–44), provides a critical-thinking approach to the matter. While listing the significant progress made in the fields of economic growth, democratization, and education during the past decade, the authors "do not underestimate how difficult the road ahead will be" (p. 439). In other words, lack of industrialization, poverty, social fracture, brain drain, political instability, climate change, and overall security will remain primary security challenges in tomorrow's Africa.

The bottom line is that each of the 13 chapters provides cultural insights on African societies that are paramount to understand the major codes and norms that prevail inside civilian and military organizations. A variety of maps, tables, and photographs enhance the text and the reader benefits from the rich bibliography added to each chapter. The first edition of *Understanding Contemporary Africa* was published 14 years ago. The success of the fifth edition confirmed its value as a leadership tool for military education, both at junior and senior levels.

Col Henri Boré, French Marines (Ret)
Africa Desk Officer
Center for Advanced Operational Culture Learning
Marine Corps University

LOOK FOR NEW TITLES IN 2016



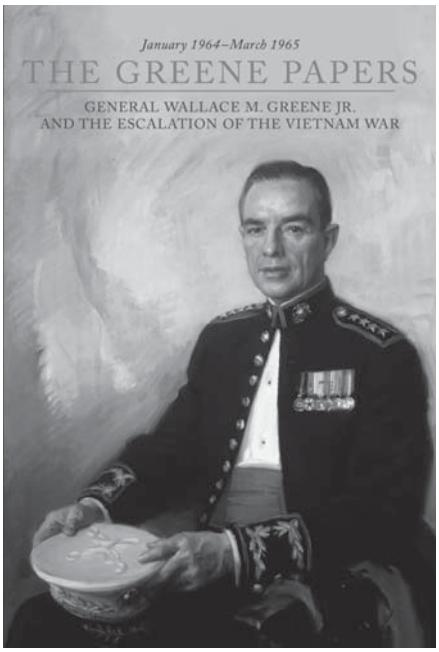
The Crisis of the African State: Globalism, Tribalism, and Jihadism in the Twenty-First Century
Edited by Anthony Celso and Robert Nalbandov
246 pp. Paperback.

The Crisis of the African State focuses on the security issues that plague the African state, particularly the impact of Islamic radicalism, tribal warfare, and jihadism. Contributors include Daveed Gartenstein-Ross, Robert Gribbin, Henri Boré, Ian Spears, and Clarence Bouchat.

Digital copies available at www.mcu.usmc.mil/mcu_press.
For a print version, send request and mailing address to MCU_Press@usmcu.edu.

MCUP
MARINE CORPS UNIVERSITY PRESS

FROM MARINE CORPS HISTORY DIVISION



The Greene Papers: General Wallace M. Greene Jr. and the Escalation of the Vietnam War, January 1964–March 1965
Edited with an introduction by Nicholas J. Schlosser
414 pp. Cloth.

The Greene Papers contains more than 100 documents from the personal papers of the 23d Commandant of the Marine Corps and is the first edited volume of personal papers to be published by History Division as a monograph. Produced by a member of the Joint Chiefs of Staff, Greene's notes provide a firsthand account of the decision-making process that led to the commitment of a large-scale American expeditionary force in Southeast Asia.

Digital copies available at www.history.usmc.mil.
For a print version, send request and mailing address to history.division@usmc.mil.

MCUP
MARINE CORPS UNIVERSITY PRESS
www.mcu.usmc.mil/mcu_press