

FLETCHER SECURITY REVIEW

Vol.3 no.1 | AY 2015-2016

EMERGING DOMAINS OF SECURITY

A FSR Double Issue



Special Edition

In Memory of

Professor William C. Martel

1955-2015

Featuring:

- *LTG Charles Cleveland*
- *Todd Diamond*
- *Anthony Gilgis*

Masthead

ADVISORY BOARD

James Stavridis | Robert Pfaltzgraff | Richard Shultz

Vol.3 no.1 - AY 2015-2016

EDITOR-IN-CHIEF

Meg Guliford

Managing Editor	Colin Bogdan
Budget Director	Geoff Carr
Contributing Editors	Alden Burley
	Neal Hussein
	Maggie Snyder
	Timothy Urban

BOOK REVIEWS/INTERVIEWS

Senior Editor	Henry Nelson
Staff Editor	Hilary Adams
	Spandana Battula
	Ronja Harder
	Robert Pulwer

CURRENT AFFAIRS

Senior Editors	Andrew Koch
	Jenn Wilson
Staff Editors	Paul Huang
	Ian Kapuza
	Andrew Taylor
	Meg Tobin

HISTORY

Senior Editor	Liam Connolly
Staff Editors	Rafael Loss
	Nicolette Roque
	Sydney Stevns
	Michael Wackenreuter

OUTREACH

Outreach Director	Jon Cheatwood
Events Director	Kerney Perlik
Outreach Assistants	Frances Burke

POLICY

Senior Editor	Matthew Keller
Staff Editors	Emily Barnes
	Andrew Clay
	Tanay Tatum
	Alex Zadel

WEB CONTENT

Senior Editor	Kaitlyn Neuberger
Staff Editors	Stephen Allen
	Denise Baltuskonis
	Carmyn Chapman
	Laura Jencik
	Steve Schemenauer
	David Sinclair
	Brianne Smith

HOW TO REACH US:

MAILING ADDRESS

160 Packard Ave, Medford, MA, 02155

WEBSITE

www.fletchersecurity.org

© 2016 by Fletcher Security Review. All Rights Reserved.

Reproduction in whole or in part without permission is prohibited.

Printed in the United States of America.

Cover photo by Charis Tsevis/ Flickr.

Used under Creative Commons License BY-NC-ND 2.0.



Editor-in-Chief's Note



This 2015-2016 special edition of the Fletcher Security Review was developed by the editorial staff to memorialize Professor William C. Martel, whose January 2015 passing stunned The Fletcher School of Law and Diplomacy's community. Professor Martel was a beloved Fletcher faculty member and colleague since 2005. In 2014, the student body awarded him the James L. Paddock Award for Excellence in Teaching. Professor Martel's commitment to his students was evident even in his final semesters at Fletcher, as he taught and conducted guest lectures via Skype.

In his honor, the FSR staff compiled memorial statements from various colleagues with whom he worked during his time at Fletcher. Among these are representatives from the school administration, the Ginn Library, the admissions office, the International Security Studies Program as well as fellow professors and a former Fletcher Registrar. However, no memorial to Professor Martel would be complete without student representation. Thus two of his former doctoral students, Dr. Alison Russell and Colonel Thomas C. McCarthy (USAF), have jointly authored an article on the roadmap for a cyberspace code of conduct.

The theme of this special edition is "Emerging Domains in Security." Coupled with previously unpublished work developed under a prior "Winning Without War" theme, the articles therein honor Professor Martel's diverse, yet forward-leaning, research interests. This edition maintains the journal's four traditional sections of policy, history, interviews, and current affairs. Our authors include established academics and practitioners as well as two Fletcher students, Nikolas Ott and Michael Wack-enreuter.

Each of the articles analyzes critical issues in the study and practice of international security, and our authors make salient arguments about an array of security-related issues. The articles are borne out of countless hours of work by FSR's dedicated editorial staff. I deeply appreciate the time and effort they have devoted to the publication of this volume. They are full-time graduate students who masterfully balanced a host of responsibilities.

I must express my gratitude for my Managing Editor (Colin Bogdan) and Senior Editors (Carmyn Chapman, Liam Connolly, Matthew Keller, Andrew Koch, Hank Nelson, Kaitlyn Neuberger, and Jenn Wilson) for working diligently as we instituted fundamental changes in FSR's business processes. I owe a very special thanks to our Directors for Budget (Geoff Carr), Outreach (Jon Cheatwood), and Events (Kerney Perlik) for improving the journal's finances and overall strategic direction.

On behalf of the entire staff of the Fletcher Security Review, I must thank the Fletcher faculty and staff for their deep support, particularly our Advisory Board members, Dean James Stavridis and Professors Richard Shultz and Robert Pfaltzgraff. Over the past year, we have sharpened our focus not only to publish engaging literature on a host of topics, but also to serve as a forum for conversations about security with practitioners, such as Sina Beaghey, Colonel Jimmy Blackmon, and Anthony Gilgis.

It is my honor to serve as the Editor-in-Chief of the Fletcher Security Review, and I am already excited for the next year. This 2015-2016 special edition of the Fletcher Security Review was developed by the editorial staff to memorialize Professor William C. Martel, whose January 2015 passing stunned The Fletcher School of Law and Diplomacy's community. Professor Martel was a beloved Fletcher faculty member and colleague since 2005. In 2014, the student body awarded him the James L. Paddock Award for Excellence in Teaching. Professor Martel's commitment to his students was evident even in his final semesters at Fletcher, as he taught and conducted guest lectures via Skype.

In his honor, the FSR staff compiled memorial statements from various colleagues with whom he worked during his time at Fletcher. Among these are representatives from the school administration, the Ginn Library, the admissions office, the International Security Studies Program as well as fellow professors and a former Fletcher Registrar. However, no memorial to Professor Martel would be complete without student representation. Thus two of his former doctoral students, Dr. Alison Russell and Colonel Thomas C. McCarthy (USAF), have jointly authored an article on the roadmap for a cyberspace code of conduct.

MEG K. GULIFORD
Editor-in-Chief

FSR Remembers Professor William Martel



William C. Martel (1955–2015), an associate professor of international security studies at the Fletcher School, is remembered as a leading scholar in the foreign policy community, but equally as an unusually devoted teacher and caring individual who always put others before himself. Martel’s books include *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy* (Cambridge University Press, 2015) and *Victory in War: Foundations of Modern Strategy* (Cambridge University Press, 2011). He was a frequent contributor to print and broadcast media on international security issues and was active in national and New Hampshire politics. He served as a senior foreign policy adviser to Mitt Romney during his 2012 presidential campaign. Martel was also the principal investigator in joint Fletcher School-MIT Lincoln Laboratory studies that formulated cyber codes of conduct and outer space rules of engagement. A 2013 Boston Globe profile of Martel described him as “among a handful of scholars and military experts trying to solve one of the most nettlesome problems in modern foreign policy: coming up with a new definition of ‘victory’ that matches the complexity of our conflicts.” Martel was chosen by the Fletcher student body to receive the James Paddock Award for Excellence in Teaching at the Fletcher commencement ceremony in May 2014. Fletcher School Dean Admiral James Stavridis stressed that Martel’s contribution to the spirit of the Fletcher community cannot be underestimated. “Bill personified what the Fletcher School is all about,” Stavridis said in a letter to the Fletcher School community. Martel served three years as chair of Fletcher’s admissions committee. After graduating from St. Anselm College, Martel earned a Ph.D. in political science at the University of Massachusetts, Amherst, and was a postdoctoral research fellow at Harvard’s Kennedy School of Government. Prior to joining the Fletcher School faculty in 2005, Martel was professor of national security affairs at the Naval War College. He also worked at RAND Corp. in Washington, D.C., and served as an adviser to the National Security Council, a consultant to the Defense Advanced Research Projects Agency, the Office of the Secretary of Defense and the U.S. Air Force. He was the founder and director of the U.S. Air Force’s Center for Strategy and Technology. Martel is the son of the late Cyprien Martel. He is survived by his wife, Dianne; his children, William Cyprien Martel Jr. and Catherine Martel of Washington, D.C.; and his mother, a sister and two brothers.

“Fletcher could use a heck of a lot more Bill Martels.”

Laurie A. Hurley, *Director, Office of Admissions & Financial Aid*

Anyone who had the pleasure of knowing Professor Martel would readily describe him as a very nice guy and a friend to all. He would literally go out of his way to offer his assistance to a student, colleague or stranger. First and foremost, Professor Martel was enthusiastic about his teaching and his students. Students were as captivated by his lectures and research as they were by his daily reports of skiing conditions in Maine. He would move around Fletcher with a bounce in his step, a big smile on his face and a twinkle in his eyes. He was both a giver and recipient of warmth and respect in all circles. The Fletcher School Admissions team was especially fortunate to have worked with Bill Martel. He served as the Faculty Chair of the Committee on Admissions for three wonderful years, allowing us to experience his true thoughtfulness as a person and decision maker. He always created an inclusive and positive environment for discussion and decision making. Bill truly valued the collaborative process and encouraged participation from everyone around the table, especially the student members of the committee. For each committee meeting he was tasked with reading several applications and arriving with notes and a tentative decision. He would carefully read and make notes on each and every application; however, he would often come to the meeting without making a decision. Bill sincerely preferred to listen and engage in the conversation first before making a final judgment. He absolutely loved it when the group was getting close to making a decision, only to be led in the opposite direction by a last minute comment by a committee member. He relished these special moments. After exhausting five-hour meetings, Professor Martel would leave the room with the same energy with which he entered. He would often return to his office and quickly dash off an email to everyone on the committee thanking them for their hard work and participation, and he genuinely meant it. Jessica Daniels, Senior Associate Director of Admissions, summed it up best in an admissions office blog post: “Bill was a true friend to the admissions office, and we loved working with him. The Fletcher faculty is loaded with nice people, but in any group of nice people, someone can still be the nicest. Bill was the nicest.” In our day-to-day work, the Admissions team is often reminded of Professor Martel, especially when we are planning an Open House or discussing tricky cases during admissions committee meetings. We will always keep him close in our hearts and minds.

Nora Moser McMillan, *Registrar/Manager of Student Academic Programs, 1994-2015*

Optimist is the first word that comes to mind when I think of Bill Martel. He possessed a joyful outlook in life. It was infectious and you could not help but smile and take on that optimism when in his presence. Even when things were not going

well, he always sought out the positive. Although he was a very accomplished scholar and teacher, this is the lesson that I will carry forward in my life.

Professor Robert L. Pfaltzgraff, *Shelby Cullom Davis Professor of International Security Studies*

Each of us who was privileged to know Bill Martel can point to qualities that made him great; humility, kindness, service to others, optimism, magnanimity, good will, and serenity in the face of adversity. No matter how much you cared about Bill – and we all cared greatly about him – he cared even more about us. I observed this not only in my case, but also in Bill’s interaction with other colleagues and, above all, with the legions of students and others inside and beyond Fletcher whose lives Bill touched. This led him to go out of his way to help so many. He was never too busy to offer to take on a new assignment. He simply did not know how to say no. He took on new burdens to help you cope with yours. This magnificent quality framed Bill’s willingness to undertake far more than his share of tasks – from serving on and providing leadership on important committees, supervising Ph.D. dissertations, or taking his students on field trips to reinforce and go beyond his impressive classroom performance that won him a teaching excellence award. Bill was a scholar, and his devotion to his students, together with a broad range of academic interests reflected in teaching and publications, could hardly have been a better fit for Fletcher. Bill leaves us with many memories and a rich academic and personal legacy. Always the optimist, he enjoyed life to the fullest. His infectious enthusiasm and good cheer radiated through and beyond this building for many years and is greatly missed. We are all so much better for having known, worked with, and benefited from Bill’s manifold contributions. He will remain a role model for all who had the good fortune to know him here at Fletcher and beyond.

On Behalf of the Ginn Library Staff, Cyndi Rubino, Director of Information Services, Ginn Library/IT, and Ellen McDonald, Reference Librarian, Ginn Library

University libraries are places for scholarship, exploration and collaboration. It’s no wonder that the staff at Ginn Library all loved Bill Martel. In a world sometimes plagued by insecurities and egos, Bill approached each research and technology quest with humility, inquisitiveness and patience. He was always quick with a smile and never too proud to ask questions and seek assistance. His friendly, open demeanor was infectious... you couldn’t help but be your best, most generous and creative self when you were around him. After Bill’s diagnosis, he never missed a beat in using Skype to teach remotely from his hospital and home. Using technology and library services, Bill embraced new resources to support his scholarship and classes. Continuing to make himself available to students and colleagues, Bill made time to advise on capstones and mentor his many devoted

students. He was always gracious and appreciative - even the smallest gestures were noticed. Never once complaining about the fickleness of technology, always patient with troubleshooting, Bill was the model of kindness and understanding. We will always remember Bill for his strength, courage, and optimism in the face of a heartless disease. But we will always be grateful for his everlasting lessons about quiet humility, generosity, and human kindness.

“A scholar, teacher, athlete, and – above all—a beloved husband and father—he is the embodiment of all that we treasure here at Fletcher.”

Gerard Sheehan, Executive Associate Dean

Bill and I chatted regularly in the corridors, in meetings, occasionally in my office, and quite often we seemed to meet and have our longest conversations in the Fletcher parking lot before each heading home. It was in the Fletcher parking lot that I learned about his political activities, his love for skiing (that he had ski jumped in high school!), all things New Hampshire, a bit about his family, and of course, we shared the weekly intrigue of Fletcher. The sum of all these conversations was that, to me, Bill was the most preternaturally positive person I have ever met. He was relentlessly upbeat, able to put a positive twist on all development. Almost any conversation that might touch on my concerns ended with a genuine offer: “let me know if there is anything I can do to help.” And Bill did help often, not only me but many others at the School. In my case, it often revolved around events or speakers or funding, or other support for students. He never once turned down a request to step in and assist, and when he did take on a task, he really took it on; no need for follow up, no need for checking in. He simply did it, and with great good cheer - his classic two-punch of energy and enthusiasm. His kindness was on daily display. I am pretty certain that every conversation I ever had with Bill touched on how I was doing. And that of course is how he interacted with everyone. Bill, unequivocally, was well liked by all. During his tenure review year, I had innumerable conversations with staff who were universally pulling for him....not only because he was considerate to all (though that surely was prominent in their thoughts) but because the tenure criteria that staff could observe, that is, service to the School, and great teaching and engagement with students, were clearly off the charts. Bill was appreciated by members of the Tufts community as well. I remember the manager of Tufts catering services telling me how deeply respected Bill was by the University’s catering staff as well as the staff of Mugar cafe, all of whom he knew by name. Really not surprising. Bill connected with everyone in the community. No one was ever faceless or nameless to Bill. In the end, leaving aside all his many scholarly and professional accomplishments, perhaps the best

tribute is that Bill was just a genuinely good guy. No pretensions. No artifice. No ego. Kind. Caring. Helpful. Cooperative. Positive. Just a really good guy.

Professor Richard Shultz, Director, International Security Studies Program

Bill Martel is the model of what The Fletcher School should demand in its faculty and what its students certainly deserve. To borrow a term from Carl von Clausewitz, the Fletcher student body was Bill’s professional center of gravity, and teaching, mentoring, and launching them his core professional interest. At Fletcher there are faculty that embrace this aspect of their professional activities as the most important thing they do, and Bill was a charter member of that club. He was a real difference maker in the lives of a legion of students. Fletcher was his natural habitat, and Martel was a difference maker in a school that produces difference makers. No one could be more positive, more encouraging, and more concerned that “all’s well” with you than Bill. When he would pop into the doorway of my office and cheerfully ask me if “all was well” I knew there was nothing perfunctory in his question - he meant it! And when I sometimes would growl back at him, jokingly, “nooo, all is not well,” his first reaction was to take the bait and ask- “what can I do to help?” Bill was a wonderful friend and colleague, a treasure to Fletcher students, a scholar, and a thinker who influenced leaders. Bill lived by the adage “attitude is everything,” and he instilled it in others. It is captured in his often-repeated maxim to his students to “always have a positive attitude, even when facing the most difficult challenges in the future.” He would tell them, “being positive is an essential ingredient for achieving success in all things that are really important in life.” Fletcher could use a heck of a lot more Bill Martels.

Kathy Spagnoli, Grants/Staff Assistant

Although we worked together briefly, I am so privileged to have had the opportunity to meet Bill Martel. I have worked at Tufts for almost ten years and he was one of the most caring faculty members that I have met. His highest priority was his students, and he treated all faculty and staff with the utmost respect. I spoke with him often by phone during his treatment and his positive attitude and spirit amazed me. He was smart, passionate, worldly, but so down to earth at the same time. Fletcher was lucky to have him. He always made me smile, and I miss that.

“His friendly, open demeanor was infectious... you couldn’t help but be your best, most generous and creative self when you were around him.”

James Stavridis, *Admiral, USN (Ret), Dean of The Fletcher School of Law and Diplomacy*

Professor Martel was among the most brilliant scholars of modern security studies and particularly national strategy this nation has produced. His two books on the subject are literally on the desk of most senior military officers. As a former Supreme Allied Commander of NATO, I often referred to his theories and scholarship on the appropriate uses of national power in keeping our country safe. He was also the best pure teacher at Fletcher, beloved by his students. Even while he was suffering with advanced cancer, he continued to teach his courses by Skype, further endearing himself to his students. He mentored a record number of graduate students on their capstone thesis projects, and led the annual skiing trip to the mountains of New Hampshire. When his death was announced at Fletcher, I walked through the corridors and saw many of our 600 graduate students in tears. His energy, enthusiasm, and courage in facing the disease that ultimately took his life were noteworthy and emblematic of a marvelous colleague whose memory will burn bright at this school for generations. He was awarded tenure in the final weeks of his life, and never was I happier than letting him know that he had attained that honor. A scholar, teacher, athlete, and —above all— a beloved husband and father—he is the embodiment of all that we treasure here at Fletcher.

Liz Wagoner, *Associate Director, Office of Admissions & Financial Aid*

I only knew Prof. Martel for a short time, but it sure was memorable! I was lucky enough to sit with him on the Admissions Committee for two years and always enjoyed chatting with him before and after the official meetings. He and I always had a special friendship as he grew up in Lewiston, where I went to college – so we’d talk all things Maine. We also had some great chats about New Hampshire, as I grew up near Bedford and have a deep appreciation for all things “603.” On the Admissions Committee he was also such a thoughtful and kind presence, always finding the good in every applicant. He was a true friend of Admissions, always happy to help whenever we needed something. Moreover, he saw us as peers and didn’t hesitate to ask us “what our gut was telling us,” which I always valued. He stood out amongst the other faculty here for his sense of humor, compassion and thoughtfulness, and was truly one of a kind. We miss him dearly and, to this day, we often remember his words of wisdom as we consider our Admissions cases.

Roadmap for a Code of Conduct for Cyberspace

by Thomas McCarthy / Alison Russell

Policy makers also face the truly modern challenge of cyber warfare in the hands of non-state actors. Never before have non-state actors, groups, and movements possessed an instrument capable of inflicting such immense harm. One element of American grand strategy must consider how to deal with groups that could attack the physical and economic infrastructure of American society. Policy makers worry that cyber hackers from an extremist organization might be able to cut off U.S. electric power during the winter or hack into the safety controls of a nuclear reactor. The old grand strategy of containment has become passé in the face of modern foreign and domestic challenges represented by these new and unpredictable sources of disorder.
– Professor William C. Martel¹

Professor Martel, author of *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy*, offers three guiding principles for U.S. grand strategy: rebuilding domestic foundations of power; exercising American leadership to restrain sources of disorder that directly threaten U.S. vital interests; and forging both alliances and partnerships to confront the most pressing threats to global stability.² The last of Martel's three principles foreshadows the three cyber security activities at the heart of the newly released U.S. Department of Defense Cyber Strategy.

The three activities around which the new U.S. DoD cyber strategy revolves are: Information sharing and interagency coordination; building bridges to the private sector; and building alliances, coalitions, and partnerships abroad.³ These three coordinating and collaborating activities are the key to building relationships between actors influencing the development of the cyber domain, and are necessary to identify and counter threats. To advance global cyber security, the Cyber Strategy suggests the U.S. must “build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.”⁴ As part of this effort, the United States seeks to build security relationships to respond to shifts in the international environment, including sources of disorder. These relationships are built upon trust and cooperation of many actors with varied interests and objectives in cyberspace. Given the wide variety of actors and interests within the cyber domain, establishing relationships of trust based on a shared un-

derstanding of acceptable conduct, expected behavior, and governing principles represents a daunting challenge.

Cooperation in Cyberspace

Cooperation is a necessary component of growth for any regime. Key aspects of cooperation include trust in the system and the predictability of action among participants. Through consistent and transparent actions, participants in a cooperative environment create a predictable pattern of behavior. This predictable pattern of behavior helps participants learn what to expect from each other and establishes a baseline for future transactions involving greater risk and reward.

The challenge for all actors in cyberspace is to create relationships of trust in the absence of a global authority to impose order on states and institutions. Within cyberspace, as with the development of predictable interactions in other fields of human interaction, codes of conduct can serve to provide a framework from which regime participants will continue to build trust in a systematic way. Codes of conduct, both formal and informal, are developed through repeated transparent interactions. They effectively set expectations of behavior that form a baseline of assessment regarding another participant's consistency and transparency. The goal of formal and informal codes of conduct is to develop a system where actors work with common purpose towards the benefit of all.

Why is a Code of Conduct Important?

A code of conduct is defined as the “principles, values, standards, or rules of behavior that guide the decisions, procedures and systems of an organization in a way that (a) contributes to the welfare of its key stakeholders, and (b) respects the rights of all constituents affected by its operations.”⁵

These principles and expectations, if widely shared, can transcend geographic, economic, and cultural boundaries and blossom into behavioral norms within the group. While norms

themselves are not binding, they are supported and reinforced through socialization and the fear of reputational-loss for transgressions against others. In an environment characterized by repeated interactions, a code of conduct provides the framework for assessing actions, establishing reputations, and demonstrating consistency in behavior.

Although not specifically covered in formalized law or treaty, codes of conduct serve as a universal frame of reference for the promotion of common understanding and the employment of “good judgment” as defined by participants. Standards of behavior spread, and come to functionally define ethical behavior across communities of interest and are even formalized by treaty, widely recognized, and internationally enforced (i.e. the Law of Armed Conflict or the Law of the Sea). Codes of conduct thus serve to regulate and place limits on our actions in the absence of formal enforcement mechanisms and serve as a frame of reference for evaluating the actions of other.

Eventually, well-established codes of conduct lead to self-regulation among the participants and communities of interest, building trust and encouraging frequent interaction. Within the cyber domain, codes of conduct serve to define relationships via the sharing of information, freedom of movement of information along global lines of communication, cooperative enforcement of mutual standards of international law and behavior, and improved communications based on standardized expectations.

How Does a Code of Conduct Apply to Cyberspace?

Much like cooperation in other domains of human competition and conflict, a cyberspace code of conduct will develop based on informal interaction by parties seeking mutual benefit through repeated interactions. Cyberspace catalyzes cooperation when strategically and creatively applied in the dynamic arena of our increasingly connected world. Success will breed success by establishing norms and rewarding conforming partners. Over time, those seeking to maximize individual benefits will become less desirable partners for interaction, gradually forcing them to adapt group norms or endure increased transactional costs. Consistency over time is the key component for development of a code of conduct for cyberspace.

Unfortunately, the pace of innovation, the technological development within cyberspace, and the relative anonymity of actors are likely to hamper development of widely accepted and enduring codes. While there are repeated interactions, it is often difficult to verify the identity of other actors and constant improvements in technology result in an ever-changing variety of interactions requiring thoughtful, and sometimes creative, responses. Thus, unlike other codes of conduct, a code of conduct for cyberspace would demand continual attention, evolution, awareness, and both an ability and a willingness to adapt to new norms of behavior among a wide variety of actors.

Ideally, as a code of conduct becomes widely accepted by leading

actors and powerbrokers within the international community, it is formalized and serves as the basis for legal restrictions to behavior. Unfortunately, competing governmental, legal, and cultural norms among cyber actors have thus far prevented and slowed the establishment of common understandings, not to mention formalized agreements. The process of overcoming differences in international norms is underway however; we have already seen the first steps of this process in cyberspace. Legal frameworks such as the European Union’s Convention on Cyber Crime have helped establish standards of behavior for its signatories since 2001. Unfortunately, no country in Asia, Africa, or South America has signed it, so its global application is limited. More recently, the Tallinn Manual on International Law Applicable to Cyber Warfare began to extend legal frameworks into cyberspace regarding rules of conduct in cyber conflicts, but there are neither formal international cyber laws nor international agents to enforce compliance.

Process of Development

A code of conduct provides a foundation for future cooperation and, because it would be voluntary, it may be able to attract participants that would not be willing or able to commit to a legal agreement. There are a variety of different actors operating in cyberspace with different legal standings and authorities, whether they are individuals, non-state actors, state-sponsored groups, states, or intergovernmental organizations. A code of conduct could provide the framework for defining and measuring behavior of all actors, not just states, and thus be more inclusive and comprehensive even if enforcement is difficult against some groups such as non-state actors. In cyberspace, actors are not assessed by their size, wealth, or capabilities but by their actions. Creating a framework to assess their actions allows for a common understanding of cooperative and professional behavior across actors in cyberspace.

The United States and other countries have engaged in a process of developing a framework for cooperation—or, at least, conflict avoidance—in cyberspace for years. For example, in 2013, the U.S. and Russia signed a pact to create a communications link on cyberspace issues, so that the activities of one state may not be misinterpreted as hostilities against the other.⁶ In April 2015, the U.S. and Japan drafted an agreement on bilateral defense rules that will bolster their efforts to defend cyberspace, particularly with regard to information sharing and critical infrastructure protection.⁷ South Korea and the United States have also recently vowed to work more closely together on cyber security, especially with regard to cyber attacks emanating from North Korea.⁸ Other types of bilateral cooperative efforts can also take place within the broader landscape of NATO and EU cooperative agreements on cyberspace. The U.S. appears to be building norms in cyberspace through a combined effort of bilateral and multilateral agreements that allow for flexibility in order to make the most progress on a variety of issues with a wide range of partners.

In this context, it is important to note that the private sector is also involved in developing standards of behavior. Microsoft has recently proposed six international cybersecurity norms aimed at limiting conflict in cyberspace through a multi-stakeholder approach. Many of the proposed norms focus on supporting the integrity of private sector information and communications technology companies while protecting civil society from cyber conflict.⁹

From the pure Hobbesian perspective, cooperation among actors seeking to gain advantages over one another will not develop without a central authority to enforce rules of behavior. However, we see cooperation among international actors everywhere. Realists, liberals, and constructivists argue about why cooperation occurs, but all acknowledge it occurs and has an effect on the relationships between actors, even if only because each seeks reciprocity to pursue an individual advantage.

According to R.M. Axelrod, reciprocity is, effectively, cooperation.¹⁰ Within systems of constant and ongoing interaction, it is the expectation of future interaction that overshadows actions in the present, creating a desire to act in accordance with norms, or in some cases codes of conduct. Within the cyber environment, the almost certainty of future interaction can act as a motivating force and is arguably a critical factor in, and incentive for, cooperative behavior. It is in the interest of most, if not all cyber actors to be easily distinguished as non-adversarial by acting in compliance with established norms of behavior, and to develop a reputation for adherence to expectations.

The most important benefits of cooperation and codes of conduct in cyberspace are that they can lead to an advancement of interests and reduce the overall risk of conflict as a result of miscalculation or misunderstanding. The single biggest challenge to cooperation is establishing codes of conduct that provide benefits of compliance to the actor, and are thus mutually beneficial for the parties involved. Over time, increased trust can lead to more permanent and formal cooperation in the cyber domain.

Despite the benefits of cooperation and collective action to regulate or govern cyberspace, not all states and actors are in favor of it. Many states say that they want a regime such as a treaty or a less formal code of conduct for cyberspace, yet differ drastically in what they want and why. Individual states have very different priorities in cyberspace. As such, they have different levels of concerns on a variety of issues making it difficult to reach consensus. Among major cyber powers, including the United States, there are concerns that treaties might reduce flexibility to pursue national interests, while simultaneously enabling other countries to build disruptive cyber capabilities or, worse, gain competitive advantage by ignoring the rules all together. In addition, the cost of organizing a collective effort increases with the size of the group. In large groups, it is difficult to establish and enforce selective incentives to shape interactions. In smaller groups, societal pressure and intense focus helps to provide the incentive for compliance.

Within any large system, it is impossible to have first-hand knowledge of all potential partners; therefore, reputation becomes the key to initial and future interactions with new acquaintances. Reputation affects how actors view and react to each other. Successful interactions increase positive reputational aspects and provide mutual benefit, increasing the return for both participants and strengthening them within the operational system. Witnessed by others, success is emulated.

Reciprocity operates both as a reward and a penalty. If a state abides by the rules, then it can reasonably expect others to do that same. In the construct of greater responsibility, states will help each other to insure good treatment for their own interests. However, if a state defects or fails to abide by the norms, then other actors no longer owe them reciprocity in future events. To make sure other nations are forewarned of defectors actions, recently, there has been a greater willingness on the part of some countries, like the United States, to engage in public “naming and shaming” of norm-breakers, such as Chinese hackers or North Korea.

Establishing reputations and transparency of action within the cyber domain is a difficult challenge. The potential for anonymity during interactions leads to risky behavior where actors are not held accountable for failure to comply with norms of behavior. This lack of transparency and accountability among the larger community of actors means that codes of conduct must begin among trusted actors, actors likely to have long standing and trusted relationships based in other domains of diplomacy and commerce. Likewise, willingness to engage in reciprocity when wronged also helps establish a reputation for action and enforces norms.

Attribution is one of the thorniest issues in cyberspace. Because the network was designed to operate with trust and minimal security checks, individuals, non-state actors, and states can mask or fake their identities. Programs, such as The Onion Router (Tor), exist to make cyber attacks or other illicit behavior extremely difficult to trace back to their origins. Even when the physical origin of a cyber attack is known (i.e., the IP address has been successfully traced), the next challenge is to prove who the user was at the time of the attack, and under what authority were they operating (individual hacker, part of a non-state group, or agent of a state). Definitive attribution is often impossible but hybrid approaches, such as those used to track down Ross Ulbricht, the founder and operators of the Silk Road, are increasingly effective.¹¹ By combining cyber and non-cyber means authorities are developing the means to attribute on-line actors with their real world counterparts. Still, these methods typically take days or weeks, whereas cyber attacks can be instantaneous and the victims may seek to retaliate immediately.

A willingness to act, combined with predictability consistent with established norms, is the key to building a reputation and acting as a role model. The overall system is strengthened when reputation allows even new partners to act in good faith expecting others will act in compliance with the code of conduct. By excluding non-compliant actors, those within the system create

pressure that leads to behavioral change. Finally, the reputation of states for compliance can create prestige within the community.

Conclusion and Roadmap Ahead

The normative power of codes of conduct provides a basis from which to address the behaviors of the wide variety of actors within the cyberspace domain. Many of the existing codes of conduct, both formal and informal, have emerged through the leadership of the major actors who set standards and impose costs on those unwilling to act in accordance with these standards. As part of this process, leading actors who stand to benefit from the establishment of widespread and powerful norms of behavior must create transparency as they work to reduce the potential for misinterpretation of actions.

In that tradition, the following roughly outlines a practical guide, or road map, for the creation of a code of conduct for cyberspace. First, epistemic communities should continue developing their own codes of conduct for their specialized areas. It is necessary to begin with small groups because the benefits of cooperation are specific and clear, and the framework for cooperation is likely limited to the issues of greatest importance. As various communities accept established norms, the collection of smaller codes of conduct, when taken together, will begin to provide a framework informing a broader, more comprehensive approach.

In order to reach that more comprehensive code of conduct, there must be consultation between states and communities of experts for the creation of international agreements and domestic laws or policy. Extant treaties or codes of conduct in other domains, such as the 1967 Outer Space Treaty, may provide useful assistance in developing the code of conduct and generating interest. Martha Finnemore, scholar of international cooperation, describes a “grafting” process whereby a new code of conduct can leverage existing frameworks and ideas for support.¹² International agreements can start between any states, but cooperation theory suggests that territoriality and proximity matter: it is easiest and most productive to begin formalizing behavioral expectations with your neighbors.

Proximity in cyberspace however, is hard to define. There are two potential ways for nations to proceed; either with their geographic neighbors or their “cyber neighbors,” the nations with whom they interact most often through cyberspace. For the United States, this could mean collaborating with Canada and Mexico, geographic neighbors, or major trading partners such as the United Kingdom, Germany, Japan and China. Once cooperative agreements have been tested and established with neighbors (however defined), participants can open the code of conduct to others and attempt to expand its reach.

Given the rapid advancement of technology, large number and variety of actors, attribution challenges, and competing interests of actors within the domain, creating a cyber code of conduct will likely be a long process. Regardless of how the process un-

folds, two things are clear: a successful cyber code of conduct will require a collaborative, multinational effort; and all collaborative efforts need a leader. The United States, by virtue of its influence in the world and its position at the forefront of cyber technology, should lead the way and forge alliances to create a code of conduct in cyberspace that will restrain cyber sources of disorder that threaten U.S. vital interests and global stability.

Colonel Thomas McCarthy, Ph.D., is a 2012 Fletcher graduate and the Commandant and Dean of the USAF’s School of Advanced Air and Space Studies, Maxwell AFB, Alabama. Commissioned in 1990 from the Air Force Academy he is an active duty officer with world wide operational and strategy development experience. Prior to his current position, Colonel McCarthy served as Director for the USAF’s Center for Strategy and Technology conducting studies to identify key characteristics of the military operating environment 30 years in the future. The opinions expressed are Colonel McCarthy’s alone and do not necessarily reflect those of the United States Air Force, the Department of Defense, or the United States Government.

Alison Lawlor Russell, Ph.D., is a 2012 Fletcher graduate and an Assistant Professor of Political Science and International Studies at Merrimack College in N. Andover, MA. She has taught course on Cyber Security, International Politics, and American Foreign Policy, among others. Dr. Russell is also a non-resident Research Scientist at the Center for Naval Analyses, where her works includes cyber security, maritime strategy, critical maritime infrastructure protection, and global engagement strategy. Dr. Russell is author of the book *Cyber Blockades*, which was published by Georgetown University Press in 2014.

-
1. William C. Martel, *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy* (New York, NY: Cambridge University Press, 2015), 350.
 2. Ibid.
 3. “U.S. Department of Defense Cyber Strategy,” (U.S, Department of Defense April 2015), 3-4.
 4. Ibid.
 5. International Federation of Accountants, “Defining and Developing an Effective Code of Conduct for Organizations,” in *International Good Practice Guidance* (2007), 5-6.
 6. Ellen Nakashima, “U.S. And Russia Sign Pact to Create Communication Link on Cyber Security,” *The Washington Post*, June 17, 2013.
 7. Cory Bennett, “U.S., Japan near Cyber Defense Agreement,” *The Hill*, April 8, 2015; Franz-Stefan Gady, “Japan and the United States to Deepen Cybersecurity Cooperation” *The Diplomat*, June 2, 2015.

8. Cory Bennett, "U.S. Vows Tighter Cyber Cooperation with South Korea," *The Hill*, May 18, 2015.
9. Angela MacKay et al., *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (Microsoft, 2014).
10. R.M. Axelrod, *The Evolution of Cooperation* (Basic Books, 2006).
11. For more information on the law enforcement operation capture Ulbricht see: <http://www.wired.com/2015/05/silk-road-2/>.
12. Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age*, ed. Kristen Lord and Travis Sharp (Center for a New American Security, 2011).

Special Operations Today:

FSR Interviews LTG Charles Cleveland (Ret.), Former Commanding General, USASOC



Lieutenant General Charles T. Cleveland, an Army Special Forces Officer, relinquished command of the United States Army Special Operations Command (USASOC) and retired after 37 years of military service on 01 July 2015. He previously commanded the Special Operations Command Central and Special Operations Command South as well as the Combined Joint Special Operations Task Force-North during Operation Iraqi Freedom. LTG Cleveland is a native of Arizona and a 1978 graduate of the United States Military Academy at West Point, New York. His military awards and decorations include the Defense Superior Service Medal and the Legion of Merit Medal.

FSR: Are you concerned that an increase in the use of SOF [Special Operations Forces] in high-profile and sometimes unavoidably political circumstances erodes the division between strategy and tactics in the national security paradigm? That US policymakers are or will become addicted to quick results and no longer have the political will to develop and pursue longer term, more comprehensive solutions?

LTG Cleveland: I think that is potentially a valid concern. I'm not sure I see it evidencing itself yet. I'm not certain that the use of SOF has reached that point. I do think that the reason SOF is being used is important to examine and that it may point to issues about how we look at our security challenges. I think that that's what we are trying to do at USASOC [United States Army Special Operations Command]. We're trying to frame this discussion. You mentioned earlier the connection between strategy and tactics. This is a critical space that we refer to in our doctrine as the Operational Level of War. It is in this space that the art of campaigning resides. It is in this space where we describe how our tactical actions will achieve those strategic goals set by our policymakers. The Army has done significant work in its schoolhouses to train its planners to think creatively about 'wicked' problems facing the nation and to develop novel solutions. As part of our ARSOF 2022 efforts at USASOC, I asked the question, "How well do we understand what we're facing, and how prepared are we in SOF for prosecuting these new types of campaigns? And where do we train our SOF Campaign Planners who will develop our SOF Operational Art?" It was

clear that we had to mature the SOF profession, especially in this vital space between tactics and strategy. Not only that, but we needed to write our own doctrine in order to stand as equals with our peers in the conventional army and further the discussion about how we should be approaching these complex challenges and what SOF's role should be in these new campaigns.

FSR: As a quick follow-up, do you feel that this understanding that you are treating a symptom and not a cause in a lot of these operations is widely shared and understood across the various aspects of government?

LTG Cleveland: I'm an Army component so I am limited in my current capacity in how much I talk to those outside the Army. I'm not so sure that it's universally a concern yet. I'm not sure that other government agencies or other folks see the problem the way we see it. In part what we are trying to do here [leading a discussion at the Fletcher School of Law and Diplomacy] is create the dialogue for that. We have had some successes, however. We have hosted semi-annual strategic war-games called Silent-Quest, in which we explore future threats and approaches to dealing with those threats. The idea being to integrate the findings of these exercises into our capabilities development and strategic planning processes. One benefit of hosting these events has been the significant participation we have enjoyed from the interagency. We have had individuals like Ambassador Thomas A. Shannon, Counselor to the Secretary of State, attend and provide crucial insights and feedback to help mature our thinking. In the end, there are various perspectives on the threats to our security and their root causes. One's perspective is understandably shaped by where one sits in the nation's security and diplomatic apparatus. The key for us has been to continue to drive a vibrant dialogue to forge common understanding.

FSR: In a recent series of meetings at the RAND Corporation, you stated: "I don't think we completely understand the fight that we are in and that this is unlike anything that we've confronted in our past." After 14 years of conflict and war, what do you think needs to change for the US writ large, and within your community to reach the necessary level of understanding these wars?

LTG Cleveland: To get to understanding about what we are currently confronting, we have to take off our blinders as military professionals and look at the security problem. Our premise is that the economic, social, political, and ideological trends in international competition are converging among State, Non-State actors and others in a new type of security paradigm. As you mentioned in your question, we've been in a particular type of combat for 14 years. Our thinking at USASOC is that the security problems of the future will not necessarily resemble those of the past. It is in this context that we feel that SOF forces are uniquely capable, through our persistent global engagement, to shape things well before crises develop. The fact of the matter is, that we are in competition with various state and non-state actors for physical, cognitive, and moral security of populations and increasingly, in this hyper-connected world, the notions of

sovereignty and identity". We have to develop a portfolio of new approaches to impose a cost calculus on our adversaries in this space, but first we must recognize and accept that the security paradigm that we grew up with has changed fundamentally. Our efforts to drive the discussion of Operational Design and explore a SOF variant of Operational Art that I mentioned earlier are aimed at just this problem.

FSR: You were also recently quoted as observing that the US has exquisite capabilities to kill people, while what it needs are exquisite ways to manipulate them. Are you concerned then that the counterterrorism aspects of SOF have in recent years been prioritized over other capabilities, such as MISO [Military Information Support Operations] and Civil Affairs? If so, what is driving that imbalance, and how can a constituency be built for possibly expanding other capabilities?

LTG Cleveland: SOCOM [US Special Operations Command] is still fairly young in terms of its history, 27 years. One must remember that the command was established with the specific goal of providing the nation a set of highly developed tactical tools that could operate at unprecedented levels of proficiency, and when applied, would episodically achieve strategic effects.

As the post-Cold War international order has become more and more chaotic, and the threats to the nation have become more complex and asymmetric, we have found ourselves militarily engaged in much longer duration campaigns, and these campaigns necessarily have multiple dimensions to them. There are Influence, Governance, and Capacity Building lines of effort to these campaigns for which our Special Forces, PSYOPS and Civil Affairs units are purpose-built.

Though these capabilities have long been part of the USASOC portfolio, they have only recently risen in prominence as we find ourselves winding down two large scale conflicts and committed to myriad smaller persistent engagements across an increasingly disordered security landscape. There is an element of this problem that is simple education. The hyper-focus on counterterrorism aspects of SOF is not intentional. We have to better inform our policymakers and national security thinkers about the broad continuum of SOF capabilities that USASOC provides the nation. We need to help them rediscover what SOF has been doing since its inception.

Influence operations are a great example of this. We need to put more resources against further developing this capability, but we must also show our policymakers how effective influence operations can be. An unfortunate choice of words when I said, "Manipulate", but that is precisely what we sometimes must do, especially when competing with something like ISIS, which has an amazingly effective information campaign that is drawing Western youth to its black banner. You absolutely have to compete in the information wars, and against an enemy like ISIS, you have to win. Effective influence operations, properly integrated with our other special operations maneuver capabilities, are critical to our success in these enduring competitions in

places you don't see on the news, but in which our adversaries are aggressively challenging us.

FSR: On a related note, highly kinetic SOF operations tend to get more press than other operations – when prominent terrorists are killed, etc. Can you give examples that you believe to be successes and models for the future for SOF on the lower end of the conflict scale?

LTG Cleveland: I think it's natural that those types of operations gain a lot of press. Long term we've had good success in the Philippines. Working with the Filipino military has gained us a little bit of notoriety.

There are some good cases in Africa, including the efforts to counter Kony [Joseph Kony, leader of the Uganda-based Lord's Resistance Army rebel group] and the influence of the Lord's Resistance Army in the region. There are lots of successes coming from our ability to message to his fighters that there is an alternative. You don't get a lot of press on that, but those are all good successes from an influence ops standpoint. There are also a lot of places where we have had capability building success. In Colombia, for example, we have shown considerable progress in their development and we've done so, by and large, under the radar. It took a long-term, disciplined approach to the campaign.

FSR: What would you characterize as the most important elements of a successful unconventional warfare campaign, or is that even something that can be done given the primacy of context?

LTG Cleveland: Every one of these [campaigns] is highly individualistic. Every campaign is going to be different. As an example, we're now changing our vocabulary to talk about special warfare as opposed to just unconventional warfare or foreign internal defense. In reality, what you see is that there are places where we are doing ostensibly a FID [Foreign Internal Defense] mission but it has unconventional warfare activities included in it.

There are places where we are doing things that are necessarily part of working 100% with your partner – there are [also] things we do unilaterally, for example at the same time as training and capability building. There are other places – we have very publicly spoken about the Syria train and equip mission. That is a very unconventional warfare activity, but it has pretty significant FID overtones to it. We're going to "train and equip" – that's even the words that we use. The Northern Alliance and working with the Peshmerga at the beginning of both Afghanistan and Iraq were unconventional warfare efforts, but again, there was a chain of command and it was done somewhat from sanctuary [at least initially] and so it had FID-like qualities to it.

There are a couple of activities in places where it is purely unconventional warfare, working with surrogate groups. So each one of these cases is tailored by the circumstance, what's gener-

ating the problem, and by the capacity and capability of whoever is there. If there is one overriding thing, it's having the ability to understand the local and indigenous problems and using that and leveraging that in order to develop the appropriate solutions. You have to know up front what it is. You can't just take the formula from the last successful venture and think it's going to work in the next one. That is why there is a premium on language understanding and area knowledge.

FSR: You were involved in Operation Just Cause, the US invasion of Panama in 1989. This was a situation where, by many accounts, the state apparatus fell apart in the wake of the invasion: widespread looting, civil servants, and police deserting. And yet, the US was ultimately able to stabilize the situation and reconstruct a functional state. Do you think that's an accurate characterization? If so (or if not) what lessons can we learn from that mission?

LTG Cleveland: I think that's a pretty accurate characterization, though I'm not sure I would attribute the looting to inadequate planning. War is going to generate chaos, and within the chaos you will find the opportunists and the crooks. So I think we were somewhat unfairly taken to task in Baghdad for not securing a lot of stuff. We went into Mosul, as an example, without a lot of force on the ground with us. There was no way you could have secured a lot of that stuff. I don't want to say that's the cost of doing business, but it is the unpredictable nature of warfare and I don't know that you can plan your way out of that. But to counter that, or try to avoid that in the case of Panama, you could have doubled or tripled the size of the force that you had to put in there. There is a cost calculus there.

FSR: What allowed it to be a success, and allowed us to pull that one out?

LTG Cleveland: I think that one of things was that we already had a deep relationship, and our cultures were pretty tied together with the Panamanians. If you go back far enough, the Panamanians owed their independence to the United States. Honestly, the Panamanian population was very pro-American.

On Christmas Day I was the S3 [the Operations Officer] of the battalion, so my job was to do the planning. We were going into David, Panama [San José de David] near the Costa Rican border and I had done an exercise up there. I had been in the TOC [Tactical Operations Center] for 5 days then and I wanted to get out of the TOC, so [Major] Kevin Higgens, who had A Company, Third of the 7th [7th SFG(A), Company A, 3rd Battalion] and was a good friend agreed to take me along on the mission and the battalion commander agreed to let me go. So we're up there and we are flying over the town on the approach to the city and the sun's coming up and out of all of these houses out there, these people were coming out cheering. They were exuberant, waving American flags. Now I assume that they didn't want to get bombed, not that we were going to bomb them, but there was a sense that people knew that they were repressed and they knew us well enough to understand our

motives. Carter had done a great thing in their eyes by giving them the [Panama] Canal back and so there was a wellspring of pro-American feeling that had been suppressed artificially by the Noriega regime. That allowed a set of conditions that are not going to be present in a place like Iraq or Afghanistan, which makes the job much more difficult.

FSR: I'm going to follow this up by asking an extremely Fletcher question, because what we have here [at the Fletcher School] is not just a mix of security folks, but also development and people who walk the line [between the two disciplines]. So in an era where the military and especially SOF is being relied on more and more for a wide variety of missions: fighting transnational crime, containing disease outbreaks, responding to humanitarian disasters and helping to rebuild failed or failing states, how do you personally define the line between what are and are not appropriate military tasks?

LTG Cleveland: That is a very Fletcher question, indeed. I would tell you that that is part of the dialogue that we are we are introspecting on, that we are looking at today.

I think what we're discovering though is that the left and right limits are starting to blur quite a bit and that at some point you actually become a DoD team player on an effort that's being run by any number of different players. It could be the State Department under the Chief of Mission and it could be distributing rice in the FATA [Federally Administered Tribal Areas in northwest Pakistan]. But because you have trucks or something and you can get the USAID [United States Agency for International Development] rice up to them, you become a part of that effort. You don't lead it necessarily, but you are part of the team.

So I think that what used to be comfortably where you could draw harder lines, the reality is in this very blurred security environment, this place where competition is happening in a way that is nonstandard to us, DoD is finding itself as a part of a broader team and has a place and role. [There could be a place] where we shouldn't be used at all because it could be prejudicial against the effort we are undertaking. There are places where we might have an "in" with the local military and we become the vehicle of choice for some project that another agency wants to execute.

FSR: Given that people in the general public don't really understand SOF, how would you as the commander of USASOC describe the role of your command in assisting the other elements of national power to achieve a country's foreign policy? What do you need as a command from the other elements of national power to help you be successful in accomplishing the missions you have set out to achieve?

LTG Cleveland: If you think about the US Army Special Operations Command, I'll use our doctrine to try to put it simply. We provide the nation two exquisite capabilities: Surgical Strike and Special Warfare.

The first, Surgical Strike, is a hyper-conventional capability, namely to conduct a precision raid. There could be many reasons to conduct that raid: kill/capture, rescue hostages, etc. In order to do that, you have to have the right kind of structure and apparatus in place. The other, Special Warfare, is an unequaled capability to work with and through indigenous peoples that allows you to garner a far deeper understanding of the environment and the problems that you are trying to solve in that complex environment. You have to carefully select, train, equip, and build the teams and organizations to be able to deliver these exquisite, but mutually supporting capabilities.

From a capabilities standpoint, the most distinguishing factor between the two is how we have to deal with uncertainty. In the case of the surgical strike capability, we build an apparatus that will take out as much uncertainty as possible, and then execute with exceptionally high probabilities of success on the objective; so that we don't kill the hostage, so that we get the target that we were after, and so forth. This strike capability requires highly trained operators and it takes an organization that is specifically designed to reduce uncertainty to the maximum extent possible and get the operator on the objective to do that job.

The other type of special operations capability, Special Warfare, is one that is defined by uncertainty, and for which we build units such as our Special Forces (or Green Berets) which are specifically designed for this type of operating environment. These teams, with their unique training, linguistic and cultural acuity, are designed to operate amongst indigenous peoples, gain a deep understanding of the environment, shape events, and report back.

Another distinguishing factor between our Surgical Strike and Special Warfare elements is scalability. If you think of the Rangers as the SOF raiding force for instance, you can scale this capability by taking a Ranger platoon, add three more platoons to get a company, and onwards up to a full Regimental size raiding element. We fight the Special Forces differently. They have built in redundancy to enable a 12-man detachment to split in to two 6-man detachments with the same capabilities (medical, intel, communications, etc). You don't scale Special Forces capability, as it works through the indigenous population. The Special Forces team is designed to survive in a denied area or in an area that's highly dangerous due to insurgent activity. The Special Forces elements deal with uncertainty by wading into it, surviving, mitigating it, and ultimately controlling a space far larger than their numbers would indicate. They accomplish this through generating something we call 'Indigenous Mass': the development of solutions through networks of indigenous peoples and forces.

I think the nation needs both of these exquisite capabilities. One has been very prominent (this ability to surgically strike) and it's probably always going to be that way. The other is much more discreet in its use, and that's OK. I would offer, however, that the security environment that we see unfolding before us, whether a resurgent Russia, the rapid rise of ISIS, or the violent

dissolution of former partner states such as Yemen, is defined by just the type of uncertainty that our Special Forces and other SOF units are purpose-built to deal with.

FSR: What do you see as we've entered this new security paradigm with non-state actors who might be motivated by religion, ideology, and perhaps ethnicity. Do you see that the second type of working within populations will gain a level of primacy that perhaps you haven't seen in the community's existence?

LTG Cleveland: I would hope so. I hope that both forms of special operations are recognized for what they contribute, and as I mentioned before, those two exquisite capabilities are mutually supporting, and should be employed holistically. I do think the larger discussion is about what is our strategy and our policy in dealing with some of these problems? There is discussion today that we are never (again) going to deploy a large army to go after some of these security problems, like stabilization, nation building, or counter-insurgent operations. I'm not so sure that is entirely up to us, as our adversaries are exercising their options around the world. There is value, however, in considering an indigenous alternative so that they own the problem.

Indigenous solutions can, however, carry their own unique risks. We can go too far in 'helping' and take on too much of the problem, and often our host nation is happy to let us. The key is to bring our indigenous force to the brink of success and no further. Let them do their fighting. We were talking about this earlier. The way I think of it is it's almost a biological approach to the problem rather than a mechanical approach. What you want to do is aggregate the right kind of things around the infection, or around the wound and then when the wound starts to heal, disaggregate and be able to peel away and allow the indigenous forces to realize success on their own. We don't do that very well, especially in large footprint operations. So, this discussion about the employment of Special Forces, Psychological Operations, and Civil Affairs capabilities is germane. Their job is to help us identify and aggregate around that 'indigenous mass', or indigenous solution, so we know what we can contribute to make them successful. Mindful that we can take on more than is necessary, we can't want it more than they do.

FSR: Just to further complicate this picture, there's obviously [been] a large push during the wars, particularly from [former Secretary of Defense Robert] Gates, to work more through multilateral alliances, to work more through regional organizations, which presents many challenges. What sorts of trends have you seen in that area? How does this affect SOF in particular?

LTG Cleveland: I think that the trend is that there is an increasing understanding that we have impediments that don't allow us to do it well, everything from foreign disclosure challenges and bringing our partners into our intelligence fold. There is a lot of friction in our systems and processes that make inter-coalition warfare challenging.

From a wider DoD perspective, we've taken some good steps. We have BICES as an example, which allows us to communicate in a secure way with a wider group of allies. All of the IMET and all the things we are doing to improve relationships with foreign militaries. Even in budget challenged times, leaders understand that we will go to war with partners and allies; therefore anything that is in this area continues to be supported.

From a SOF perspective, I would offer that the same skills and attributes that make our Special Warfare professionals so effective partnering with indigenous populations stand them in good stead operating in coalition environments. Aside from language and cultural skills, their maturity, sound judgment, and expertise make them highly effective operating by, with, and through allied partners and NGOs (Non-governmental Organizations). In the aggregate, I think the trends are good.

FSR: Do you think it's realistic to think that we'll be able to work with our partners on small-scale missions?

LTG Cleveland: I think we're doing that now. You see that we have expeditionary partners that are going with us to places like Central America, like the Colombians for example, who are helping us take on some of those issues. I think it's important to consider the sheer value of US presence and engagement in some of these places around the world that are in either conflict or pre-conflict stages. Partner nations may not commit until we do, and the whole point of a US SOF solution, is that the commitment need not be large. Consider Iraq of today, where other nations joined in bolstering the Iraqi army once the US committed to the effort. So yes, I think that's where most success will take place, where others take on some of these things in their regions, and facilitating them when they help address own issues. Everyone understands who needs help in their own neighborhood.

FSR: A question about you...in your 30 plus years of experience, how would you describe the evolution in the integration of SOF and conventional forces and what do you think needs to be done to maintain the lessons you've learned and the progress you've made in that regard for your community.

LTG Cleveland: Both theaters of war, Iraq and Afghanistan, were excellent forcing functions in terms of bringing SOF and conventional forces together in, frankly, a pretty wide array of circumstances. If you think about the beginning of the war you have just to use my own example, so I'm commanding the 10th Special Forces Group, and the CFLCC Commander, then LTG McKiernan, gives Tactical Control (TACON) of the 173rd ABN Brigade to the 10th SFG(A). So now a Colonel of infantry from the 173rd is now working for a Colonel of Special Forces. At that same time, the 26th MEU came in and they gave the 10th Special Forces Group TACON of the MEU. Additionally, I had attached to me an infantry battalion, the Golden Dragons. So here you are at a very kinetic phase and you have a very mixed organization. Add onto that the 65,000 Kurds that

are partnered with you. That was a paradigm-breaking moment. Here you are giving one of the Army's premier infantry brigades to a Special Forces unit. We proved that we could do this.

Ever since that point, as that campaign shifted into a stability operation, there were SOF teams on the ground, increasingly in a supported/supporting role to the conventional force. There were cases, as the campaign changed in its complexion, in which the conventional force started peeling off capability to give to the SOF force. As time went on, we got pretty good at shifting the supported/supporting relationships as the nature of the problem changed. One of the things that the Chief of Staff of the Army wanted me to do upon taking command of USASOC was to make sure we didn't lose that. We had just come out of Iraq when I took over command of USASOC and we saw on the horizon that Afghanistan would be drawing down. So the Chief's guidance to me was, "make sure we don't lose that relationship".

The good thing is that we were given the opportunity for the first time in our 60-year history to write our own doctrine. Up to that point we had field manuals. Field Manuals tell us how to do our business. If someone from the outside wanted to learn about Special Forces or PSYOPS, they would pick up our manual and 'learn us'. That is not the same as doctrine. In August of 2012 we published for the first time, our own doctrine. Once that happened, it allowed us then to use approved doctrine as a platform to put teams in the TRADOC Centers of Excellence to teach that doctrine. Now we are teaching the young Lieutenants and young Sergeants that Special Warfare and Surgical Strike, Army Special Operations is part of their Army. Educating them that USASOC, one of their Army Service Component Commands, is 51% of the nation's SOF capability.

The current Army Operating Concept outlines the concept of SOF-centric campaigns, hybrid campaigns, and conventional-centric campaigns. It's written as though Army SOF was part of the Army, and I think that is indicative of the maturing of the Army's thinking and the understanding that we are all part of one great Army. I'm optimistic about that, and I think everything from the JRTC/NTC type rotations, which is where everyone kind of says SOF integration with conventional forces happens, it now actually happens on a more fundamental level in the education system and in the doctrine and in the concepts. Since we've won that part of it, the rest of it will fall in place.

FSR: You at one time oversaw the management of the Army Special Forces Officer Career Field. Do you think that the current SOF officers are being sufficiently trained? Does the need for increasingly specialized cultural and language training in order to operate in certain environments limit your flexibility?

LTG Cleveland: I think SOF operators have never been better, frankly. The assessment and selection process absolutely brings in the best soldiers we've ever had. Across all of our regiments, the quality has never been better. The training program that

they get at the foundational level has never been better. I think after their entry into their various branches, we've been pretty innovative on ways to get them advanced degrees for example, and get them to places like NPS or NDU (NDU has a master's program located at Fort Bragg). We even get them up here to the Fletcher School. That allows them time to reflect, think, and write about their profession and their part of the defense portfolio. So, I'm pretty optimistic, even amid sequestration challenges.

One of the things we did at USASOC was as we entered into sequestration, the first round of the problem, we dedicated ourselves to making ourselves better, not bigger. If we had to get a little smaller to get better, we'd take that. We shrunk the size of our force, reduced the number of SF ODAs [Operational Detachment Alpha, or 12 person SF teams] out there, we reduced the number of Rangers, we reduced the number of Civil Affairs teams and then we were able to plow some of those savings into making our units better. So I'm very optimistic. The training level is higher, the language skills are getting better, the organizations that are getting redesigned have an impetus for the soldiers in the business to learn some of the higher end skills necessary for this 21st Century environment that we are in. I think everything is coming together.

FSR: So through this sort of refocusing, you feel like you have been able to hold on to the operational experience coming out of the last 15 years?

LTG Cleveland: I think so. The problem is that we are part of the Army and the Army is drawing down. As the Army looks at its sizing mechanisms, our officers and NCOs [non-commissioned officers] are going to be involved in that sizing exercise. Like the rest of the officers in the army, they are subject to being removed if their performance hasn't been at a level that is commensurate with their peers. But again, I think we have enough of an inventory that we are okay with that.

FSR: To turn it back a little bit, what do you think about the current priorities and procedures across all the agencies when it comes to providing assistance to foreign states? Many have expressed concern that what is easy to measure and requested by our partners – that is, train and equip [their forces] - will inevitably be prioritized over efforts to train them for success in the hearts-and-minds aspect of counterinsurgency, such as in human rights and such. Do you think that is a valid criticism, and if so what options do we have to keep things moving in the right direction?

LTG Cleveland: That's really a good point ... When I was a captain in the special forces we went on a mission to Bolivia to train the UMAPAR, which are the Bolivian rural police. And we were the first team in there, so it was an ideal SF mission. You had coca paste being sold and processed all over the place. The force that we had fallen in on was corrupt, they were ill-trained, they were living in these dilapidated Brazilian-donated tents that weren't really providing any overhead cover except

from the sun.

It was a perfect SF mission, it really was. You were right in the middle of the problem, and they had asked us to come in and fix this force. You have to remember, there are a lot of drug lines in Colombia that were using the Chapare as a source region for their coca paste, they ran their lines into the Chapare, and of course they were bringing in a lot of money to buy off those who needed to be bought off so the business could continue. We learned pretty quickly that the problem was the motivation, not as they would say “por falta de medios,” you know, “If only I had new uniforms, we would be so much better, or a new mochilla (backpack).” Really, at the end of the day, when I would get frustrated with my counterparts, which was quite a bit, I’d say, “I could take 12 Indians with blow guns and they would do a better job interdicting these guys”. So it’s all about motivation.

What I am afraid of is that often progress is measured by spending a lot of money on equipment and training. You can’t spend enough, really, for training on these problems if the government doesn’t have the credibility. It doesn’t matter what you put on their back, it doesn’t matter how much training you give them, you are going to have serious problems when you encounter a serious enemy who is motivated. And so, I guess my concern is that we have to be very careful that we are judging the motivation and addressing the motivation issue and in some cases that means a different kind of policy. How good is that government on governing, and how respected are they by their people? You can only do so much, and you can’t fight your way out of bad policy.

FSR: To follow up on that quickly, we’re in the situation now, no longer being in Iraq and Afghanistan, where we are working with host governments on priorities are important to us. We know what we want to see, including better governance and better civil-military relations because we feel like that has a connection to containing insurgency. But our interests are not perfectly lined with theirs, [and at the same time] we are not occupiers. How do we achieve the things we need to achieve in that kind of environment, where we have that mismatch in incentives?

LTG Cleveland: Part of it is understanding that whenever you are going down the path of supporting an indigenous group or country, you’re not in the driver’s seat. One of the sages here at our headquarters compares it to taking a taxicab. The cab is going to go where the driver wants to take the taxi. You are paying him hopefully to take it where you want it to go. But the path it takes and the ultimate destination is going to be up to the guy driving. We, the US, often have a hard time with that.

Sometimes these paths will do things that are just not aligned with US interests. You have the nuns being killed in El Salvador, for example. But those kinds of things are going to unfortunately happen when you are not in the driver’s seat. You have to understand that in this business of supporting indigenous forces or host nation forces, that it takes a long time. In the case of El

Salvador, we had real success when Salvadoran officers we had trained in basic training and at the basic infantry course were coming back to us and attending our War College, and then going back down to take over their Army. That’s a generational approach to what is often a generational problem. So we have to have patience.

We have to have a sense of operational time, and we have to understand that there will be deviations on the path because inherently it’s their problem, and it exists in their space. The choices often are, “don’t do anything”, which certainly is going to let this problem go in a direction that may be totally against our interests; “take it over and do it ourselves”, which is normally very expensive and sometimes problematic; or take the approach that is going to take a while, do everything you can do to avoid taking over their problem for them, but be there to help influence, even if incrementally and slowly, the path that the taxi cab is taking.

FSR: To follow up on that, do you think that the will exists in our institutions to stick it out when it comes to stabilization and conflict prevention missions?

LTG Cleveland: I think so. I do think that it is interesting to watch the President as he has laid out a longer-term strategy in Iraq and Syria, and yet he has taken heat, politically, as others look for more direct intervention or quicker solutions. You are always going to have that debate. I think it is a healthy debate. But when the case is made appropriately, I think the patience is there. I think we have some good examples. For example, Colombia, which was almost a failed state, in a way. It was almost a narco-state, depending on what intel report you are reading. But I think that is a great example of a success story.

FSR: One final question about you and what you perceive to be your legacy at USASOC. You’re about to pass your unit colors this spring. What do you consider the Command’s most important accomplish during your tenure as Commander for USASOC’s future fights?

LTG Cleveland: I hope that we were able to take what could have been a tumultuous and chaotic situation surrounding sequestration and coming out of Iraq and drawing down Afghanistan, and turn those challenges into opportunities for change. We had a vision, we knew where we wanted to take the command, we were honest with ourselves about our problems and we forthrightly addressed them. Most importantly, we did not do this in a manner that would be lost to the changing of the guard. We published all of this in a three-part document called ARSOF 2022 which spelled out in writing everything we intended to do, and we held ourselves accountable. Such large scale change is challenging, and momentum has to be achieved. We achieved that critical momentum, and did so without the command imploding. Ultimately, we are collectively stronger for it. Time will tell.

**Interview has been lightly edited for clarity. Brackets indicate editorial additions.*

Profile in Security: CW5 Wendy A. Wayman

Wendy Ann Wayman never imagined she would still be serving her country more than three decades after enlisting in the United States Army, let alone rise to rank of Chief Warrant Officer 5 and become the first Command Chief Warrant Officer for Army Intelligence and Security Command (INSCOM). Born and raised in Aberdeen, South Dakota, CW5 Wayman has traveled the world and advised the highest-ranking military leaders in the United States. She has also amassed a legion of professional colleagues who describe her using such phrases as “no one better,” “shaping the future of military intelligence,” “a consummate professional,” “my dear mentor,” and “a complete badass.” The Fletcher Security Review is honored to feature INSCOM Command Chief Warrant Officer, CW5 Wendy Wayman’s “Profile in Security.”



Official Photo of CW5 Wayman (Jocelyn Broussard/U.S. Army INSCOM)

FSR: What initially made you want to enlist in the armed forces?

Wayman: When I was just eight years old I spent a weekend fishing with my Great Uncle Leo who regaled me with tales of friendships and brotherhood that would span a lifetime. He told me of those soldiers whom I would come to appreciate as our Greatest Generation, those young men who fought for us and for each other as a Band of Brothers. Following that weekend of fish tales and war stories, the kind you tell an impressionable young girl, I went home to tell my mother that I wanted to be a U.S. Army Soldier. She, of course, responded to me with the same response that any mother gives her child when greeted with such a revelation. She gave me that cautious smile that hides the hope that the following week I would come back and tell her that I had yet again changed my mind and wanted to be a veterinarian or country singer.

Eight years later I made my first foray into the recruiting office and began the next portion of the journey. I was not allowed to actually begin lobbying for a job until after my 17th birthday. In 1983, in the fall of my senior year of high school, I began my pursuit in earnest. In the time period between having made the decision that I wanted to serve and the actual contract negotiations with the Army recruiter, I had further developed a plan. My paternal grandparents were friends with a couple who were doctors from Chicago, Dr. and Mrs. Hebert, who would come to our little corner of the heartland to hunt pheasant every October. They used to provide medical care in the gulags in Siberia and would talk of the language and places and customs of the Russian peoples and thus developed my next career goal. I wanted to learn Russian and that was exactly what I told the recruiter.

The first recruiter offered me the glamorous job for which I had been wishing, that of Army cook (of course, this was before Steven Seagal and the fight to save a ship). The same recruiter then offered me the honor of ammunition specialist, technically counting bullets. I asked if either of those would get me training as a Russian linguist, but he did not seem to want to work with me. About a month later, as I was walking past, I noticed that there was a new guy in the recruiting office. SGT Vic was

more than happy to help me get exactly what I wanted because he quickly figured out that I would not be swayed. SGT Vic told me that I would have to take a test to check my potential, and because I was still a minor, my mom and dad would have to come and sign the papers in order for me to officially begin the process. What followed was my first commercial airplane flight to get me to our Military Entrance Processing Station (MEPS) to take some tests and a physical. I was tested and found worthy. I would then sign the contract that would pave the path for my past 31 years of service. I got back on a plane and went back to life as a high school senior and had to listen to folks who were convinced that I wouldn't make it through Basic Training. On the other hand, there were those convinced that the possibilities were unlimited. I am proud to say that those cheerleaders, my family, friends, and some of my church family and teachers seem to have been right.

FSR: When you graduated from boot camp, how did you imagine your career evolving? At 10 years, how did you imagine your career evolving? At 20 years, how did you imagine your career evolving?

Wayman: When I first signed my contract to join the Army—and contrary to most of the stereotypes from the early 80s, I was not a Private Benjamin kind-of-girl, my influence was more Bill Murray and Stripes—I had typical starry-eyed kid delusions of grandeur and glamor. I just knew that I was going to learn Russian and, since my job was SO secretive that the recruiter couldn't even tell me what I would be doing, I was going to be a spy and live in Russia and work in the Embassy and blend in with the locals and defend America against the Red-Threat. Little did I know that it would take me until 2003 to actually cross the Russian border.

I did learn Russian at the Defense Language Institute on the beautiful Presidio of Monterey in California. Although I knew what the contract said, I did not expect that Uncle Sam would really send me to live just steps from the ocean for the first year of my Army life. We began that 49-week course with 72 students and graduated 56 linguists. Fifty-four graduates of that class from the Army, Navy, and Marine Corps left Monterey to eventually arrive at scenic locations around the globe and my roommate and I had orders to beautiful sunny Sierra Vista, Arizona. Needless to say, it wasn't Russia. My time at Ft. Huachuca, Arizona allowed me the opportunity to enhance the technical and tactical train of incoming Military Intelligence (MI) Officers (translation: I was a member of the Opposing Force (OPFOR) element that was charged with the mission of providing a countering force to the young lieutenants as they attempt to maneuver across the desert). The results were scripted, of course. Sometimes we won, sometimes they won but I always enjoyed it. Not many young Soldiers get the chance to "shoot at LTs" once a month for a week at a time. Interestingly enough, there are folks who would remember the "Jeep with the mounted M60 and the enthusiastic M60 gunner" for years to come. I have run into at least two who are now Military Intelligence General Officers.

In addition to the OPFOR missions, we were charged with teaching the junior officers how to employ the MI assets which they would have under their purview at their gaining tactical units. It was there, at Ft. Huachuca, that I would meet my first Warrant Officer and, as a young Private First Class, would set my next Army goal. I wanted to be a Warrant Officer. CW2 Greg Glass knew everything about everything, and if he didn't, he knew where to find it and would point you in the right direction. He didn't just hold the knowledge to himself, he imparted it on us.

Later, in 1988, as I approached my first reenlistment, the Army had begun to make changes. The Army had moved to commission CW2s and as Chief's first great act of defiance, he conducted my reenlistment. Following that assignment, I would finally be assigned overseas in Germany. We enjoyed life in Germany until Sadaam Hussein changed our lives on 2 August 1990 when he invaded Kuwait. I would deploy to DESERT STORM in Saudi Arabia, Iraq, and Kuwait. I would move assets around the battlefield and respond/react to enemy troops advancing on my closest friends, and I would be the one to tell them to cease operations and defend their positions. I would later traverse the infamous sector known as "Death Highway" as it was being attended to by our forces. To this day I can still remember the stench of burnt and decaying bodies and the sites of heavy equipment moving vehicles and remains. It was 1991, and we would return to Germany in the spring and I would move to Maryland in the fall. I would finally arrive at a point where my analytic skills would be truly tested and honed and I could actually use my language skills and focus on my next phase of what was quickly approaching the point where I could call it a career.

In my mind, I had set a checklist of things to do to be postured for consideration of accession into the Military Intelligence Warrant Officer Corps: a school assignment – check; a tactical assignment – check; a combat deployment – check; and now a strategic assignment – check. I was approaching the "too much time in service" 12-year benchmark and knew that it was now or never. I submitted my packet and waited. The results came out and I was not selected, I was devastated but not defeated. I made some calls to find out why. "Back in the day" you could get some answers and I was told that the delimiter was a degree. By the time the next board met, I had a degree and was selected. I was going to be an Electronic Warfare Signals Intelligence Technician Warrant Officer. Warrant Officer Candidate School was essentially Basic Training on steroids with an attitude. The training was good, the training was stressful, and the focus was attention to detail. Our class had 36 Military Intelligence candidates, nine Aviation candidates, 11 Special Forces candidates, and some scattered odds and ends. Before we even hit our active phase of the course, our class had adopted a rule that said the best defense is a good offense and it must have worked because we graduated with everyone we started (unheard of) and never lost our class colors (unprecedented in that training year). I managed to make life-long friends and learned a lot about the rest of the Army and about myself. If I had to go back and start over, I wouldn't change a thing on my career path.

FSR: What factors motivated you to apply to join the Warrant Officer Corps?

Wayman: Simple, I love what I do! I loved my Soldiers and enjoyed leading them, but at the end of the day, I loved my specialty more and I'm pretty good at Signals Intelligence (SIGINT) if I do say so myself. SIGINT is solving puzzles every day at work and getting paid to do it. I had great examples of what a Warrant Officer should be and some who showed me what a Warrant Officer should not be. All in all, they definitely showed me that it's "good to be the Chief". Being a Warrant Officer is about finding the answers to questions you haven't yet been asked and looking for a way to get your mission accomplished, within legal boundaries, regardless of obstacles. I would tell you that being a technical Army Warrant Officer is a bit of a puzzle in and of itself.

FSR: Given its small size, can you describe the unique attributes, if any, of the camaraderie of the Warrant Officer corps?

Wayman: The Warrant Officer Corps, officially now known as the Army Warrant Officer cohort inside of the Officer Corps, is limited by law. The Warrant Officer population is only allowed to be 5% of the total force, Army, Marines or Navy. Because of that we tend to be a tight-knit group and tend to both take care of each other and police our own. The military is a family and the Warrant Officers inside the forces are simply a microcosm of that family. We know that we are looked upon to be the subject matter experts and that each of us is entrusted with the reputation of the Warrant Officer cohort as a whole. Most Warrants safeguard that reputation with the same zeal they guard a perimeter surrounding themselves and their brothers- and sisters-in-arms.

FSR: As the mother of two soldiers, can you describe your emotions about sharing a highly kinetic battlespace with your children with equal, if not superior, knowledge about the threats facing them?

Wayman: Being the mother of a service member is challenging. Every mother deals with it differently; however, when you too wear a uniform you know the reality of their service. The most challenging times for me as both the mom and the Chief were the times that the kids and I spent deployed separately together. On my first shared deployment with our son, I was on the phone with him one day, just checking in and he told me that he had to go prepare for a mission. I will tell you that, although I am meticulous in my over watch of the mission for every mother's son or daughter, when it was my kids, I would vacillate between hyper-attentive with an inability to focus on anything other than what might be happening and the desire to completely shut down until I knew they were back. I had to tell my kids and their commanders that I did not want to know when they were "busting the wire" and leaving the semblance of security of a forward operating base. They could check in when they got back, if they had time. There is a challenge when you have the "luxury"

of seeing everything that happens on the battlefield on a very short lead time. Knowing the threats that they would face made my every day shared with them in combat a challenge.

Don't get me wrong, seeing my kids in theatre was such an incredible boost to my morale and getting to spend time with them and hear their commanders' praise for their work ethic, their dedication to duty, and their professionalism was more than any mother could ask. My pride in them knows no bounds. Now, having said all of that, it was harder for me to return to the U.S. knowing that my kids were still in Iraq or Afghanistan. I stopped watching the news because I couldn't handle wondering if those cold non-descript crawlers across the bottom of my TV screen could be either our son or daughter. When our kids came home I started watching again but to this day every number that a news media throws out there is someone's mother/father, sister/brother, daughter/son, and my heart remains tied to those we have lost. I work hard to help ensure that we do whatever we can to keep those numbers as close to zero as possible.

FSR: How did you feel when your children decided also to enlist in the armed forces?

Wayman: I was so incredibly proud of both of the kids—what more could I be? We had raised them to salute the flag and honor those who had gone before. It only made sense that they would follow in our footsteps. I will admit to a bit of bias and many will see that there is probably some sexism in it too. We wanted our son to join the Marines, like his father before him, because he needed the structure and discipline that the Marine Corps could provide. He didn't become a Devil Dog but instead became an Army Combat Medic and he was met with discipline and structure and continues to exceed our wildest expectations. We wanted our daughter to join the Air Force and follow her dreams. She didn't "Aim High" but instead joined the Army, Military Intelligence Corps as an interrogator. I realized at a very young age that, much to my chagrin as a Signals Intelligence professional, I was raising a child with Human Intelligence skills, a budding interrogator. She was absolutely convinced that our paths would not cross because of course she had chosen a different specialty. That was a wrong assumption and even to this day, after she hung up the boots and her uniform, she is still working inside of one of the INSCOM formations as a contractor, INSCOM where I am the Command Chief Warrant Officer.

FSR: In a career that caused you to travel frequently, how specifically did you balance having a husband, children, and a successful career?

Wayman: In a way, it helped that my husband had served in both the Marines and in the Army because he understood the military life. His perspective was that of a mid-grade, non-commissioned officer and the challenges associated with more senior positions and higher ranks were something that we learned about together. Communication is the key and the evolution of technology over my career has greatly improved access where



Chief Warrant Officer 5 Wendy A. Wayman, the U.S. Army INSCOM's newly-appointed Command Chief Warrant Officer, is joined by Command Sgt. Maj. Panapa R. Willis (left), former INSCOM command sergeant major, and Maj. Gen. George J. Franz III (right), INSCOM commanding general, during the ceremonial cake cutting at an Investiture Ceremony establishing the position of INSCOM's first official Command Chief Warrant Officer at Fort Belvoir, Virginia, April 8, 2015 (Sgt. Jesus J. Aranda, Jr./U.S. Army INSCOM)

none had previously existed. Right behind that comes understanding—that is the toughest piece. Husbands understand but don't like it; kids don't understand it, don't like it and don't forget; dogs don't understand it, don't like it, but forgive immediately—cats could care less. Thank heavens for the dog. Across my career when I have had those jobs where I could set down some roots and not travel as often or for as long, it was those times that my husband was required to travel for his work. We've learned to adapt to whatever life has thrown us and have been able to find that happy middle ground.. The other key is that time with family was fenced and was for them alone. As I continued to gain more responsibility the kids too were getting older and had their own lives to live and balance. To be completely frank, the easiest and oftentimes most fulfilling jobs are those while you are deployed. Deployment time has three or four mandatory elements and they are work, eat, sleep, and physical fitness. I was always able to do plenty of the first and ration the rest over the few remaining hours in the day. Deployment jobs are fraught with incredible highs and lows but are among the most fulfilling I have had. As I reflect back on my childhood conversations with my Uncle Leo, I have grown to completely understand and appreciate the brotherhood of arms.

FSR: Throughout your career, how, if at all, did you strategically manage your assignments to balance these priorities?

Wayman: Throughout my career, I did my best to ensure that some things would happen according to plan. Many of my assignments simply fell into place. I went overseas (after the first assignment) when I wanted; I went to the National Security Agency when I wanted; and I went to school to become a Warrant Officer when I wanted. As we were preparing to leave my second Warrant Officer assignment in California and the beautiful High Mojave Desert, we wanted to return to the east coast and the area around Washington, D.C. There was a job waiting for my husband in the area. All I had to do was get him there, and—voilà—the stress of job hunting was nullified.

The next concern was the big one: our kids were high school age and we wanted them outside of a big urban area. Our daughter would move with us from California and our son would move in and join us from Connecticut where he had been living with his biological mother. I worked with my assignments manager to try to find something that would meet that criteria and was convinced that I was not going to accomplish it. Unbeknownst to me, there was an opportunity at the Joint Warfare Analysis

Center in Dahlgren, Virginia. I had no earthly idea where that was but on a map it looked like the absolute right place for us. We moved the kids, and the high school was definitely what we wanted for them.

Family is such a part of who I am and I emphasize that to my Soldiers. In March 2004, while we were in Dahlgren, my dad was diagnosed with cancer and told that he had six months to live. I made a decision that I needed to be home with him and dropped a set of retirement papers. My leadership supported this decision but asked me to consider another option, a compassionate assignment back home. I told them that I would but doubted that the Army could get me to Aberdeen, South Dakota and let both sets of papers begin to process.

At the time, I had the honor to have come to know and work for Brigadier General Richard Quirk. BG Quirk had also had the opportunity to meet my folks when I was promoted to Chief Warrant Officer Three in January of 2003. Not only had the General met my folks, he hit it off with my dad. When I went home on emergency leave to take my dad to MD Anderson in Houston and then the Mayo Clinic in Minnesota, he called to see how things were going. While I awaited the Army response, I began the process of preparing for retirement and began attending the required classes. On 20 May 2004, my phone rang while I was in a class to teach me how to “dress for success”

after camouflage. On the other end of the phone was BG Quirk. He had personally and continually kept in touch to check on me and to check on my dad. General Quirk was calling to tell me that he had just gotten off the phone with Compassionates Branch and my request had been approved. I called my assignments branch and told them to pull my retirement and I began preparing to move home for a year or until I was no longer needed there.

After I had been in South Dakota with and for my parents for almost a year and was contemplating another attempt at retirement, assignment branch called to tell me that I was on a short list for a deployment. My family and I discussed the pros and cons, and I made the decision that since the Army had taken care of me when I needed them that I would return the favor. I moved my daughter into her college dorm, left my husband and dog at home with my family, both mom and dad, packed a couple of suitcases and got on a plane to Germany, and 13 days later, got on another one bound for Baghdad. When I needed the Army to support me, they have always come through. The rest, as they say, is history.

I found out that I would be considered for promotion to Chief Warrant Officer Four on the upcoming board, was selected, and promoted at a joint ceremony with my son on the third floor balcony of the Al Faw Palace in Baghdad. I returned to

Chief Warrant Officer 5 Wendy A. Wayman accepts the Commanding General’s Charter for the Command Chief Warrant Officer (CCWO) position from Maj. Gen. George J. Franz III, commanding general, U.S. Army INSCOM. Wayman became the command’s first CCWO during an Investiture Ceremony held at Fort Belvoir, Virginia, April 8. Wayman accepts the newly-established position following more than 30 years of service in the signals intelligence and electronic warfare field as a noncommissioned officer and a warrant officer (Jocelyn Broussard/U.S. Army INSCOM).



the States, picked up my husband and my things, and moved to Maryland where I would face the challenge, as a Chief Warrant Officer Four, of filling one of only two billets in the Army for Chief Warrant Officer Five SIGINT Soldiers. That job was one I had been introduced to in 1997 as a young Warrant Officer One after having just returned from a deployment to Bosnia. That was a job that I told myself I would like to try and had ideas (WO1s have “ideas”). I put those ideas into play and it became one of the most incredible opportunities to bring SIGINT to the conventional force in the history of our profession.

After trying my hand at that job for two years, I convinced my Commander to let me volunteer for another deployment to Iraq as the Corps SIGINT Advisor to I Corps. Every job just kept getting better. I would then apply for an accessed position at the Army’s Asymmetric Warfare Group and was accepted. While assigned there I would be considered for promotion to Chief Warrant Officer Five, a rank for which the Army only had two authorizations positions in my field and there were currently five others in the force. I was selected for promotion and subsequently moved back to the brigade where both of the actual billets exist. I don’t know that I would call the next move a strategic one, but it was a definite step up. I have always said that “they can’t tell you no if you don’t ask”. I put my name in the hat for the job I currently hold. I guess it doesn’t get, both figuratively and literally, much more strategic than that.

FSR: How do you differentiate your leadership style as a warrant officer from Sergeants Major and from General Officers?

Wayman: Every leader has his or her own approach to leadership and the levels of stratification within the ranks can tend to widen the gaps. For instance, Army Privates are young and straight off the street and have many lessons to learn about life, the Army, and their jobs. The senior Non-commissioned Officers (NCO) are those who will teach them the ropes and bring them along to become the next generation of NCOs. Army Lieutenants (LT) are also straight off the street but, in general, tend to normally be older than the Privates. The LTs still have many lessons to learn about their roles and responsibilities and much to learn about leading but they have already been given the basics before they step in front of their first formations. Most Warrant Officer One (WO1), with some exceptions for aviators, have already learned about the Army and their craft and that is why they chose to follow that path. The WO1 needs to bring with them the backbone that is the Non-Commissioned Officer Corps from which they transitioned and continue to hone their skills as technicians and leaders. Warrants lead not by or with their rank, they are most often informal leaders who lead by virtue of knowledge. Not everyone would agree with that statement; however, not everyone is answering these questions either.

FSR: You are INSCOM’s first Command Chief. As such, what type of legacy do you hope to leave for your successor?

Wayman: Legacy, have I told you how I dislike that word? My legacy, if I must use that word, is the generation of Warrant Of-

ficers that will follow in my footsteps and surpass my wildest dreams of success in supporting an operation on a battlefield yet to be imagined. For my successor, I want them to be able to step into the job and not have to teach people what it is that a Command Chief Warrant Officer (CCWO) brings to the table and that they actually get a seat at the table, very near the head. I am not comfortable with asserting the “rank has its privileges” mantra but I owe that to the next CCWO, so at a minimum I will push those boundaries and help to solidify the precedent. As a young Soldier you often grouse about the fact that seniors have things like drivers and parking spots but as you progress through the ranks you realize that there are reasons for perceived privileges: parking spots and drivers keep leaders on-time and on-target because time is one of the most valuable commodities, and lost time cannot be regained, a statement that cannot be more true.

FSR: Who are the people who have most inspired you in your career?

Wayman: In my career the people who have been the most inspiring are not those you might expect. I have told you of the technical expertise of my first Warrant and of the General who helped me find a way to be with my family when we all needed it the most, those are obvious answers. As a Chief Warrant Officer Two, when it comes to SIGINT acumen, I was inspired by a junior Soldier who brought me a science-project answer to finding a way to defeat an adversary on the wargame battlefield of the Army’s National Training Center. I love my geeks. We took that science-project and turned it into Tactics, Techniques and Procedures to teach our U.S. Army maneuver forces how to work through and learn to circumvent communications interference. I have been inspired by my fellow Warrant Officer and classmate, an Army Aviator, who had his leg amputated as a result of a combat injury and worked his way back into the cockpit and then inspired others to follow his example. I am inspired by my friends who wanted to serve their country and in so doing had to hide their true selves from the military through the eras of proverbial witch-hunts, Don’t-Ask-Don’t-Tell, and finally the repeal of that policy on 20 September 2011. I am inspired by leaders who know their Soldiers by name. I am inspired by those who have come before, our veterans who wear their pins and hats and stand to salute the flag and remember their brothers and sisters in arms. I am inspired by our wounded warriors to persevere and continue to carry on despite the odds. Everywhere I look, as I travel to the numerous military installations around the world, I have opportunity to see at least one thing every day that pushes me to drive myself to be better. Every day I am inspired by the young men and women who raise their right hands to enlist and the older men and women who serve throughout their lives, giving back what was once given them.

FSR: Your career is obviously not yet complete, but of what are you most proud in your career?

Wayman: Please do not take this answer as cliché, but the thing in which I have the most pride is the service of my children

and that of the dedicated professionals who have worked beside me, with me, for me and for whom I have worked. Service to country cannot be understated. If I must and if you are going to pin me down to an answer outside of that, I would say STG (pronounced STaG). I would tell you that SIGINT Terminal Guidance (STG) is the one most significant accomplishment that brings me pride. I was in the right place at the right time in the right job to help the Army bring SIGINT to the conventional tactical force through the creation of the SIGINT Terminal Guidance process. Suffice it to say that was the “sexiest” that our field has ever been and it taught commanders at all levels to appreciate and employ their SIGINT capabilities.

FSR: You work involves long hours and (often) extensive travel. What activities do you enjoy outside of work and the United States Army?

Wayman: I love to travel but need to figure out how to do that for fun and not for work, more beaches and mountains that don't require me to fill out a travel voucher upon my return. I enjoy driving and riding motorcycles and fast cars—I have both. I love to cook and enjoy doing yoga and working out—calories in and calories out. I have a constant companion, a stuffed blue raccoon named Bill that was a Christmas gift from a friend the year I turned sixteen. Bill has been to every school, on every temporary-duty trip, every assignment and every field exercise and



deployment I've had, except Basic Training. I have a soft spot for animals and as my parents could tell you, there were never any strays on our farm. Every cat who crossed our driveway was tame and had a name within a week. We only had cats as pets because they could live in the barn and fend for themselves. I, as most of my girlfriends could tell you, am the most girly of nearly every group in which I find myself. I truly enjoy the finer things in life, fine red wine with gourmet fruit and cheese, going to dinner and dancing in a great pair of high heels, watching the sun rise and set, and simply enjoying time with my friends who are family and family who are friends.

FSR: How many female CW5s are there in the Army?

Wayman: I honestly don't know, I actually have tried to find the answer but [have found] nothing definitive yet. We can make this a math problem to reach a potential answer. There are a total of approximately 490,000 people currently on active duty. Of that total, only 15.6% of the force are female which brings us to 76,400. Only 5% are authorized to hold the rank of Warrant Officer which brings us to approximately 24,500 female U.S. Army technical and aviation Warrant Officers. Of that number, only 3.4% are in the grade of CW5. Once you get through the numbers, the approximate number of female CW5 in the United States Army is right around 130 in the active force. Again, this is a result of math and not actual current numbers on-hand. Outside of the math problem, U.S. Army Military Intelligence only has a total of six female Chief Warrant Officer Five, and I am the only female of the eight total who are Signals Intelligence professionals.

This just in: I heard back from my point of contact at Human Resources Command and there are a total of 40 women in the U.S. Army active-duty force who wear the rank of CW5. That total means that, in actuality, we are only 8.16% of the total active force. I decided that I would leave the math so that you can see how far we have come and yet still have so far to go to meet our math-only numbers inside the force.

**Interview has been lightly edited for clarity. Brackets indicate editorial additions.*

A 'Bastard' Feudal State: Governance by the Military Class in Late Medieval England

by Dr. Andrew Mark Spencer



A Norman knight slaying Harold Godwinson (Bayeux tapestry, c. 1070). The rank of knight developed in the 12th century from the mounted warriors of the 10th and 11th centuries. (Wikipedia/Myrabella)

Two key facts about late medieval England: The kingdom had no standing army and was at war for most of the period between 1294 and 1485. Given these circumstances, it might seem ambitious to identify a role for the military of the time in a non-war environment.

Nonetheless, this peacetime role existed, and created a state of preparedness that was crucial to success when the kingdom went to war. Under 'bastard feudalism' the leaders of the army, trained in war and incubated in a thoroughly military ethos and culture, through their efforts in domestic governance, provided the stability at home and the financial and material resources which were as vital to the victories of the Hundred Years' War as

the much better known and remembered archers of Crecy and Agincourt.

This article will provide background into medieval military and landed society before tracing how the governmental role of this group increased alongside 'bastard feudalism' in response to the crown's need to find the resources for war. It will then show how 'bastard feudalism' worked for king, nobles and gentry in tandem and how this, in turn, created experienced administrators who were able to support the war effort.

'Feudalism' is a term synonymous with the Middle Ages. The feudal pyramid, with the king at the apex, his nobles and knights

beneath, and peasants on the bottom, will be familiar to readers from their school days. ‘Bastard feudalism’, on the other hand, is less well-known and usually has currency only in academic journals. Both are highly controversial terms among medievalists and some even deny the existence of one or the other, or both. Most historians, however, would accept that, in England at least, there was a gradual transition from feudalism—where the principal means by which the king or nobleman rewarded his followers was through a permanent grant of land—to ‘bastard feudalism’—where rewards were primarily paid in cash payments. Where historians do not agree, however, is on the timing, causes and results of such a change.

Medieval Landed Society – An Overview

Before getting into the details of this change and of how the operations of the ‘bastard feudal’ state domestically helped to equip the English for war, it is necessary to provide some background detail on the way contemporary society was constructed. Medieval society was depicted in many ways by contemporary commentators but one of the most persistent was the tripartite model, which divided society into those who prayed, those who worked, and those who fought.¹ Such a model was, of course, far from perfect: groups such as townspeople were left out as, indeed, were women. Equally, some people did not fall neatly into a single category. Many agricultural laborers volunteered or were pressed into military service as archers or footmen, while some clergymen (such as the notorious Bishop Despenser of Norwich, who took “such delight in deeds of arms” and commanded an ill-fated ‘crusade’ against the French in 1383), were as keen warriors as any knight.² In broad terms, however, it was and remains a useful model for understanding how medieval society thought of itself. Our focus will be on the third group, those who fought. These were the landed and military elite who dominated English society and governance.

At the very top were the titled nobility, the earls, to whose ranks were added in the course of the fourteenth and fifteenth centuries dukes, marquises and viscounts. There were usually around a dozen titled nobles at any one time and rarely more than fifteen. They were the super-rich of medieval England with annual incomes of a minimum of £1,000. Most had incomes between £2,000 and £3,000, while the very wealthiest, such as the royal dukes of Cornwall and Lancaster, received well in excess of £6,000.³ To put this into context, an archer in the Hundred Years’ War was paid three pence per day, giving an annual income, if he served every day, of around four and a half pounds, similar to the amount a student at medieval Oxford or Cambridge would need to live on.⁴ To build a small stone castle would cost a baron at least £350.⁵ Below the earls were, from the Norman Conquest of 1066 through to the early fourteenth century, the barons. This was a rather amorphous group and was gradually whittled down from around 250 baronies in the mid-thirteenth century to a parliamentary peerage of perhaps 150 by 1350 and to just seventy-five families a century later. The parliamentary peerage consisted of those major landed families not

in possession of a hereditary title but in receipt of a hereditary individual summons to parliament, something which marked them out as among the most powerful and influential men in the kingdom, whose advice in parliament for the king to be able to say that he had taken full counsel from the realm. A handful were as wealthy as the poorest earls but most had an income of between £350 and £750 a year.⁶

Beneath the nobility were the gentry. Like the nobility, these too were stratified according to wealth and status as the Middle Ages wore on. From the undifferentiated mass of knights in the century or so after the Conquest emerged the graded ranks of the gentry with knights at the top, esquires in the middle, and gentlemen at the bottom who, by dint of lordship over other men, maintained their status above the wealthiest yeomen peasantry.⁷ By example, in 1436 there were just under 1,000 knights, around 1,200 esquires and about 1,600 gentleman, making a total of just under 4,000 members of the gentry. The greater knights, those with several manors, had an average income of £208; the lesser knights £60; esquires £24 10s; and gentlemen £12.⁸

A Military Elite? Theory and Reality

In theory, then, these men formed the military elite of English society. They held their land by knight service and were thus pledged to provide forty days of military service a year when called upon by their lord. The feudal bond, with its obligations of military service, was formalized through the ceremony and oath of homage. While men did not always follow through on their obligation to serve their lord, the bond was recognized as strong enough to shield a man against charges of treason against the king when the defendant could claim he was simply following his lord into rebellion in accordance with his oath. The forty days of obligated feudal service were, however, increasingly impractical for the actual conduct of war and service was often commuted in return for a cash payment that could be used to employ mercenaries, a standard feature of eleventh- and twelfth-century warfare. Gradually English kings moved away from mercenary armies towards armies raised from their own subjects and paid for by parliamentary taxation as these armies were bigger, more reliable and cheaper. The theory of obligation remained, however, even after kings stopped raising feudal levies in the fourteenth century, and those at the very top of military society expected and were expected to serve the king as a matter of course.

For many below the nobility, however, military service and active campaigning were far more rare. There were times when landed society did turn out in very large numbers—during the Crecy-Calais campaign under Edward III between 1346 and 1348, for instance, or for the conquest of Normandy by Henry V from 1417 onwards—but such examples were exceptional. During Edward I’s Scottish campaigns at the turn of the fourteenth century, it was rare for participation by the gentry in any county to top 40 percent in any single campaign, and it was usually

below 30 percent.⁹ That said, around 60 percent of nobles and gentry in these counties did go on campaign at least once during these years.¹⁰ For many members of the gentry, then, participation in war was something of a rite of passage—an activity that you did once or twice when young, after which you hung your shield above your hearth and spent the next thirty years as upstanding members of county society boring your neighbors with tales of youthful exploits in France or Scotland. Despite this, war and membership of the military elite remained central to the gentry's identity, as can be shown by their pastimes of tournaments, chivalric literature, hunting, and hawking, by their military titles and the rituals surrounding knighthood, and by their habit of plastering their coats of arms on everything from church windows and castle gates to cutlery and jewelry.

Running the Country

This military elite spent most of its time in the decidedly non-military setting of rural England. Although parts of the kingdom, particularly the Welsh Marches from the eleventh to the late thirteenth centuries and the Scottish borders from the end of the thirteenth century onwards, were militarized zones and there was occasional political unrest, medieval England was generally one of the most peaceful parts of Europe—the English tended to export warfare elsewhere in Britain and on the continent rather than suffer the consequences themselves. Partly as a result of this and the insular nature of the kingdom, England was also one of the most highly governed and centralized polities in medieval Europe. Because of the extent and spread of royal landholding and the fact that the estates of the great nobles were scattered across numerous counties rather than concentrated in discrete blocks, England avoided the dispersal of power into the hands of local aristocracies at the expense of royal authority that happened across much of western Europe in the aftermath of the collapse of Roman power. England was divided into shires or counties which emerged from the ninth to the mid-twelfth century (Lancashire being the last) as the kingdom of Wessex expanded and transformed itself into England, and these lasted with minimal change until the Local Government Act of 1974. Each shire was further sub-divided into hundreds (or wapentakes as they were known in parts of the east and north) which varied in number and size between counties.¹¹

The multipurpose agent of royal government in the shires was the sheriff (from 'shire reeve') and he was tasked with executing royal orders (known as writs) in his county, with collecting crown revenue and debts to the crown and delivering them to the exchequer at Westminster, with summoning the posse comitatus (the 'force of the county') to uphold the peace or to lead to the king as shire levies in time of war, with summoning and presiding over the monthly county court and occasionally over the individual hundred courts as well, and also with other legal duties including the arrest and detention of criminals in the county jail and the empanelling of local juries to serve either in the county court or at the law courts in Westminster.¹² After the Conquest, many sheriffs were so-called 'curial' sheriffs:

men with close links to the royal court but often with little or no connection to the county where they held office. Gradually, however, the local gentry gained control of the shrievalty for themselves and by the fourteenth century the sheriff was almost inevitably a local knight of reputable standing, often one who had seen extensive military service in his career.¹³

As powerful and important as the sheriff was, it increasingly became clear that it was impossible for the sheriff and his small permanent staff to do all that was being asked as the demands and reach of royal government and law grew. This was especially so in the aftermath of the outbreak of war with France in 1294. This war, prompted by the French attempt to confiscate Gascony from King Edward I, dragged in first the Welsh and then the Scots who rebelled against Edward's attempts to coerce them to help defend his French lands.¹⁴ The war with Scotland lasted until 1328, restarted in 1332, and subsequently flared and quietened at different points for the rest of the Middle Ages. The original French war petered out with a truce in 1298 before a peace settlement restored the status quo ante in 1303. The French had not given up their designs on Gascony and tried unsuccessfully to seize the duchy in 1324-5. A third attempt in 1337 precipitated the Hundred Years' War which lasted, with only intermittent breaks, until 1453.¹⁵ This war dominated the history not just of England and France in the fourteenth and fifteenth centuries but of western Europe, devastating large parts of France with the fallout affecting Scotland, Wales, the Low Countries, Spain and Italy as well.

'Law State' to 'War State'?

This near-permanent state of war naturally had a profound effect on England and English governance, despite the fact that aside from the occasional invasion scare, the only direct impacts of the war were intermittent Scottish raids across the border and the odd French attack on towns on the south coast. An important argument about these effects, put forward by the historian R.W. Kaeuper in the 1980s, was that the outbreak of war brought to an end a long period of legal and constitutional development of the English 'law state', and heralded the development of a 'war state' where the central government relinquished control over governance and law in return for the resources to fight on at least two fronts against France, the largest and most powerful kingdom in Europe.¹⁶ The crown simply could not sustain both war and state-building and it chose the former at the expense of the latter. This analysis fits quite well with a much older historiography, dating back to Whig historians such as Bishop Stubbs and Charles Plummer, which saw the later Middle Ages as a decline from the achievements of the thirteenth century.¹⁷ It was comprehensively rejected, however, by Gerald Harriss in 1993 when he argued that, far from stifling growth and innovation in government and justice as Kaeuper had thought, prolonged war acted as a driver of important developments in both.¹⁸ The vibrancy of late medieval political culture is now broadly recognized by historians, superseding the Whig view of continuous decline and stagnation before the Renaissance and Reformation.

Harriss' view also conforms to the conclusion historians accept in studies of other periods—that war is a prime factor in state building.

There was a long period in the fourteenth century of experimentation in the delivery of justice, before the justices of the peace (JPs) and the assize (where those indicted by the JPs were sent for trial) emerged as the principal vehicle.¹⁹ Many of the most active justices were drawn from the landed military elite of the shires who, in their different guises, formed the backbone of England's armies, its law enforcement, and its local government. They overwhelmingly staffed the panoply of local administrative offices that emerged in order to provide the king with the money, men, and materiel that he so desperately needed. Unlike the shrievalty, most of these offices were temporary and filled for short periods for a specific purpose usually relating to the war. These included commissioners of array, who raised and lead peasant levies to the muster station; commissioners of tax assessment and collection, who were tasked with raising the money from the 'subsidies' granted by parliament; and commissioners of purveyance, who had the unenviable job of requisitioning – with the questionable promise of payment at an unspecified later date – the huge quantities of food and supplies necessary to feed armies which usually numbered around 10,000 but might be as large as 30,000.²⁰ The military elite also provided the core of the representatives in the Commons, the knights of the shire. England's landed military elite thus served in the king's armies, voted his taxes and collected them, and raised his armies and provided the food to keep them moving, all while keeping the peace at home. Harriss thus saw late medieval England as, at its best, a partnership among the crown, nobility, and gentry that enabled the country to punch hugely above its weight militarily and diplomatically and to compete with France that had ten times the population. Without the contribution of this military elite back home the famous victories won by Edward III at Crecy, the Black Prince (Edward's long-time heir) at Poitiers, and Henry V at Agincourt would simply not have been possible.

'Bastard Feudalism' and English Governance and Society

As hinted at above, prevailing Whig historiography in the late nineteenth and early twentieth centuries saw the late Middle Ages as a period of stagnation, even degeneration. Nowhere was this more marked than in their attitudes towards the nobility and the practice of so-called 'bastard feudalism.' This deliberately pejorative tag was coined by Charles Plummer who regarded 'bastard feudalism' as a debasement from the original concept of feudalism, with the grants of land in return for service which bound a lord and his tenant being replaced by cash fees.²¹ These fees, Plummer thought, were paid to mostly landless ex-soldiers who hung around in the lord's household and enforced his will locally through a combination of inducement, intimidation and, occasionally, brute force. This system, it was argued, thus helped to destabilize English politics in the late Middle Ages, was instrumental in the deposition of no fewer than seven monarchs between 1327 and 1485, and culminated

in the Wars of the Roses where the nobles, with their affinities of armed thugs, turned on the king and each other. That conflict resulted in the self-immolation of the ancient nobility and the emergence of Tudor rule, which presaged the re-establishment of state-building.

K.B. McFarlane, the Oxford medievalist, accepted the name but rejected this interpretation of 'bastard feudalism.' He saw 'bastard feudalism' as something which superficially resembled feudalism rather than something which was simply a debased version of it. Although the currency of reward had changed, from land to cash, it was still the landed gentry, and not Plummer's household thugs, who were receiving it. Far from a corruption of the established order, 'bastard feudalism' was, in the words of one of McFarlane's early students, "part of the normal fabric of society."²² McFarlane's legacy has been much discussed and disputed in the fifty years since his death, but the most convincing picture presented in his work is that of a society where the nobility acted as the gatekeepers between the central government and the gentry in the localities.²³ As Bishop Russell put it in a speech in 1483, "the politic rule of every region well ordained stands in the nobles."²⁴ Of course not every region was "well ordained" all of the time (indeed far too often England's regions were not) but this was not the fault of the 'bastard feudal' system per se.

How did 'bastard feudalism' arise? McFarlane thought it originated in the needs of the nobles to find men-at-arms for Edward I's wars but subsequent historians have seen its purposes as principally domestic and grounded in lords' desire to extend their local power. The truth is that we are not certain how and when it came about. Historians have a good understanding of what 'bastard feudalism' was and how it worked in the last quarter of the fourteenth century and in the fifteenth century. While recent research has rejected the idea that it existed in this form in the thirteenth and even twelfth centuries, scholarship on the intervening period of the fourteenth century has yet to illuminate when, how, and why it did develop.

As yet we cannot be certain, but it seems that the reign of Edward III and the needs of war were the setting and the driving cause behind 'bastard feudalism' and that each point of the triangle—crown, nobility, and gentry—gained from it.²⁵ For the crown, as the number of local offices proliferated, 'bastard feudalism' provided a conduit through which it could access reliable men, nobles being the obvious choice, to fill these vital roles. For the nobility, the pervasiveness of royal government, which had increased to facilitate the waging of war, made it impossible to resist its encroachment on their private jurisdiction. Both at home and in war, 'bastard feudalism' offered them the chance to serve their king as a fully-functioning service nobility, maintaining peace and order in their areas of influence while royal favor offered them a new way to maintain and extend their power at a local level. For the gentry, membership of a 'bastard feudal' affinity, as historians call a lord's following, offered the individual knight, esquire, or gentleman two main things. First, it gave him a way of becoming known to the central government through

his lord's auspices and thus a means of advancement. Secondly, and most importantly, it provided him with the security of his lord's protection. His lord would guarantee his property transactions and would defend his interests through his influence socially, legally and, in extremis, through violence. These things had all previously been done in the lord's feudal court but as the authority of these had waned, there were now achieved through the 'bastard feudal' affinity.

'Bastard feudalism' was thus a system that offered significant advantages to those of the military elite who participated in it. There were certainly losers in the system, those who found themselves excluded from the dominant local affinity for instance, but this is true in any society. Nobody planned the societal shift toward 'bastard feudalism'; all parties rather stumbled into it over a period lasting at least half a century and arguably much longer. It worked, at least until its original purpose—ensuring that the military elite contributed to the war effort domestically as well as in theatre—disappeared with the English defeat in the Hundred Years' War. Before Henry VI's inadequacy as king led to failure abroad and civil war at home, 'bastard feudalism' helped combine both the 'law state' and the 'war state' to great effect.

Dr. Andrew Mark Spencer is a College Lecturer in Medieval History at Christ's College of the University of Cambridge. His research interests focus on governance and warfare in the Middle Ages with particular emphasis on the thirteenth and fourteenth centuries and the development of 'bastard feudalism.' In 2013, Dr. Spencer published his book, *Nobility and Kingship in Medieval England: The Earls and Edward I, 1272-1307*.

1. Adalbéron de Laon, *Poème au Roi Robert*, ed. C. Carozzi (Paris, 1979).
2. *Copiale prioratus Sanctiandree: the letter-book of James Haldenstone, prior of St Andrews, 1418-1443*, ed. J. H. Baxter, St Andrews University Publications, 31 (1930): 219-20
3. A.M. Spencer, *Nobility and Kingship in Medieval England: the earls and Edward I, 1272-1307* (Cambridge, 2014), chapter 1; G.L. Harriss, *Shaping the Nation: England, 1360-1461* (Oxford, 2005): 99.
4. S. Painter, *Studies in the History of the English Feudal Barony* (Baltimore, 1943): 172.
5. Painter, *Studies in the History of the English Feudal Barony*, p. 173.
6. Harriss, *Shaping the Nation*: 99.
7. The fullest account, though by no means universally accepted, is P.R. Coss, *The Origins of the English Gentry* (Cambridge, 2003).
8. Harriss, *Shaping the Nation*: 138.
9. A.M. Spencer, 'A Warlike people? Gentry enthusiasm for Edward I's Scottish campaigns, 1296-1307', in *England's Wars, 1272-1399: the soldier experience*, eds. A. Bell & A. Curry (Woodbridge, 2011): 98. This research is based on knights with two or more manors. The participation of the whole gentry is likely to have been considerably lower.
10. Spencer, 'A Warlike people?': 102.
11. H.M. Cam, *Hundred and the Hundred Rolls* (London, 1930).
12. Cam, *Hundred and the Hundred Rolls*: 67-128, for the best description of the duties of the sheriff.
13. D.A. Carpenter, 'The Decline of the Curial Sheriff in England, 1194-1258', *English Historical Review*, 91 (1976): 1-32.
14. M.C. Prestwich, *Edward I* (New Haven and London, 1997): chapters 15, 16, 18.
15. M. Vale, *The Origins of the Hundred Years' War: the Angevin legacy* (Oxford, 1996).
16. R.W. Kaeuper, *War, Justice and Public Order: England and France in the Later Middle Ages* (Oxford, 1988).
17. W. Stubbs, *The Constitutional History of England* (4th edn., 3 vols., Oxford, 1906).
18. G.L. Harriss, 'Political Society and the Growth of Government in Late Medieval England', *Past and Present*, 138 (1993): 28-57.
19. B.H. Putnam, 'The Transformation of the Keepers of the Peace into the Justices of the Peace, 1327-1380', *Transactions of the Royal Historical Society*, 4th Series, 11 (1928), is the classic account of the development of the magistracy, though it has been challenged recently by Ted Powell and Christine Carpenter who place the full emergence of the peace bench a little later than Putnam. E. Powell, *Kingship, Law and Society: criminal justice in the reign of Henry V* (Oxford, 1989): 14-17; M.C. Carpenter, 'War, Government and Governance in England in the Later Middle Ages', *The Fifteenth Century*, 7 (2007): 1-22.
20. Spencer, *Nobility and Kingship in Medieval England*: 112-13.
21. John Fortescue, *The Governance of England: otherwise called the difference between a limited and an absolute monarchy*, ed. C. Plummer (Oxford, 1885): 15-16.
22. G.A. Holmes, *The Later Middle Ages, 1272-1485* (Edinburgh, 1962): 167.
23. R.H. Britnell and A.J. Pollard, *The McFarlane Legacy: studies in late medieval politics and society* (Stroud, 1995).

24. S.B. Chrimes, *English Constitutional Ideas in the Fifteenth Century* (Cambridge, 1936): 172.

25. M.C. Carpenter, *The Wars of the Roses: politics and the constitution in England c. 1437-1509* (Cambridge, 1997): 1-66 provides the best explanation of the functions of a 'bastard feudal' society.

Moving East and South: U.S. Navy and German Navy Strategy in the Eurasian Theater 1991-2014, A View from Germany

by Dr. Sebastian Bruns

The Cold War ended rather suddenly in 1991. With it went the model on which the United States' maritime strategy of the 1980s had rested. Driven by individuals like John Lehman, President Ronald Reagan's long-time Secretary of the Navy, that series of strategic documents promulgated a forward, offensive, counter-force approach and the famous '600-ship Navy' force structure.

With the formal dissolution of the Soviet Union on December 25, 1991, the sole challenger to U.S. naval power vanished practically overnight. Red Fleet warships were rusting away in port or dismantled altogether. In the United States, the military lost significant human capital through a number of force reduction rounds, which reflected how the U.S. Navy could and would take on the post-Cold War world intellectually. In the wake of this strategic recalibration, allied militaries and their navies—such as the Federal German Navy, soon to be renamed German Navy—also underwent substantial transformations. These were often guided by the shifting geopolitical landscape as well as the popular desire to reduce the inflated defense budgets of Cold War days in order to obtain a peace dividend.

This analysis will focus on the Eurasian theater—very broadly speaking, the waters that surround the European and Southwest Asian landmasses¹—in U.S. and German naval strategy between 1991 and 2014. The maritime sphere has become increasingly important as a domain of emerging security since the end of the Cold War, yet comparatively little time and resources are being devoted to research on naval strategy and relationships between allies at sea. As a result, the use of naval force for political and diplomatic ends and the dynamics of maritime geopolitics have suffered.

This essay seeks to underline the challenges that have confronted the U.S. Navy in the past generation and analyze their long-term effects. While the U.S. Navy's geographic focus and operational interests have increasingly shifted from Europe to the

Middle East and Asia, and from control of the "blue water" high seas to the littorals, these key interests should not be overlooked. In the view of the author, the fall of the Soviet Union and the implication that allies like Germany would do more to patrol their own maritime neighborhood provided the U.S. Navy with a convenient reason to de-emphasize their previously highly valued naval hub in the Mediterranean Sea. In rebalancing from the Sixth Fleet area of responsibility (AOR) to other regions of the world, the U.S. Navy accepted the consequences for fleet design and ship numbers, perhaps willingly using it as a bargaining chip for force reduction rounds in Washington, D.C. Implicitly, European allies and the U.S. Air Force² were expected to fill the gap left behind in terms of naval presence and crisis response, in particular after the successful campaigns in the Adriatic Sea in responding to unrest and war in the Balkans. European allies, however, were largely uninterested in stepping up to the plate; they considered their near abroad safe enough. Most importantly, they were somewhat wary of delivering a combined 'pocket Sixth Fleet' of their own. Finally, they were preoccupied with managing German unification, enlargement of the European Union, and establishing a common market and currency, among other things. Accordingly, this paper sheds a light on some key German strategic documents for a time when the reunited country sought its new place in the security environment of the post-Cold War world.

By taking a unique view from Germany, one of the U.S. Navy's premier NATO allies, this analysis also considers the transformation of the Bundesmarine from an escort navy to an expeditionary navy.³ It seeks to conceptually explain how Germany's security policy addressed the maritime challenges of the new era. The German Navy was principally drawn south- and eastward geographically after 1991, usually in close cooperation with other allied and friendly navies (and mandated by NATO, the EU, or the UN).⁴ It was increasingly asked to address maritime security challenges to which the U.S. Navy no longer, or only in a supporting role, responded. The German Navy went



Sailors aboard the German navy frigate FGS Hessen (F 221) watch as the ship enters Boston Harbor to participate in Boston Navy Week 2012 (MC1 Elisandro T. Diaz/U.S. Navy/120629-N-L0372-154).

into the breach with what were essentially Cold War assets and a mindset fundamentally dominated by the inability to think strategically.

This paper is split into two sections. The first section discusses the 1991–2001 timeframe and the second section covers the period from 2001–2014. 2001 marked the inauguration of President George W. Bush in January and the terrorist attacks on September 11 eight months later. Each section looks at the strategic developments of the U.S. Navy and the German Navy, their major naval operations, and some areas of cooperation between the two navies in Eurasia.

Strategic Shifts, Crisis Management, and Embracing and Empowering of Allies (1991–2001)

The strategic change of the post-1991 world was nothing short of fundamental. Where the old security environment was rigidly bipolar, leading to a certain—if dangerous—predictability of the Communist bloc, the emerging environment fashioned itself as multipolar, complex, and rather uncertain. Alliances such as NATO and international organizations such as the UN underwent significant changes in their mandates, and policy-makers’

expectations towards them often oscillated between high hopes and deep disappointments. The U.S. faced substantially more diverse but much more ambiguous threats. These were no longer directed at U.S. survival (such as a nuclear-tipped conflict over Germany), but rather at U.S. interests (such as regional instability, proliferation, or terrorism). Needing to reevaluate the costs and effects of deterrence, naval missions such as power projection and expeditionary operations became more important.⁵

The U.S. Navy was well suited to address this new complex security environment given its practice as a forward present, combat-ready, and credible force. Intellectually, it retained such a posture and outlook into the 1990s, navigating a number of force-structure reviews such as the Bottom-Up Review (BUR) without too many bruises. In fact, “From the Sea” (1992) and “Forward... From the Sea” (1994) provided the U.S. Navy with a conceptual framework that focused on the littorals and coastal waters—an area to which, as a Norwegian analyst has pointed out, America’s blue-water navy would simply be shifted, rather than be re-built from scratch.⁶ Established Cold War naval missions such as anti-submarine warfare (ASW), anti-air warfare (AAW), anti-surface warfare (ASuW), and escort duties diminished in importance. Amphibious capabilities, strike, sea-based ballistic missile defense (BMD), humanitarian assistance and

disaster relief tasks (HA/DR), more general maritime security operations (MSO), and patrol and presence tasks rose in relevance.

The evolution of U.S. Naval Forces Europe from a “steel-gray stabilizer”⁷ of Cold War days into a slimmer, effective crisis management tool for the emerging conflicts thus remained in a fledging stage. In 1990s Washington, the predominant political elite asked a lot from its Navy. The service would have to simultaneously shrink its fleet size while retaining a sensible force structure, speak to how it would address challenges of the emerging post-Cold War security environment, and still serve as a ‘Swiss Army knife’ to the demands of the Clinton administration’s foreign policy. The European theater, once the front-line of the bipolar conflict, risked dropping off the map.

The trade-off was a substantially decreased military presence in Europe, which yielded a significant reduction of ship numbers and a markedly different posture in particular in the Sixth Fleet AOR.⁸ In any case, the military focus of the United States increasingly moved ‘East of Suez’: The Arabian Gulf and the Horn of Africa became focal points of military action in the early 1990s, even if the Mediterranean remained the site of some major naval operations.⁹

The shift in geopolitical focus areas also left the German military out. If Germany were a book, it would best be characterized as a coming-of-age novel. Germany had recently been reunited and began a process of reconciliation and the rebuilding the former East German economy when the Gulf War broke out in the summer of 1990. During those early years, Chancellor Helmut Kohl (a conservative within a liberal-conservative coalition government) was able to mute allied requests for German boots on the ground through checkbook diplomacy.¹⁰ The effort to punish Iraq for invading its neighbor, Kuwait, was backed diplomatically by a UN Security Council mandate. It also mustered a broad coalition of countries from both former Cold War camps. Still, the German public did not express much sympathy for the U.S.-led military campaign to oust Saddam Hussein from the Emirate. Large organized anti-war protests brought droves of people to German streets and market squares in January and February 1991. In the Rhineland, even the annual Karneval street festivities (a traditional equivalent to Mardi Gras in New Orleans) were cancelled.¹¹

What is often forgotten, but was hardly uncontroversial at the time from the viewpoint of the German public (and that of some allies), was Germany’s important naval contribution in the wake of the Gulf War. “Operation Südflanke” (Operation Southern Flank) ran from 16 August 1990 through 13 September 1991. The German Navy was tasked with supporting the alliance by deploying naval assets in the Eastern Mediterranean—in part to assure partners in the region, but also to fill the void left by the shift of allied troops and ships to the Gulf region. The naval task group of minesweepers and tenders was supplemented by two destroyers, two frigates, and two replenishment ships. Sur-

prisingly, the German Navy, which just a few summers ago had focused exclusively on the Baltic Sea, the North Sea, and parts of the North Atlantic, was now temporarily forward-deployed to Souda Bay, Greece. In the second stage of the operation, the mine-countermeasure ships were deployed to the Persian Gulf to sweep the area in question. Mines posed a serious threat to the naval forces operating in the area. For example, the U.S. Navy’s amphibious assault ship *Tripoli* (LPH 10) suffered significant damages after hitting a mine on 18 February 1991.¹²

After the Middle East dropped off news headlines, the focus of U.S. foreign policy briefly shifted to East Africa. The humanitarian intervention in Somalia resulted in a loss of life and the hasty withdrawal of troops and personnel. The German Navy, having all but absorbed the consequences of taking over the remnants of the East German People’s Navy, was eventually dispatched to Mogadishu in an effort to support the removal of German UN blue helmets in the spring of 1994 (Operation Southern Cross).¹³

By then, Europe had once again caught the attention of U.S. foreign policy. The Clinton Doctrine sought to stabilize former Warsaw Pact member states through economic integration in order to encourage processes of democratization, prosperity, freedom, and value-based politics. America’s relationship with Russia, the main survivor of the disintegrated Soviet Union, was also of premier importance. Militarily and diplomatically, NATO’s Partnership for Peace (PfP) program provided the political avenue to engage with Moscow.¹⁴

Kinetically, the Balkan Wars required substantial military and diplomatic attention. It was only after U.S. intervention that the conflicting parties were amenable to a peace agreement. An international naval coalition, under U.S. leadership and with German participation, upheld an embargo against the warring parties in the Adriatic Sea.¹⁵ This major naval operation gave Germany an opportunity to test and train operationally, but it also engraved the idea that naval contributions were a convenient opportunity to show alliance solidarity without committing boots on the ground for a society still fraught with a number of political caveats when it came to expeditionary operations. At the same time, this was neither reflected conceptually or strategically in German thinking, nor in the fleet design.¹⁶

Germany, a country that expected a serene new world order after managing to peacefully overcome 40 years of division and the frontline status of the superpower conflict, deployed a forward military presence largely through air forces and armies. It was now much less defined by its own or foreign/allied naval forces. This was a function of the existential threat perception that was deeply engraved in the continental (vs. a more maritime) German mindset. It also meant that the German public and policy-makers did not understand the challenges and opportunities associated with the deployment of naval forces.

This contributed to Germany’s reluctance to publish a more substantial strategy for the post-Cold War era. The 1994 White

Book—the first such publication since 1985, and the last until 2006—was all that was deemed necessary to provide the top cover.¹⁷ The transformation of the German Armed Forces from their Cold War mindset, posture, and materiel was painfully slow. Everything else was left to NATO (to which Sen. Richard Luger famously quipped in 1993, “‘Out of area’ or ‘Out of business’”) and, to a degree, the European Union, which was just emerging at the time to be a more prominent common security and defense institution. Conveniently, recent events had demonstrated that a nation which would occasionally support international military missions, but otherwise keep a backbencher’s seat, would fare pretty well. In the absence of territorial threats, Germany could thus increasingly focus on reconciliation, European integration, and general welfare.¹⁸ It also freed the government and the Bundeswehr from the most ravaging demands of modernization, critical thinking, and the formulation of a strategic perspective. In hindsight, it appears that the largest transformation was the name of that particular military branch, which was changed from *Bundesmarine* (or Federal German Navy) to *Deutsche Marine* (German Navy).¹⁹

This is not to imply that the feat of transforming the German

Armed Forces into a modern force was anything but easy; unfortunately, in the absence of political guidance of both Chancellor Kohl and his successor Gerhard Schröder (a Social Democrat in a red-green coalition government), there simply was no debate about German interests, the implications of U.S. withdrawal from Europe, or general security political measures other than where the peace dividend could be invested best.

Only in 1999, when NATO conducted an air war against Yugoslavia over Kosovo, did the public debate in the new capital (Berlin) center on security and defense again. The recently elected coalition of Social Democrats and Greens had to fight vigorously to convince their parties of German participation in the effort.

The following table lists the major naval operations of the United States and Germany for the first full post-Cold War decade. It also includes relevant capstone documents of naval strategic scope.²⁰

On the eve of 11 September 2001, the German Navy was increasingly supporting low-intensity expeditionary operations

Table 1: Major Naval Operations, Capstone Documents 1991-2001		
	United States of America	Germany
Major Naval Operations in the Eurasian Theatre ²¹	August 1990-February 1991: Operations Desert Shield, Desert Storm	August 1990-September 1991: Operation Southern Flank
	August 1992-March 2003: Operation Southern Watch	
	1992-1994: Somalia	January-April 1994: Operation Southern Cross
	June 1993-October 1996: Operation Sharp Guard ²²	
	March-June 1999: Operation Allied Force	
	STANAVFORLANT, STANAVFORMED, Exercises/Work-Ups (temporarily/on occasion)	
	Major Capstone Documents/Policy Reviews ²³ (italics denote overarching guidance)	The Way Ahead (1991)
<i>Base Force Report</i> (1991)		
From the Sea (1992)		<i>Defense Policy Guidelines</i> (1992)
<i>Bottom-Up Review</i> (1993)		
Forward... From the Sea (1994)		<i>White Book</i> (1994)
Anytime, Anywhere (1997)		
<i>Quadrennial Defense Review</i> (1997)		
Strategic Concept of the [NATO] Alliance (1999)		

Table 2: Major Naval Operations, Capstone Documents 2001-2014

	United States of America	Germany
Major Naval Operations in the Eurasian Theatre	Operation Active Endeavour (since 2002)	
	Operation Enduring Freedom (TF 150) (since 2002, German participation ended)	
	Operation Iraqi Freedom (2003)	
	Tsunami Relief (2004/2005)	
		UNIFIL (2006, ongoing)
	Counter-piracy ops (GER: EU NAVFOR Atalanta; US: CTF-151, NATO's Ocean Shield, since 2008, ongoing)	
	Operation Odyssey Dawn (2011)	
	Operation Reccyr (2014)	
	SNMG 1/2, Exercises/Work-Up (temp./on occasion)	
		SNMCMG 1/2
Major Capstone Documents/Policy Reviews (italics denote overarching guidance)	<i>Quadrennial Defense Review</i> (2001)	
	Sea Power 21 & Global CONOPS (2002)	
		<i>European Union Security Strategy</i> (2003)
	Naval Operations Concept (2006)	
	<i>Quadrennial Defense Review</i> (2006)	<i>White Book</i> (2006)
	CS-21 (2007)	
	Naval Operations Concept (2010)	
	<i>NATO Strategic Concept "Active Engagement, Modern Defence"</i> (2010)	
	<i>Quadrennial Defense Review</i> (2010)	
		<i>Defense-Policy Guidelines</i> (2011)
	<i>[NATO] Alliance Maritime Strategy</i> (2011)	
		<i>European Maritime Security Strategy</i> (2014)

that the German government by implication—not by strategic clarity—tasked it to do. The U.S. Navy, in the meantime, had to overcome threats to its substantial force structure, battle with the effects of a number of scandals, and address the increasingly littoral challenges of the emerging, unipolar security environment.

9/11, Maritime Security, and Europe's Flanks

Soon after the 9/11 attacks on New York City and Washington, D.C., a PASSEX (passing exercise) took place at sea off the coast of East Africa. The officers and crew of the German destroyer Lütjens (D 185) rendered honors to the U.S. Navy's guided-missile destroyer Winston S. Churchill (DDG 81) by lining the rails in their dress blues as they came alongside in a passing exercise. The German sailors, who had become good friends with many of the crew on board Churchill, were flying an American flag at half mast and had hung a homemade banner that read, "We Stand by You." The ships had been conducting joint exercises off the coast of the United Kingdom prior to the terrorist attack on the United States.

Aside from the marked details that should excite almost every naval historian, this encounter signaled a new chapter in U.S.-German relations. The Global War on Terrorism (announced in the wake of the terrorist strikes) finally and fully shifted the focus of the United States away from Europe to the Middle East and Southwest Asia, where they fought the perpetrators and supporters of 9/11 in two larger wars. The attacks on the World Trade Center and the Pentagon as well as the downed aircraft in Shanksville, Pennsylvania threw the U.S. off-balance conceptually, and strategists scrambled to bring strategy up to date to the perceived and actual threats. In terms of naval missions, strike warfare and maritime security operations were in increasingly high demand, while the demand (and appreciation for) mine warfare, ASW, AAW, and ASuW further diminished in the absence of a sea control challenger.

Geopolitically, the focus area—dubbed the 'broader Middle East' or even the 'Arc of Instability'—had massive maritime flanks, yet the conflicts were largely land-centric and relied heavily on Army, Air Force, and Marine Corps units. Still, the sea lanes of communication were quickly considered a possible route for terrorist networks to do their harm: "Operation Active Endeavour" in the Mediterranean, to date NATO's only Article 5 operation, and "Operation Enduring Freedom" in the Western Indian Ocean (Task Force 150) were counter-terrorism naval operations with significant U.S. and German naval commitments.²⁴ When the political and military focus moved to Afghanistan and Iraq (in what turned out to be lengthy and costly ground campaigns), public attention also shifted away from the maritime scene, even as the naval operations continued. In Germany, the Horn of Africa once again became a focal point with the rise of pirate activity in the years until 2008, and the subsequent European Union counter-piracy effort.²⁵ In the German Navy's mindset and that of its political masters in Berlin, the

European maritime flanks played little to no role.

The United States, under the burden of fighting two wars in the Middle East, shifted its focus away from Europe and its neighbors. Anecdotal, but illustrative nonetheless, is the U.S. Navy's participation in the annual BALTOPS exercise in June in the Baltic Sea, led by the U.S. since 1971. In the 1990s, the heyday of NATO's Partnership for Peace initiative, U.S. participation in the exercise consisted at times of two Ticonderoga-class guided-missile cruisers, state-of-the-art attack submarines, or even Coast Guard cutters. Since the turn of the century, the aging command ship Mount Whitney (LCC 20), the sole remnant of forward-based U.S. naval power in the Mediterranean, became the principal and largest unit to participate in the exercise (on occasion accompanied by a frigate or a cruiser) to symbolize the shift of attention and resources away from Northern Europe.²⁶

Germany too, in what little security outlook it had developed, was principally focused on Afghanistan. Even the brief Russo-Georgian War in 2008 did little to shift attention to a possible return of great-power politics in the Eurasian arena—in part because Germany and the U.S. were devoting considerable attention to the management of a financial crisis.

In the background, two developments of note for naval strategy occurred. First, in the rapid globalization of goods and services, it became clear that the maritime lifelines of the "First World" were more and more vulnerable to disruption, given the amount of cargo transported by ships and often passing through narrow chokepoints on their way from exporter to importer.²⁷ In parallel, this offered a glimpse into what academic circles labeled as "securitization" of maritime security. As the term broadened, the wording soon meant many different things to many different people.²⁸ Eventually its meaning and potential political leverage diluted.

At the same time in the U.S., a new maritime strategy was being drawn up. In part to make sense of a Navy in an era of counterinsurgency campaigns in Central Asia, but also in part to console allies who were irritated by President George W. Bush's policies, the Navy devised a fundamentally new conceptual idea to explain the use of naval forces in the 21st century. Instead of emphasizing geographic regions of the world, the defense of maritime trade routes took center stage. This was in principal attractive to allies such as Germany (which was Europe's industrial powerhouse and very dependent on functioning maritime trade). Unfortunately, the capstone document ("A Cooperative Strategy for 21st Century Seapower", issued in the fall of 2007) never got a complementary force-structure plan and was furthermore subject to the broader political shifts at stake (e.g., policy focus on management of financial crisis, wars in Afghanistan/Iraq, a change of Presidents from George W. Bush to Barack Obama, political gridlock in Washington, the emergence of the Chinese People's Liberation Army Navy as a peer competitor for the United States, etc.).

In Germany, President Horst Köhler, then Germany's constitu-

tional head of state, carefully articulated that trade routes needed to be defended using military force on 31 May 2010. In an interview, the President had rephrased this notion (having the Horn of Africa in mind), which could already be found in the White Book issued in 2006; the resulting media frenzy led to his early withdrawal from office. The conservative-liberal government voted against deploying the Bundeswehr (and the German Navy, for that matter) in the NATO-led operations against Libya in 2011, which underlined Germany's uneasy relationship to the use of force once more. As it stands, this decision occurred for domestic reasons. While politically sensible in hindsight (currently, Libya is descending into civil war and makes for the site of thousands of refugees seeking to cross the Mediterranean), the withdrawal of the frigate *Niedersachsen* (F 208) from the NATO SNMG sent a disastrous signal to Germany's allies. At the same time, the German Navy remained active in OAE and Operation Atalanta, integrated modern air-defense frigates into U.S. aircraft carrier strike groups, and supported an international coalition's effort to neutralize Syrian chemical weapons at sea in 2014.

The following table lists the United States and Germany's major naval operations for the second full post-Cold War decade. It also includes relevant capstone documents of naval strategic scope.²⁹

In the decade since 9/11, there has been a considerable uptick in the use of naval forces by the U.S. and Germany even when land-centric thinking and military campaigns dominated the first few years. The development of strategy, naval operations, and the real-world politics is a murky and ultimately chaotic one set to confuse the electorate, motivate the policy-maker to shy away from strategic thinking, and leave it to the political scientist and later, to the naval historian, to try to understand.

Conclusion

After the end of the Cold War, the North Atlantic alliance and Europe enjoyed a sudden period of relative peace and stability. The major geopolitical and intellectual threat that had galvanized strategic thinking and military action for more than four decades had vanished. New challenges emerged quickly, forcing naval forces and their political masters to re-organize to meet them organizationally, strategically, and operationally, at sea. In the aftermath of 9/11, Southwest Asia was thrust into the focus of world events. Towards the end of the first decade of the 21st century, with potential political-military solutions underway for the conflicts in Afghanistan and Iraq, with the development of a new U.S. maritime strategy (CS-21), and the general conflict fatigue in Europe and North America, the components and conditions of the new multipolar world order began to take shape. The rise of China as a naval and geostrategic competitor was set to occupy the minds of President Barack Obama's administration. Politically, the 'pivot to Asia' insinuated to Europe and the Middle East that the U.S. could potentially leave them alone for good. Recent events in these very regions, such as the

rise of the Islamic State and the war in Syria as well as Russian actions have demonstrated is a disheartening sign.

Conceptually and strategically, the 'pivot to Asia' remains a bridge too far for Central Europe. Germany does not regard China, but rather the turmoil in the wake of the 2011 revolutions in the Arab World as well as the fallout of the Euro crisis and the war in Syria as more direct challenges to its security and interests. While it is certainly too soon to call the verdict on what the events since 2014 in the European perimeter really mean, it could very well be that a re-pivot to Europe is already underway. The Sixth Fleet AOR is gaining increasingly more importance, seeing more U.S. naval forward presence, and NATO and the EU hope that their strategies and militaries will be appropriate to the emerging environment. The U.S. Navy's CS-21R, the forthcoming German White Book (2016), and the work-in-progress German maritime strategy will be benchmarks to estimate how much of a crucial political tool naval forces can be, and how much strategic leverage they can provide.

Dr. Sebastian Bruns directs the Center for Maritime Strategy & Security at the Institute for Security Policy (University of Kiel Germany). This paper was prepared for the McMullen Naval History Symposium, United States Naval Academy, Annapolis, MD (September 2015) for the section *From Interregnum to Rivalry: U.S. Navy Strategy in the Post-Cold War World, 1991-2014*. Abbreviations and acronyms are explained in the appendix.

Abbreviations & Acronyms

AAW: Anti-Air Warfare
AOR: Area of Responsibility
ASuW: Anti-Surface Warfare
ASW: Anti-Submarine Warfare
BALTOPS: Baltic Operations
BMD: Ballistic Missile Defense
CTF: Combined Task Force
EU: European Union
EU NAVFOR: European Union Naval Forces
HA/DR: Humanitarian Assistance/Disaster Relief
MSO: Maritime Security Operations
NATO: North Atlantic Treaty Organization
PfP: Partnership for Peace
SNMCMG: Standing NATO Mine Counter-Measures Group
SNMG: Standing NATO Maritime Group
STANAVFORLANT: Standing Naval Force Atlantic
STANAVFORMED: Standing Naval Force Mediterranean
WEU: Western European Union
UN: United Nations
UNIFIL: United Nations Interim Force Lebanon

Bibliography

Autorenteam Flottenkommando (2012), "Die Deutsche Marine ist eine Marine im Einsatz", in *MarineForum* 11/2012, pp. 8-13.

British Broadcasting Company (2016), "How music is helping Cologne move on from New Year's Eve", <http://www.bbc.co.uk/newsbeat/article/35515642/how-music-is-helping-cologne-move-on-from-new-years-eve>.

Bruns, Sebastian (2014), *U.S. Navy Strategy & American Sea Power from 'The Maritime Strategy' (1982-1986) to 'A Cooperative Strategy for 21st Century Seapower' (2007): Politics, Capstone Documents, and Major Naval Operations 1981-2011*. Kiel: Dissertation.

Bueger, Christian (2013), Theorien der Maritimen Sicherheit: Versicherungstheorie und sicherheitspolitische Praxeographie, in Sebastian Bruns/Kerstin Petretto/David Petrovic (eds.), *Maritime Sicherheit*, Wiesbaden: VS-Verlag/Springer, pp. 25-36.

Chiari, Bernhard (2007), Von der Escort Navy zur Expeditionary Navy. Der deutsche Marineeinsatz am Horn von Afrika, in Militärgeschichtliches Forschungsamt (ed.), *Horn von Afrika. Wegweiser zur Geschichte*, Paderborn: Schöningh, pp. 127-139.

The Federal Ministry of Defence on behalf of the Federal Government (1994), White Paper on the Security of the Federal Republic of Germany and the Situation and Future of the Bundeswehr, Bonn: Press and Information Office.

Hattendorf, John (ed.) (2006), *U.S. Naval Strategy in the 1990s: Selected Documents* (=Naval War College Newport Papers #27), Newport: Naval War College Press.

Haynes, Peter (2015), *Toward a New Maritime Strategy. American Naval Thinking in the Post-Cold War Era*, Annapolis: U.S. Naval Institute Press.

Hoch, Gottfried (1994), "Southern Cross – Marineverband Somalia", in *MarineForum* 7/8-1994, pp. 230-232.

Horten, Dirk (1999), Die Seeinteressen der Bundesrepublik Deutschland (1996), in Jörg Duppler (ed.), *Seemacht und Seestrategie im 19. und 20. Jahrhundert*, Hamburg: Mittler, pp. 265-282.

Jopp, Heinz Dieter (1995), „Aus maritimer Sicht brauchen wir eine Strategiediskussion in der Öffentlichkeit“, in *MarineForum* 10-1995, pp. 2-4.

Lippke, Hajo (2009), *Die Zukunft der Deutschen Marine*, Frankfurt et al.: Peter Lang (=German Strategic Studies #5).

Lundesgaard, Amund (2011), "US Navy strategy and force structure after the Cold War", Report, Oslo: Institutt for Forsvarsstudier (IFS).

McGrath, Bryan, Eaglen, Mackenzie (2014), "America's Navy Needs 12 Carriers and 3 Hubs", Washington, D.C.: Hudson Institute, <http://www.hudson.org/research/10159-america-s>

<http://www.hudson.org/research/10159-america-s> navy-needs-12-carriers-three-hubs (1 September 2015).

North Atlantic Treaty Organization (2005), *Sicherheit durch Partnerschaft*. Brussels: NATO Public Diplomacy Section.

Papadopoulos, Sarandis (2005), "The Steel Grey Stabilizer: The Sixth Fleet in Three Crises, 1946-1958", unpublished working paper, Washington, D.C.: Naval Historical Center.

Papadopoulos, Sarandis (2013), "The U.S. Navy's Contribution to Operation Sharp Guard," in Gary E. Weir/Sandra Doyle (eds.), *You Cannot Surge Trust. Combined Naval Operations of the Royal Australian Navy, Canadian Navy, Royal Navy, and United States Navy, 1991-2003*, Washington: Naval History and Heritage Command, pp. 83-99.

Schneller, Robert (2007), *Anchor of Resolve: A History of U.S. Naval Forces Central Command Fifth Fleet*, Washington, D.C.: Naval History and Heritage Command.

Seidler, Felix (2013), Enduring Freedom und Active Endeavour: Wie effektiv kann maritime Terrorismusbekämpfung sein?, in Joachim Krause/Stefan Hansen (ed.), *Jahrbuch Terrorismus 2013-2014*, pp. 379-400.

Seidler, Felix (2015), *Maritime Herausforderungen der NATO. Strategische Auswirkungen und die Effektivität des Handelns*, Frankfurt et al.: Peter Lang (=German Strategic Studies #8).

Swartz, Peter M., with Karen Duggan (2012a), *US Navy Capstone Strategies and Concepts (1991-2000)*, Strategy, Policy, Concept, and Vision Documents, Alexandria: Center for Naval Analyses, <http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/u/us-navy-capstone-strategies-concepts-1991-2000.html> (1 September 2015).

Swartz, Peter M., with Karen Duggan (2012b), *US Navy Capstone Strategies and Concepts (2001-2010)*, Strategy, Policy, Concept, and Vision Documents, Alexandria: Center for Naval Analyses, <http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/u/us-navy-capstone-strategies-concepts-2001-2010.html> (1 September 2015).

Vego, Milan (2007), "On Major Naval Operations", *Naval War College Review* Vol. 60, No. 2, pp. 94-126.

1. The Baltic Sea, the North Sea, the Norwegian Sea, the Arctic Sea, the (Eastern) Atlantic, the Mediterranean Sea, and the Black Sea, the Arabian Gulf, and the (Western) Indian Ocean.

2. Peter Swartz, email to author, 04 September 2015.

3. Chiari (2007), pp. 127-139.

4. White Paper on the Security of the Federal Republic of Germany and the Situation and Future of the Bundeswehr 1994.

5. Bruns (2015), p. 184.
6. Lundesgaard (2011), p. 11.
7. Papadopoulos (2005), n.p.
8. Many critics who today blame the deteriorating security in the Mediterranean perimeter in the wake of the 2011 Arab Spring, and the lack of American political and military leverage, on the withdrawal of major force projecting naval units from the theater often fail to recognize that the strategic outlook of the 1990s – and the corresponding foreign policy of President Bill Clinton – simply did not lend itself to maintaining a forward hub like in the Cold War days. What they imply, however, is still valid: naval forces are expensive, but once they are withdrawn or scaled down, it is difficult to stand them back up quickly. For an example, see McGrath/Eaglen (2014). As a Captain (USN), Bryan McGrath was the lead author of the “Cooperative Strategy for 21st Century Seapower” (2007).
9. Bruns (2014), pp. 225-232.
10. This was, in part, also motivated by constitutional concerns. The German Supreme Court ruled only in 1994 that German military deployments abroad – outside of European Union/ NATO areas – were constitutional.
11. BBC (2016), n.p.
12. Schneller (2007), p. 29.
13. Hoch (1994), pp. 230-232.
14. NATO (2005), pp. 4-13.
15. Papadopoulos (2013), pp. 83-99.
16. It would, in 2006, be reflected in the organization of the German Navy which then changed from half a dozen type flotillas to two comprehensive flotillas based in Wilhelmshaven and Kiel.
17. The German defense ministry currently works on the 2016 incarnation of the White Book, the first since 2006.
18. Herfried Münkler, a noted German political scientist, has diagnosed this as a “post-heroic” mindset. Heinz Dieter Jopp’s scathing critique of the lack of a strategy discussion in the public goes back to 1995 (Jopp: 2-4).
19. The Army (*Deutsches Heer*) and the Air Force (*Luftwaffe*) retained their name over re-unification.
20. The relevant U.S. documents can be found in Hattendorf (ed., 2006). For details on the 1991-2001 evolution of U.S. Navy capstone documents in context, see Swartz (2012a). Analyses of that period may be found in Lundesgaard (2011: 6-16), Bruns (2015: 173-240), and Haynes (2015: 35-147). For Germany, the documents and, more importantly, sound academic analyses for the naval realm are difficult to come by. Aspects were touched on by Horten (1999) and Lippke (2009: 70-92, 162-184).
21. For the purpose of this paper, a major naval operation is understood as the deployment of naval assets in significant numbers to an expeditionary operation, in peacetime, crisis, or war, in joint and combined operations. On the concepts of major naval operations, see Vego (2007).
22. Two preceding operations were merged: Operation Maritime Guard (NATO) and Operation Sharp Fence (WEU).
23. A direct comparison of capstone documents is challenging due to the distinct framework conditions (institutionally, politically, etc.) in different countries. The documents often have varying audiences, altitudes, and authors. They are listed here and in illustration 2 merely for the sake of outlining the principal guiding documents of the era for the U.S. Navy and the Germany Navy.
24. Seidler (2013), 379-400.
25. For political reasons, Germany is very active in the EU’s naval operation, but not in NATO’s complementary counter-piracy efforts, nor in the U.S.-led CTF-151.
26. Even if the U.S. naval presence in Northern European waters was substantial, it fell dramatically short in comparison to the 1980s where, in line with “The Maritime Strategy”, battleships such as the Iowa (BB 61) and helicopter carrier/amphibious assault ships pulled into Kiel and the Baltic Sea.
27. Although the threat of maritime terrorism, in the view of this author, is largely overblown, there were some marked instances of attacks on warships and commercial vessels in the period under observation.
28. Bueger (2013), pp. 25-36.
29. For details on the evolution of U.S. Navy capstone documents since 2001 in context, see Peter Swartz (2012b). For thorough analyses of that particular period of time, see Lundesgaard (2011: 17-26), Bruns (2015: 241-310), and Haynes (2015: 148-238). For Germany, see Autorenteam Flottenkommando (2012). On NATO, see the recently published German-language analysis by Felix Seidler (2015).

The Bypass: Ahmad Chalabi, Dick Cheney, and the Disbanding of the Iraqi Army

by Michael Wackenreuter

On March 12, 2003, a week before the invasion of Iraq, a Principals Committee meeting of the National Security Council was held at the White House to formally decide the fate of the Iraqi Army.¹ The participants, having all received extensive briefings on the subject prior to meeting, voted unanimously and with little discussion that after disbanding the Republican Guard, the “regular soldiers” of the Iraqi Army would be called “back to duty.”² In spite of this decision, on May 23, 2003, L. Paul Bremer III—President Bush’s “special envoy” in Iraq—announced Coalition Provisional Authority Order No. 2, “Dissolution of Entities.” Among the relevant entities to be dissolved by the decree was the Iraqi Army.³

In an interview with the journalist Robert Draper at the end of his presidency, President Bush commented on this apparent dissonance when he remarked, “The policy was to keep the army intact; didn’t happen.” When asked further of his reaction when he found out about the decree, Bush replied, “Yeah, I can’t remember, I’m sure I said, ‘This is the policy, what happened?’”⁴ Having endured significant criticism over CPA Order No. 2, Mr. Bremer was quick to defend himself, providing letters to *The New York Times* to and from the president “in order to refute the suggestion in Mr. Bush’s comment that Mr. Bremer had acted to disband the army without the knowledge and concurrence of the White House.”⁵

Such a puzzling exchange over such an important topic serves to illustrate a larger point. That is, despite its centrality to America’s involvement in Iraq, from the emergence of the insurgency onward to its current conflict with ISIS, it still remains unclear how and why the decision to disband the Iraqi Army was made.

In this paper, I demonstrate that the impetus for CPA Order No. 2 came from the prominent Iraqi exile Ahmad Chalabi, and was carried out under the authority of Vice President Richard “Dick” Cheney by a small group of Chalabi’s supporters in the Office of the Vice President and the Pentagon. I do so first by establishing the lengths to which those in the vice president’s office, in concert with like-minded officials at the Defense Department, were willing to go in order to support Chalabi, who

avored disbanding the army. Secondly, I identify the striking similarities between the events surrounding the order and other instances involving the vice president that involved a bypass of the normal interagency policy-making process.

The Plan

On January 17, 2003, Douglas Feith, the Undersecretary of Defense for Policy, “called Jay Garner, a retired lieutenant general, and asked him to take charge of postwar Iraq” as the head of the Office of Reconstruction and Humanitarian Assistance (ORHA). Having served as the commander for Operation Provide Comfort—a humanitarian mission to provide assistance to Iraqi Kurds following the Gulf War—Garner was considered a natural choice for the type of short occupation mission envisioned by policy-makers at the time, given both his familiarity with Iraq and his “experience providing humanitarian aid on Iraqi soil.”⁶

As Garner began preparing to assume his duties, he asked “Feith for copies of planning documents that had been drawn up in the Pentagon and elsewhere in the U.S. government.”⁷ Despite the fact that Garner was given only 7 weeks to prepare for assuming responsibility for postwar Iraq (equivalent to “what it takes to get a computer connection at the Pentagon,” said one DOD official),⁸ Feith told Garner “that nothing useful existed and that he should develop his own plans.”⁹

This was not the case, however.

In fact, under the State Department’s “Future of Iraq Project,” a team of over 200 Iraqi exiles comprising seventeen working groups had been drafting working documents “designed systematically to cover what would be needed to rebuild the political and economic infrastructure” of postwar Iraq.¹⁰ On the subject of what to do with regard to the Iraqi Army, the recommendations of the “Future of Iraq” project, along with the Army War College and the Center for Strategic and International Studies (CSIS), were unambiguous: it should be left intact.¹¹

The case for reforming, rather than disbanding, the Iraqi Army was clear, and given ensuing events, hauntingly prescient. The first concern outlined was that by dissolving the army, one created “an instant enemy class: hundreds of thousands of men who still had their weapons but no longer had a paycheck or a place to go each day.” Manpower that could be used for security could instead become part of the “security threat.” The second concern, according to the Army War College, revolved around the fear that dissolving the “army in the war’s aftermath could lead to the destruction of one of the only forces for unity within the society.”¹²

Chain of Command

On February 28, 2003, Garner was able to meet for the first time with the President and his “war cabinet” to discuss his plans for Iraq in the war’s aftermath. In particular, Garner focused on how he “planned to maintain stability in Iraq after combat.” Referring to a talking point entitled, “Postwar use of Iraqi Regular Army,” Garner stated, “We’re going to use the army. We need to use them. They have the proper skill sets.”¹³

When asked to speculate on how many he would use, he answered, “I’m going to give you a big range. It’ll be between 200,000 and 300,000.” As he looked around the room, Garner saw “all the heads were bobbing north and to south. Nobody challenged. Nobody had any questions about [the] plan.”¹⁴

Garner’s plan was predicated partially on his suspicion that the war plan being devised by Secretary Donald Rumsfeld and Army General Tommy Franks “called for a force level dramatically below the 500,000 in the initial war plan for Iraq.” He believed, however, that “with another 100,000 U.S. forces that could flow in after combat began, plus some 200,000 to 300,000 from the Iraqi army who could be turned to work with the U.S. forces, it was possible to have some measure of security and stability.”¹⁵

The 500,000 troops number Garner referenced closely matched the findings of a RAND Corporation study conducted before the war which found, using examples from seven previous occupations, “that to achieve stability in the initial years after military occupation there should be twenty occupying troops for every one thousand people in the country occupied.” Given that the population of Iraq at the time was approximately 25 million, meeting the proposed ratio required a troop presence of 500,000, or “more than three times the number of foreign troops” that would eventually deploy to Iraq.¹⁶

Military commanders were also on board with the decision, having long integrated “the idea of using the Iraqi Army” as part of their plans. According to Colonel John Agoglia, who served as a war planner on General Franks’ staff at Central Command, “Starting in June 2002 we conducted targeted psychological operations using pamphlet drops, broadcasts and all sort of means to get the message to the regular army troops that they should

Secretary of Defense Donald H. Rumsfeld with US Ambassador to Iraq, L. Paul Bremer III at Baghdad International Airport, February 23, 2004 (Lisa M. Zunzanyika/USAF/DOD 040223-F-0881Z-001).



surrender or desert and that if they did that we would bring them back as part of a new Iraq without Saddam.”¹⁷

Chalabi and the Neocons

To understand why Feith declined to inform Jay Garner of the existence of the Future of Iraq Project in the first place, one must understand the connection between Chalabi and prominent neoconservatives in the Bush Administration, beginning in the Office of Special Plans.

The Office of Special Plans was established under Deputy Secretary of Defense Paul Wolfowitz by Douglas Feith, and was overseen by William J. Luti, a retired naval officer who had previously worked in Vice President Cheney’s office. The most important function of the Office of Special Plans was to provide a “closer examination of all intelligence information to find links between Iraq and al-Qaeda and evidence of Saddam Hussein’s weapons of mass destruction that other analysts might have overlooked or underappreciated.” The office’s other function, and one in which it maintained “close contact” with the Vice President’s Chief of Staff Scooter Libby, was to “manage the Pentagon’s relationship with its favored candidate to replace Hussein, Iraqi exile Ahmad Chalabi, a leading supporter of anti-Saddam intelligence.”¹⁸

A highly educated, secular Shiite from a prominent Baghdad family, Chalabi—as the head of the Iraqi National Congress (INC)—had assiduously cultivated a network of hawkish supporters around Washington since the mid-1990’s who supported his goal of regime change. Following the demise of Communism, “the neoconservatives were eager for a new cause, and Chalabi...who was accepting of Israel and talked about spreading democracy throughout the Middle East - capitalized on their enthusiasm.”¹⁹ Included among those he met with during this period were Richard Perle, Paul Wolfowitz, Douglas Feith and Dick Cheney, all of whom would play crucial roles in his journey during the Bush administration.²⁰

Despite such influential supporters, however, Chalabi was not without his detractors. “At CIA headquarters in Langley... Chalabi was so despised that no one there wanted anything to do with him - period.”²¹ The CIA’s disdain for Chalabi stemmed from a failed operation conducted jointly between Chalabi’s Iraqi National Congress and the CIA in 1995 to overthrow Saddam from a base inside Iraqi Kurdistan. “Chalabi didn’t deliver a single lieutenant, let alone a colonel or general,” remarked Robert Baer, the CIA agent who oversaw the operation.²²

Despite this hostility, Chalabi’s campaign to move the policy of regime change in Iraq to the forefront of American foreign policy making reached a turning point in October, 1998 with the passage of the Iraq Liberation Act. “Crafted by Chalabi” and his “allies in Congress,” the legislation formally made regime change the policy of the United States government with regard to Iraq.²³

Chalabi, The Bush Administration, and Weapons of Mass Destruction

Following the 9/11 attacks and the anthrax scare that swept the nation, Chalabi received a call from John P. Hannah, a national security aide of the vice president. Hannah told Chalabi that “the administration [was] looking for people who know about Iraq’s weapons of mass destruction, Iraqis who know about these weapons firsthand,” and asked if he could introduce them to any.²⁴

This exchange began “what would become perhaps the signature scandal in the lead-up to the 2003 invasion of Iraq: the procurement of Iraqi defectors whose bogus tales of WMD and Iraqi-sponsored terrorism permeated the press and circulated at the highest levels of the U.S. government.”²⁵ These defectors would assert among other things that the Iraqi military had been given training “for airline hijacking and assassinations”, as well as that Saddam was working on “secret facilities for biological, chemical and nuclear weapons [located] in underground wells, private villas and under the Saddam Hussein Hospital in Baghdad.”²⁶

Despite the reservations of those in the CIA’s Counterterrorism Center regarding the veracity of these defectors, some of whom were suspected of being “coached to lie by the INC,” senior Pentagon officials remained confident that “Chalabi [was] a valuable conduit of information with a track record that was far and away better than the agency’s.”²⁷ Chalabi also “provided defector allegations to just about every respectable news outlet in the country, including The Wall Street Journal, Time, Newsweek, Vanity Fair, The New Yorker, USA Today, UPI, and Fox News.”²⁸

According to David Frum, a Bush administration speechwriter, the vice president’s relationship with Chalabi was also deepening during this period:

*I was less impressed by Chalabi than were some others in the Bush administration. However, since one of those “others” was Vice President Cheney, it didn’t matter what I thought. In 2002, Chalabi joined the annual summer retreat of the American Enterprise Institute near Vail, Colorado. He and Cheney spent long hours together, contemplating the possibilities of a Western-oriented Iraq: an additional source of oil, an alternative to U.S. dependency on an unstable-looking Saudi Arabia.*²⁹

Cheney’s growing affinity for Chalabi during this period may be explained by the influence of the noted academic Bernard Lewis, a widely hailed expert on the Middle East. “Over a series of lunches at the vice president’s residence in 2002, Lewis laid out his case for using American military power to change the regime in Iraq...Force was what Arabs respected. A conclusive show of strength could catalyze a change in the opposite direction.” In Lewis’ analogy, “the exiled Chalabi would play the role of the secularizing Mustafa Kemal Atatürk, reorienting his

country toward the West.³⁰

By the spring of 2002, the hard work that Chalabi and the INC had put in was paying off:

*Rumsfeld and Wolfowitz began urging the President to release more than ninety million dollars in federal funds to Chalabi. The 1998 Iraq Liberation Act had authorized ninety-seven million dollars for the Iraqi opposition, but most of the funds had not been expended. The State Department opposed releasing the rest of the money, arguing that Chalabi had failed to account properly for the funds he had already received. "The Vice-President came into a meeting furious that we hadn't given the money to Chalabi," the former official recalled. Cheney said, "Here we are, denying him money, when they"—the Iraqi National Congress—"are providing us with unique intelligence on Iraqi W.M.D.s."*³¹

Having helped to provide the intelligence necessary to secure public support for the war to his benefactors in the U.S. government, Chalabi now stood to benefit as policy began to take shape under the influence of his most influential admirers, none of who stood more powerful than Cheney.

The Threat of Thomas Warrick

On February 21, 2003, Garner convened a "pre-deployment rock drill" at the National Defense University. As the meeting began, he noticed—first to his annoyance, and later to his grudging respect—that one man in particular "was asking the right questions and providing insightful comments" among the over 100 attendees. The man in question was Thomas Warrick, head of the Future of Iraq Project.³²

After speaking with him and learning of the extensive research he had overseen as director, Garner quickly offered Warrick a job with ORHA. Within a week, however, Rumsfeld informed Garner that he had to remove him:

"Why?" Garner replied. "Warrick has a difficult personality, but he's probably the smartest guy I've got."

"Look, I got this request from above me," the defense secretary said. "I can't defer it. You're just going to have to do what I ask."

*Garner said he was told later that Dick Cheney had objected to Warrick's involvement in ORHA. The reason, like so many foolish decisions before the war, had to do with Ahmad Chalabi. Warrick regarded Chalabi as a smarmy opportunist who believed in democracy only so long as it suited his own interests. The vice president's office, which wanted Chalabi to lead a liberated Iraq, deemed Warrick a threat to its man.*³³

Thomas Warrick was not to be the last "threat" the vice president's office would remove in order to protect their man, however. In fact, "Chalabi's backers in the Bush administration never wavered from their commitment to installing him in power.

After Bush decided against establishing a government-in-exile, Chalabi pushed his backers to endorse the formation of a nucleus provisional government. When this failed, the Pentagon reverted to Plan C."³⁴

Plan C would involve a "rolling transition" where "ORHA would hand over power to an interim Iraqi administration that would run day-to-day affairs and reconstitute Iraq's military...Once the constitution was written, a sovereign administration would be established and elections organized within two years. Chalabi's backers reasoned that giving Chalabi and the Iraqi National Congress control of Iraq's reconstruction would eventually put him in a position to assume political leadership in Iraq."³⁵

Despite the failure of these plans to come to fruition, the faith of Cheney in Chalabi was virtually unshakeable. In the fall of 2003, amidst signs of the impending chaos that would engulf Iraq following the initial success of the invasion, "Dick Cheney approached his longtime colleague [Secretary of State] Colin Powell, stuck a finger in his chest, and said, 'If you hadn't opposed the INC and Chalabi, we wouldn't be in this mess.'"³⁶

Change of Plan

Following the successful invasion and capture of Baghdad, Colonel Paul Hughes was charged by Garner with establishing contact with officers of the Iraqi Army in order to identify soldiers and units who could be recalled to provide security and help with the reconstruction effort. Although the CENTCOM psychological operations campaign had "instructed army units...to stay in formation and surrender," upon arriving "coalition forces found that rather than standing aside from the fight as intact units, the Iraqi army was nowhere to be seen."³⁷ Despite this unexpected complication, however, "before going on leave" to attend his daughter's college graduation, Col. Paul Hughes "had been meeting every day with a group of Iraqi generals, and with them had developed a list of 125,000 former Iraqi soldiers" to recall to duty.³⁸

During the same period Hughes was making his push, Lieutenant General David McKiernan "and a select few senior U.S. officers met at the Abu Ghraib palace with Faris Naima, a former Iraqi officer, in a meeting coordinated by the CIA." Naima had "been the commander of al-Bakr Military College, a training ground for Iraq's top officers." Speaking fluent English, he stressed the overwhelming importance of security for Iraq in the post-Saddam landscape. In order to provide it, he "urged the Americans to establish three Iraqi military divisions to be deployed in northern, central, and southern Iraq," with an army unit "stationed in each major town to back up the police."³⁹

New Leader, New Vision

By the time of President Bush's "Mission Accomplished" speech, it was clear in Washington that Garner was soon to be

replaced, having lost the support of several administration officials, including Cheney, whose office never saw him “as part of the team.” The specific incident that precipitated his downfall may have come at a press conference Garner held a few days before leaving for Kuwait. “When a reporter asked whether he would hand power over to Chalabi and the INC, Garner replied, ‘I don’t intend to empower the INC. I don’t have a candidate. The best man will rise.’” That night, Garner “received several agitated calls from [Undersecretary] Feith,” who said, “You’ve damaged the INC, you’ve caused Ahmad embarrassment.”

Garner replied, “Hey, goddamnit, then what you need to do, Doug, is have a little press conference in the morning and say, ‘We’re firing Garner because he embarrassed Ahmad Chalabi.’”⁴⁰

The vice president “moved quickly to bring in what he hoped would be a stronger figure.” After Wolfowitz’s bid to be considered was denied, Scooter Libby, Cheney’s chief of staff, contacted Bremer to inform him that he was being considered for the position.⁴¹

Following his appointment, Bremer and his deputy Walt Slocombe began preparing at the Pentagon. During this period according to Bremer, Slocombe began meeting with Wolfowitz to discuss “the policy implications of Saddam’s army having melted away.”⁴² “According to Bremer, Rumsfeld approved an outline of the plans [to disband] on May 9,” and later approved a final plan on May 19. “After the draft order was reviewed by Feith on May 22, Bremer sent President Bush a three page letter which was an update on the conditions in Iraq. Near the end of the letter he mentioned that he was going to dissolve ‘Saddam’s military and intelligence structures.’”⁴³

During a National Security Council meeting from which he was participating from Baghdad via video that day, Bremer claims to have informed the president of his plan. According to National Security Adviser Condoleezza Rice, however, several participants in the meeting recall the order being “brought up only in general terms during a discussion of de-Ba’athification. It was certainly not a request for permission to issue the order.” She further notes that the “decision to dissolve [the army] explicitly ran counter to the earlier plans to retain as many as three to five divisions to form the nucleus of a new Iraqi Army.” She adds finally, “I was surprised when I read in the newspaper on May 24 that the Iraqi military had been dissolved by order of the U.S. envoy.”⁴⁴

The fact that Rice has admitted to being surprised by the order leads to one of the most fundamental questions of this whole episode: did President Bush know of and approve the order before it was issued?

For his part, Bremer has been consistent in his insistence that President Bush gave his approval for disbanding the Iraqi Army during the disputed videoconference. Powell contradicts his contention, however:

*When we went in, we had a plan, which the president approved. We would not break up and disband the Iraqi Army. We would use the reconstituted Army with purged leadership to help us secure and maintain order throughout the country... The plan the president had approved was not implemented... These actions surprised the president, National Security Adviser Condi Rice, and me, but once they had been set in motion, the president felt he had to support Secretary Rumsfeld and Ambassador Bremer.*⁴⁵

Seconding both Rice’s and Powell’s characterization of the unusual process that led to the order is Franklin C. Miller, a decorated member of the NSC staff, who recalls:

*Anyone who is experienced in the ways of Washington knows the difference between an open, transparent policy process and slamming something through the system... The most portentous decision of the occupation, disbanding the Iraqi army, was carried out stealthily and without giving the president’s principal advisors an opportunity to consider it and give the president their views.*⁴⁶

Their characterizations are further supported by several curious incidents that took place in Iraq during this period. Among them was Colonel Greg Gardner’s attempt—at the behest of Bremer’s deputy Walt Slocombe—to obtain McKiernan’s opinion of the order “the day before it was issued.” While Gardner claims “that a member of McKiernan’s staff told him over the phone that McKiernan accepted the policy decision,” McKiernan himself says, “I never saw that order and never concurred. That is absolutely false.”⁴⁷ Lieutenant General J.D. Thurman, who served as McKiernan’s top operations officer at the time, concurs, adding: “We did not get a chance to make a comment. Not sure they wanted to hear what we had to say.”⁴⁸

Similarly, Colonel Michael Barron, who was a “senior advisor to Garner, participated in the heated discussions between Garner and Bremer over the CPA orders 1 and 2.” As someone who “had been involved in the Army planning for the post-military victory administration of Iraq,” Barron knew that “the assumption all along had been that reestablishing the Iraqi Army was essential for both security and economic reasons.” Despite that, however, Bremer “arrogantly dismissed the concerns of military leaders and continued to insist that in making the decisions he was following the president’s orders and that they were final.”⁴⁹

Left in the Dark

Given the importance of CPA Order No. 2 for America’s involvement in Iraq, it is worth considering in full just how many key members of the military and President Bush’s cabinet—some of whom were already referenced—were left in the dark when news broke of Bremer’s decision.

- Lieutenant General David McKiernan, “the senior American military commander at the time...neither reviewed nor backed the decree.”⁵⁰

- General Richard B. Myers, Chairman of the Joint Chiefs of Staff, “said the issue was never debated by the chiefs. ‘I don’t recall having a robust debate about this issue, and I would have recalled this.’”⁵¹
- General Peter Pace, Vice Chairman of the Joints Chiefs of Staff: “We were not asked for a recommendation or for advice.”⁵²
- Major General Victor Renuart—director of operations at Central Command—remarked, “We were surprised at the dissolution of the army.” Colonel Kevin Benson, another CENT-COM planner, added, “We expected to be able to recall the Iraqi army. Once CPA took the decision to disband the Iraqi army and start again, our assumptions for the plan became invalid.”⁵³
- CIA Director George Tenet writes in his memoir that, “without any formal discussion or debate back in Washington—at least any that included me or my top deputies—Bremer, on May 23, ordered the dissolution of the Iraqi Army.”⁵⁴
- Deputy National Security Advisor Stephen Hadley “first learned of the orders on de-Baathification and disbanding the military as Bremer announced them to Iraq and the world. They hadn’t been touched by the formal interagency process... [Condoleeza] Rice also had not been consulted.”⁵⁵
- Secretary of State Colin Powell “was not informed about it, much less consulted.” When he asked National Security Advisor Condoleeza Rice about it later, she replied, “I was surprised too, but it is a decision that has been made and the president is standing behind Jerry’s decision. Jerry is the guy on the ground.”⁵⁶

The consequences would be immediate, and catastrophic.

Fallout

According to Agoglia, Bremer’s order was the moment when “we snatched defeat from the jaws of victory and created an insurgency.” Colonel R. Alan King—civil affairs officer for the 3rd Infantry Division—concur, recalling that, “When Bremer did that, the insurgency went crazy... When they disbanded the military, and announced we were occupiers – that was it. Every moderate, every person that had leaned toward us, was furious. One Iraqi who had saved my life in an ambush said to me, ‘I can’t be your friend anymore.’”⁵⁷

Furious protests from ex-soldiers and other Iraqis began immediately once the order was announced, with protestors offering chilling warnings of violence to come.

A New York Times report from May 25 on a “demonstration in Basra by dismissed Iraqi soldiers quoted one former Iraqi tank driver as saying, ‘The U.S. planes dropped the papers telling us to stay in our homes... They said our families would be fine.’” Another soldier at the protest remarked, “We have guns at home.

If they don’t pay us, if they make our children suffer, they’ll hear from us.”⁵⁸

“On June 2, about 1,000 ex-soldiers gathered in Baghdad outside the gates of the CPA headquarters to protest the army’s disbanding.” Said one protestor, “The entire Iraqi people is a time bomb that will blow up in the Americans’ face if they don’t end their occupation.” Said another, a former military officer, “All of us will become suicide bombers. I will turn my six daughters into bombs to kill the Americans.”⁵⁹

“On June 18 an estimated two thousand Iraqi soldiers gathered outside the Green Zone to denounce the dissolution decision.” Some were carrying signs that read “PLEASE KEEP YOUR PROMISES” – an obvious reference to the psychological operations campaign waged by the United States before the war to convince Iraqi soldiers to give up before fighting started on the promise that they would be brought back. One of the demonstrators vowed, “We will take up arms. We are all very well-trained soldiers and we are armed. We will start ambushes, bombings and even suicide bombings. We will not let the Americans rule us in such a humiliating way.”⁶⁰

The most haunting story of the missed opportunity presented by the order was the case of Lieutenant Colonel Jeff Ingram, a battalion commander for the 2/70 Armor Battalion out of Fort Riley. Upon arriving in the Iraqi capital, Ingram found himself “responsible for securing a section of the city that far exceeded his grasp.” Luckily, however, he “was meeting daily with an Iraqi major general who told [him] that he had an entire division of some 10,000 troops standing by to provide security on the streets. All [he] had to do was pay them.”⁶¹

After Ingram “informed the Iraqi general of [CPA Order No. 2], the astonished Iraqi officer informed him, ‘This means that I will be fighting you tomorrow.’” After “acknowledging the possibility” of impending conflict, “the two officers gravely saluted each other. Although [Ingram’s] sector had been quiet to that point, attacks on his troops began the next morning.”⁶²

For Hughes, the man who had spent more time on recalling the Iraqi Army than any other government official, what made the situation all the more disheartening was the amount of leverage that had been squandered. “I had them by their balls,” he recalled. “They would have stood on their head in the Tigris River for me as long as we were dealing fairly with each other. It was just so tragic, so needless.”⁶³

As Agoglia put it, “We wanted to rapidly call the soldiers back, get them on our side, and then sort out who could and could not be trusted.” In doing so, “The generals wanted to use the Iraqi forces as a means to generate the troop levels that would be needed to guard the borders and establish a military presence throughout the country.” Instead the plan subsequently offered by Slocombe in the wake of the order called for building a “New Iraqi Corps” battalion by battalion, a process that would take “two years to train and equip a three-division force.”

“It would have been a lot faster than building one battalion at a time,” remarked Agoglia on the original plan. “And we wanted to send a psychological message that they were going to be part of the new Iraq, to prevent them from turning against us.”⁶⁴

After violent protests in Mosul following the order left 16 of his soldiers wounded, Lieutenant General David Petraeus—then commander of the 101st Airborne Division—told Slocombe at a change-of-command ceremony “that the decision to leave the Iraqi soldiers without a livelihood had put American lives at risk.”⁶⁵

As David L. Phillips writes in describing Petraeus’ lament, “Not only did the decree turn 400,000 former soldiers against the U.S.-led coalition, but if you consider that an average Iraqi family includes six persons, the decision directly affected the lives of 2.4 million people, or roughly 10 percent of Iraq’s population.”⁶⁶

Planting the Seeds of Al-Qaeda in Iraq (and ISIS)

“If Abu Musab al-Zarqawi could have dictated a U.S. strategy for Iraq that suited his own designs for building a terrorist network, he could have hardly come up with one that surpassed what the Americans themselves put in place over the spring and summer of 2003,” writes Joby Warrick in his acclaimed book, *Black Flags: The Rise of ISIS*.⁶⁷

Following the de-Ba’athification order and the order disbanding the Iraqi Army, Sunnis across Iraq found themselves newly powerless, and enraged. As Warrick writes, “It was in this reordered Iraq that Zarqawi would find both freedom to maneuver and powerful allies willing and able to support his cause. Captains and sergeants who once served Saddam Hussein now enlisted in Zarqawi’s army, and some rose to leadership positions. Others offered safe houses, intelligence, cash, and weapons, including, investigators later concluded, the aerial munitions and artillery shells that provided the explosives...for Zarqawi’s biggest car bombs.”⁶⁸

Warrick’s assessment is shared by noted counterinsurgency expert (Army, Ret.) John Nagl, who writes, “A large group of organized, angry men who knew how to use weapons that were lying literally loose in the unsecured ammunition bunkers of what had fairly recently been the world’s fourth-largest army now had no job and no prospects...and they took their anger out on the people they believed responsible for this disaster.”⁶⁹

And thus was an insurgency born.

Identifying the (Elusive) Culprit

As both Fred Kaplan of *Slate Magazine* and James P. Pfiffner of George Mason University have cited, there exist several compelling facts that point to the vice president’s office as the

originator of the order within the U.S. government. First is a quote from Tenet’s memoir in which he writes that when Garner and the CIA station chief in Baghdad confronted Bremer about the order to outline their objections, Bremer told Garner “that he could raise the issue with the secretary of defense if he wanted to, but that this was a done deal and a decision made at a level ‘above Rumsfeld’s pay grade.’”⁷⁰ Considering that only the president and vice president stood above Rumsfeld in terms of “pay-grade,” as well as that President Bush admitted to being surprised by the decision in an aforementioned interview with Robert Draper of *The New York Times*, these statements seem to clearly implicate the vice president. Second, Cheney’s office was known as “one of the most leak-proof offices in Washington.” Given the intense interest this subject has generated over the past 12 years, it seems likely that “had the order originated somewhere else, that fact would have been leaked by now.”⁷¹

It is in considering the motive of the vice president and those in his office that the picture emerges clearest, however. As Tenet writes in his memoir, for those admirers of Chalabi in the vice president’s office and in the Department of Defense, maintaining “control” of the Iraqi political process so as to promote his interests was of paramount importance. He writes:

*Hovering over this entire process was...Ahmad Chalabi. Time and again, during the months leading up to the invasion and for months thereafter, the representatives of the vice president and Pentagon officials would introduce ideas that were thinly veiled efforts to put Chalabi in charge of post-invasion Iraq.*⁷²

General Anthony Zinni (USMC, Ret.), the former CENTCOM commander, is even more explicit, believing that “de-Baathification and the dissolution of the army were [done] at Chalabi’s insistence...he saw the army as a threat to him. If the army stayed intact, he wouldn’t have control of the security forces.”⁷³

The most convincing evidence of all, however, comes from Jack O’Connell, a former CIA officer and long-time confidant of King Hussein of Jordan, who ruled his country for nearly a half century from 1952-1999:

*To pave the way for him to head the Iraqi government, he said he had to destroy the existing Iraqi power structure, which consisted of Saddam, the Iraqi Army, and the Ba’ath Party. He was instrumental in eliminating all three. At a meeting in London, on his way back to Iraq, he told us he was going back to ensure the army would be disbanded. Our question was whether this would eliminate the only force capable of maintaining law and order. He explained that the army had already disbanded itself. The soldiers had all gone home and their barracks had been looted...Disbanding the army was, later, generally recognized as a major blunder, but there were no apologies from Chalabi. It was part of his agenda.*⁷⁴

As Michael Gordon and Bernard Trainor write in *Cobra II*, Chalabi’s intent resulted from his rivalry with fellow exile leader Iyad Allawi. Allawi, who “had contacts among the Baathists

and the Iraqi military...calculated that they could be a part of his power base.” This led him to push for “limited de-Baathification and an appeal for Iraqis affiliated with the old order to switch sides.” Chalabi, meanwhile, “had pushed for a strong de-Baathification policy and for disbanding the Iraqi military, figuring this would not only remove the vestiges of Saddam’s regime but also undermine his rival.”⁷⁵

The Cheney Modus Operandi

In addition to the substantial evidence already cited, the manner in which the decision to disband the Iraqi Army was carried out is yet another powerful indicator of Vice President Cheney’s involvement.

An earlier example of a similar bypass of the interagency review process came on November 13, 2001, during a weekly lunch Cheney shared with President Bush. On this occasion, Cheney had brought an order his lawyer David Addington “had drafted in strict secrecy.” The order concerned a fundamental question the United States was facing in the newly launched War On Terror: “What should they do with a captured fighter from al-Qaeda or the Taliban?”⁷⁶

In order to consider the question, Powell had earlier “appointed Pierre Prosper, ambassador-at-large for war crimes, to lead a working group.” Prosper’s working group would eventually include “representatives from Justice, Defense, and the Joint Chiefs of Staff.” Tellingly, however, not one member of Cheney’s staff showed up.⁷⁷

Instead, Addington “typed out an order that stripped foreign terrorist suspects of access to any court – civilian or military, domestic or foreign.” The terrorists “would be tried, if at all, in closed ‘military commissions,’ modeled on the ones Franklin Roosevelt set up for Nazi saboteurs in World War II.”⁷⁸

After dismissing the concerns of Attorney General John Ashcroft, Cheney brought Addington’s order to the aforementioned lunch with President Bush, at which he secured his approval to move forward.⁷⁹ Neither Powell nor Rice were made aware of the order being brought to the president. When both officials found out they were left furious, leaving Powell to ask the same question many did in the wake of the disbanding of the Iraqi Army, “What the hell just happened?”⁸⁰

In considering the Vice President’s pattern of behavior, the similarities between the events described and the events surrounding the disbanding of the Iraqi Army are striking:

One NSC lawyer had been shown drafts of the policies to de-Baathify Iraq and disband the military—but that was only to give a legal opinion. The policy-makers never saw the drafts, never had a chance to say whether they thought they were good ideas or even to point out that they were radical departures from what had earlier been planned and briefed to the president... General Myers, the principal

*military adviser to Bush, Rumsfeld and the NSC, wasn’t even consulted on the disbanding of the Iraqi military. It was presented as a fait accompli.*⁸¹

Clearly for the vice president, the interagency process was not a tool to help the president avoid making mistakes, but a hindrance to achieving his policy goals. And would thus be avoided at all costs.

What About Rumsfeld?

Defining the role that Rumsfeld played in the disbanding of the Iraqi Army has proven quite difficult, even for Rumsfeld himself.

On April 24, 2006, Rumsfeld wrote a memo to several Pentagon officials with the subject, “Disbanding the Iraq Army.” The memo was in regard to a recent story in the New York Times entitled, “Criticizing an Agent of Change as Failing to Adapt.” In it, Rumsfeld wrote that a particular statement in the story “does not ring true to me.” The statement in question read, “The decision of L. Paul Bremer III, the head of the occupation authority, to disband the Iraq army only added to the deficit of forces. Mr. Rumsfeld approved that decision. Neither Condoleezza Rice, then the national security adviser, nor the Joint Chiefs were consulted about the decision.”⁸²

To which Rumsfeld responded, “It is difficult for me to imagine that I approved something of this nature without the kind of interaction we normally have around here that involves the Chairman or the Vice Chairman.” He further asked that a review be conducted of “briefing and meeting notes from that period to refresh all our memories on the way this issue may have been discussed with Jerry Bremer.”⁸³

The stunning reply from Assistant Secretary of Defense Peter W. Rodman came a month later. It is recreated fully herein:

You asked that we review relevant briefing and meeting notes from 2003 to determine how the decision to disband the Iraqi army was made and approved.

The relevant material is attached.

Our review yielded the following chronology:

21 Jan 2003: OSD Policy/Joint Staff produced a draft brief “Rebuilding the Iraqi Military: recommending the elimination of organizations tainted with crimes of the Ba’ath regime (e.g. the security services) but retaining the regular army.

3 Mar 2003: OSD Policy produced a “Draft Agreement between USG and Iraqi Interim Authority” which called for disestablishing the Ba’ath party and the military and security agencies tainted with the crimes of the Ba’ath regime (but retaining the regular army).

7 Mar 2003: The Joint Staff produced an updated version to the 21 Jan 2003 brief. The new brief, renamed “Reshaping the Iraqi Military, recommended that, following combat operations, Iraq’s regular army should “maintain its current status in assembly areas and permanent garrison.”

7 May 2003: OSD Policy produced a draft De-Ba’athification policy guidance paper recommending dismantling Saddam-era organizations tainted with the crimes of the Ba’ath regime (not including disbanding the regular army).

– Note: The above papers and briefings were discussed at daily Executive Steering Group meetings held in the Pentagon and chaired by the NSC staff

19 May 2003: Ambassador Bremer informed you that he intended to issue an order dissolving Iraqi military and security organizations (including the regular army) as part of the de’Ba’athification effort.

23 May 2003: Ambassador Bremer signed CPA order #2 officially dissolving key Iraqi security ministries including the regular army.

– Note: Ambassador Bremer did not vet/coordinate CPA order #2 or the decision to disband the army with OSD Policy or the Joint Staff⁸⁴

Rumsfeld’s documented confusion over CPA Order No. 2 raises fascinating questions about the Bush administration during this period. The first and most obvious of which is, if Rumsfeld approved the order—as this memo apparently confirms—why order the review in the first place? Especially when doing so provides a rather humiliating rejoinder for historians to marvel over in perpetuity?

Although definitive conclusions at this point remain impossible to draw, what is clear, as Rice writes in her memoir, are these facts: “Don [Rumsfeld]...received a memorandum [on disbanding]...on May 19, but he did not bring it to my attention or that of the president.” Furthermore, she concluded, “something was wrong when a decision of that magnitude could be made without Washington’s full and considered deliberation.”⁸⁵

As is now clear, such laments were common in the Bush administration on matters of significance to Cheney.

The Rise of ISIS

From an American perspective, of all the numerous and often excruciating ironies that have resulted from the invasion of Iraq, few can compare to the legacy of disbanding the Iraqi Army given the chaos caused by the rise of ISIS. As a Washington Post article describes, “The original sin...was the disbanding of the Iraqi army following the U.S. invasion in 2003, which toppled the country’s long-ruling dictator Saddam Hussein... Military officers belonging to Hussein’s Ba’ath party — a nominally secular institution — eventually emerged as the key figures running the Islamic State.”⁸⁶

“Under its leader, Iraqi jihadi Abu Bakr al-Baghdadi,” describes another article from the Associated Press, “the Islamic State group’s top command is dominated by former officers from Saddam’s military and intelligence agencies, according to senior Iraqi officers on the front lines of the fight against the group.”⁸⁷

In describing the importance of their presence to the terrorist group, the article continues, “The experience they bring is a major reason for the group’s victories in overrunning large parts of Iraq and Syria. The officers gave IS the organization and discipline it needed to weld together jihadi fighters drawn from across the globe, integrating terror tactics like suicide bombings with military operations. They have been put in charge of intelligence-gathering, spying on the Iraqi forces as well as maintaining and upgrading weapons and trying to develop a chemical weapons program.”⁸⁸

In May 2015, the Iraqi Army suffered a stunning defeat against the Islamic State in Ramadi, the capital of Anbar Province. “The unexpected collapse of Iraqi forces in Ramadi, including elite counterterrorism troops from Iraq’s Golden Division, suggests that the Iraqi forces may be weaker than many in the U.S. government had thought,” reported a story from The Washington Post the following day, leading Secretary of Defense Ashton Carter to remark, “The Iraqi forces just showed no will to fight...They were not outnumbered, but in fact, they vastly outnumbered the opposing force. And yet they failed to fight.”⁸⁹ To which Chairman of the Joint Chiefs of Staff Martin Dempsey added, “The Iraqi Army ‘was not driven out of Ramadi. They drove out of Ramadi.’”⁹⁰

In explaining the defeat, and in particular the disparity between the quality of commanders for the Iraqi Army and the Islamic State, a writer for Foreign Policy remarked, “The Islamic State’s advantages on the battlefield represent a long-term unintended byproduct of the U.S. decision to disband the Iraqi army in 2003 after Saddam Hussein’s regime melted away. A generation of Sunni military expertise was essentially turned out onto the streets and eventually lost to the insurgency.”⁹¹

Conclusion

One Iraqi colonel told me, you know, our planning before the war was that we assumed that you guys couldn’t take casualties, and that was obviously wrong. I looked at him and said, ‘What makes you think that was wrong?’ He goes, ‘Well, if you didn’t want to take casualties, you would have never made that decision about the army.’
– Charles Duelfer, U.S. weapons inspector⁹²

I think that’s the lesson learned, is that you have to have great intelligence, and I think that the decision...to disband the Iraqi military rather than to co-opt it to create a secure Iraq first for its citizens was a mistake. And that’s the lesson. The lesson is you can—American power, military power—is still the greatest in the world. And we can have the desired effect militarily, but we need to think through

how we create security and peace afterwards, or we have chaos.

– Jeb Bush, former Republican Presidential candidate⁹³

Although there exists no “smoking gun” evidence to connect Vice President Cheney to CPA Order No. 2, in this examination we have been able to build upon and advance the narrative first offered by Kaplan and later Pfiffner identifying the vice president as the culprit, through several avenues. The first is by establishing that the vice president—in concert with allies like Wolfowitz and Feith—sought over a period of several years to use his influence and knowledge of the policy-making process to advance the interests of Chalabi as the new leader of Iraq; the second, by establishing that Chalabi sought to have the Iraqi Army disbanded so as to eliminate a possible competing center of power in the Iraqi post-Hussein landscape; and lastly, by establishing that the decision making process surrounding CPA Order No. 2 bears remarkable similarities to other vice presidential interventions during the Bush Administration that involved a bypass of the normal interagency process.

Furthermore, subsequent events have demonstrated that the decision to disband the Iraqi Army was one of the most damaging decisions of the entire war, as it contravened the U.S. military’s strategy regarding post-war stability operations, which led to a security vacuum that allowed for and even hastened the rise of the insurgency, and has left a crippled Iraqi military in its wake.

That the mystery surrounding the whole episode has been maintained for this long is a reflection ultimately of just how devastating it is for the legacies of all those involved – a legacy that unfortunately continues to worsen with time.

Mr. Michael Wackenreuter is a candidate for a MALD at The Fletcher School of Law and Diplomacy. Prior to his graduate studies, he served in the United States Army as an Infantryman for three and half years, and in that capacity deployed to Afghanistan in 2012. Mr. Wackenreuter received his undergraduate degree from Tulane University.

1. The Principals Committee of the National Security Council serves as the senior interagency forum for consideration of policy issues affecting national security. It is composed of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Chief of Staff to the President, and the Assistant to the President for National Security Affairs (who serves as chair). The purpose of the particular meeting referenced was to decide on several matters related to postwar Iraq, including De-Ba’athification and the Iraqi Army. “National Security Presidential Directive 1: Organization of the National Security System.” Federation of American Scientists, February 13, 2001.

2. Kaplan, Fred. “Who Disbanded the Iraqi Army?” *Slate Magazine*, September, 7, 2007.

3. Gordon, Michael R. “Fateful Choice on Iraq Army Bypassed Debate.” *The New York Times*, March 17, 2008.

4. Andrews, Edmund L. “Envoy’s Letters Counters Bush on Dismantling of Iraqi Army.” *The New York Times*, September 3, 2007.

5. Andrews, Edmund L. “Envoy’s Letters Counters Bush on Dismantling of Iraqi Army.” *The New York Times*, September 3, 2007.

6. Chandrasekaran, Rajiv. *Imperial Life in the Emerald City: Inside Iraq’s Green Zone*. New York: Alfred A. Knopf, 2006, 33.

7. Chandrasekaran, 34.

8. Packer, George. *The Assassins’ Gate: America in Iraq*. New York: Farrar, Straus and Giroux, 2005, 122.

9. Chandrasekaran, 34-35.

10. Fallows, James. “Blind Into Baghdad.” *The Atlantic*, January 28, 2004.

11. Ibid.

12. Fallows, James. “Blind Into Baghdad.” *The Atlantic*, January 28, 2004.

13. Woodward, *State of Denial*. New York: Simon & Schuster, 2006, 133.

14. Ibid, 133.

15. Ibid, 137.

16. Bremer, L. Paul, and Malcolm McConnell. *My Year in Iraq: The Struggle to Build a Future of Hope*. New York: Simon & Schuster, 2006, 10.

17. Gordon, Michael R. “Fateful Choice on Iraq Army Bypassed Debate.” *The New York Times*, March 17, 2008.

18. DeYoung, Karen. *Soldier: The Life of Colin Powell*. New York: Knopf, 2006, 397.

19. Mayer, Jane. “The Manipulator.” *The New Yorker*, June 7, 2004.

20. Ibid.

21. Bonin, Richard. *Arrows of the Night: Ahmad Chalabi’s Long Journey to Triumph in Iraq*. New York: Doubleday, 2011, 177.

22. Isikoff, Michael, and David Corn. *Hubris: The Inside Story of Spin, Scandal, and the Selling of the Iraq War*. New York: Crown Publishers, 2006, 50; See Mayer also.

23. Bonin, 193; See Mayer also.

24. Bonin, 193.
25. Ibid, 195.
26. Ibid, 198.
27. Bonin, 200.
28. Ibid.
29. Frum, David. "The Speechwriter: Inside the Bush Administration During the Iraq War." *Newsweek*, March 19, 2013.
30. Weisberg, Jacob. *The Bush Tragedy*. New York: Random House, 2008, 204.
31. Hersh, Seymour. "The Stovepipe." *The New Yorker*. October 27, 2003.
32. Chandrasekaran, 36.
33. Chandrasekaran, 37.
34. Phillips, David L. *Losing Iraq: Inside the Postwar Reconstruction Fiasco*. New York: Westview Press, 2005, 131.
35. Ibid.
36. Packer, 147.
37. Bensahel, Nora. *After Saddam: Prewar Planning and the Occupation of Iraq*. Santa Monica, CA: Rand Arroyo Center, 2008, 121.
38. Ricks, Thomas E. *Fiasco: The American Military Adventure in Iraq*. New York: Penguin Press, 2006, 161.
39. Gordon, Michael R., and Bernard E. Trainor. *Cobra II: The inside Story of the Invasion and Occupation of Iraq*. New York: Pantheon Books, 2006, 552.
40. Packer, 128.
41. Baker, Peter. *Days of Fire: Bush and Cheney in the White House*. Anchor, 2014, 270-271.
42. Bremer, L. Paul, and Malcolm McConnell. *My Year in Iraq: The Struggle to Build a Future of Hope*. New York: Simon & Schuster, 2006, 54.
43. Pfiffner, James. "US Blunders in Iraq: De-Baathification and Disband the Army." *Intelligence and National Security* 25, no. 1 (2010): 76-85. Accessed May 14, 2015. Doi:February 2010.
44. Rice, Condoleezza. *No Higher Honor: A Memoir of My Years in Washington*. New York: Crown Publishers, 2011, 238.
45. Powell, Colin. "Colin Powell on the Bush Administration's Iraq War Mistakes." *Newsweek*, May 13, 2012.
46. Gordon, Michael R. "Fateful Choice on Iraq Army Bypassed Debate." *The New York Times*, March 17, 2008.
47. Pfiffner, 76-85.
48. Gordon, Michael R. "Fateful Choice on Iraq Army Bypassed Debate." *The New York Times*, March 17, 2008.
49. Pfiffner, 76-85.
50. Gordon, Michael R. "Fateful Choice on Iraq Army Bypassed Debate." *The New York Times*, March 17, 2008.
51. Ibid.
52. Pfiffner, 76-85.
53. Ricks, 163.
54. Tenet, George, and Bill Harlow. *At the Center of the Storm: My Years at the CIA*. New York: HarperCollins Publishers, 2007, 429.
55. Woodward, Bob. *State of Denial*. New York: Simon & Schuster, 2006, 197.
56. Pfiffner, 76-85.
57. Ricks, 163-164.
58. Tenet and Harlow, 429.
59. Woodward, 211.
60. Ricks, 164.
61. Nagl, John A. *Knife Fights: A Memoir of Modern War in Theory and Practice*, 64-65.
62. Nagl, 64-65.
63. Woodward, 207.
64. Gordon and Trainor, 484-485.
65. Ibid, 556.
66. Phillips, David L. *Losing Iraq: Inside the Postwar Reconstruction Fiasco*. New York: Westview Press, 2005, 152.
67. Warrick, Joby. *Black Flags: The Rise of ISIS*. New York: Doubleday, 117.

68. Warrick, 119.
69. Nagl, 64-65.
70. Tenet and Harlow, 429.
71. Kaplan, Fred. "Who Disbanded the Iraqi Army?" *Slate Magazine*, September 7, 2007.
72. Tenet and Harlow, 419.
73. Ricks, 162.
74. O'Connell, Jack and Vernon Loeb. *King's Counsel: A Memoir of War, Espionage, and Diplomacy in the Middle East*. New York: W.W. Norton, 2011, 224.
75. Gordon and Trainor, 476.
76. Gellman, Bart. *Angler: The Cheney Vice Presidency*. Penguin Books, 2008, 162.
77. Ibid.
78. Gellman, 163.
79. Ibid, 166.
80. Ibid, 168.
81. Woodward, 197-198.
82. "The Rumsfeld Papers." The Rumsfeld Papers. Accessed September 9, 2015. <http://papers.rumsfeld.com/>.
83. Ibid.
84. "The Rumsfeld Papers." The Rumsfeld Papers. Accessed September 9, 2015. <http://papers.rumsfeld.com/>.
85. Rice, 238.
86. Tharoor, Ishaan. "Why the Iraqi Army Keeps Failing." *The Washington Post*, May 19, 2015. Accessed October 12, 2015.
87. Hendawi, Hamza, and Qassim Abdul-Zahra. "ISIS Top Brass is Iraqi Army's Former Best and Brightest." *Haaretz*, August 8, 2015. Accessed October 12, 2015.
88. Ibid.
89. Jaffe, Greg, and Loveday Morris. "Defense Secretary Carter: Iraqis Lack 'Will to Fight' to Defeat Islamic State." *The Washington Post*, May 24, 2014. Accessed August 19, 2015.
90. McLeary, Paul. "Why Are the Islamic State's Commanders So Much Better Than the Iraqi Army's?" *Foreign Policy*, May 26, 2015.
91. Ibid.
92. Murphy, Cullen, and Todd S. Purdum. "An Oral History of the Bush White House." *Vanity Fair*, February 1, 2009.
93. O'Keefe Ed. "Jeb Bush: When It Comes to Talk About Iraq, His Last Name 'Doesn't Matter.'" *The Washington Post*, August 14, 2015.

Development Challenges and Tools in Conflict Environments

by Todd Diamond



USAID relief commodities at the Port-au-Prince airport are readied for distribution to the local populace, January 17, 2010, (Candice Villarreal / U.S. Navy).

For at least a generation, conflict resolution has been predominantly the domain of international development practitioners seeking to use their skills and tools to avert war and reduce the suffering of civilian populations. More recently, the U.S. military added similar exercises to its planning efforts, primarily for the strategic purpose of reducing its own potential future deployments around the world. Working occasionally in parallel and at other times seemingly at cross-purposes, the military, donors and non-governmental organizations have begrudgingly come to accept that in any given crisis each can play a role. The nature and extent of each actor's role depends on the circumstances and the severity of the situation.

As the military concludes the longest war in U.S. history in Afghanistan, and as pressure mounts to intervene in additional

conflicts in the Middle East, it is worth examining what role development can play in reducing that pressure, who should be responsible for providing that assistance, and what form it should take. In most cases, whether in a pre-conflict environment, an active conflict, or a post-conflict phase, development agencies and their partners are well placed to provide warnings and respond to civilian crises, though not without coordinating and collaborating in certain instances with their military counterparts.

Pre-conflict: Development as a Prevention Tool

In 2006, at a time when the U.S. military was engaged in full-scale combat in both Afghanistan and Iraq, General Charles F.

Wald, Deputy Commander of the U.S. European Command, wrote an article entitled “The Phase Zero Campaign.” The goal of the campaign, which focused on “terrorism’s long-term, underlying conditions,” was to “prevent conflicts from developing in the first place.”¹¹ In coordination with other U.S. government agencies – the article mentions the Department of State and the Department of Energy, but not the U.S. Agency for International Development (USAID) – the preventative approach taken by the military focused on greater military training with partner nations and “hearts and minds” communications initiatives to counter extremist ideology.

Around the same time, however, several current and former military and defense officials, including then-Secretary of Defense Robert Gates and retired General and former Secretary of State General Colin Powell, questioned whether the military should be engaging in traditional civilian-led activities. Recommendations on how to limit military involvement in a pre-conflict phase included guidance that “Phase Zero should only be applied in a linear, progressive manner once a military campaign commences.”¹²

Similarly, the development community expressed alarm at interventions that would be “likely to reflect U.S. military priorities and give short shrift to broader political and developmental considerations” because “DoD’s primary concern in weak and failing states is to build the capacity of local security forces. Whether those forces are under effective and accountable civilian control is a secondary concern.”¹³ Another reason for discomfort with military involvement in the pre-conflict phase is that the development community has its own experience with early warning mechanisms for identifying potential conflict.

Conflict early warning systems in the development field date at least to the early 1990s, when the end of the Cold War led to relatively unpredictable outbreaks of violence, most notably the 1994 Rwandan Genocide. In late 2013, USAID released a report entitled “Advancing Early Warning of Mass Atrocities against Civilians” in which it laid out a spectrum of approaches for responding to threats depending on how quickly they were likely to occur. Traditionally, more immediate threats – ranging from imminent to the next 12 months – have been addressed by the security sector. The report identifies hot spots, potential triggers, and troop deployments in the context of ongoing armed conflicts as a way to head off attacks against civilians or respond to such conflicts should there be an outbreak of violence.

For longer-term assessments on the likelihood of atrocities being committed against populations within a few years, the report identified statistical models, largely comprised of societal indicators (e.g., wealth, ethnic divisions, regime type), as key tools in helping to determine the likelihood of future violence. Over the years, many quantitative and qualitative analyses have been done to incorporate lessons learned from previous events and support forward-looking policy and planning. However, in addition to this empirical work, development practitioners are also well placed to interpret warning signals on the ground and provide

solutions.

In Colombia, for example, despite a pronounced reduction in insurgent violence in recent years, many communities still suffer from severe insecurity, massive displacement, and weak government institutions. To help combat these threats and warn against recurrences of instability, USAID has worked with indigenous leaders to create community-run self-protection networks. These networks allow indigenous communities to police their own populations, while also integrating with government administered protection mechanisms. More broadly, USAID has also worked to promote a culture of respect for human rights through its support of the Colombian government’s National Ombudsman’s Early Warning System. The Ombudsman’s office established and operates a mobile registration unit for victims of human rights violations.

In addition to the formal mechanisms being employed to provide redress in Colombia, the development community’s insight into the pulse of communities as tensions rise is a valuable first step in heading off potential conflict. In Lebanon, the legacy of the 15-year civil war and decades of community-level violence has honed a sense of when and how political, religious, or social divisions can flare into full scale conflict. Using their experience on the ground, local development practitioners were among the first to realize that the influx of Syrian refugees into Lebanon could enflame social tensions within host communities. To help promote social cohesion and mitigate these tensions, in 2013 USAID project teams in the northern border area and in the Beqaa Valley supported local civil society activities that enabled people to come together to challenge the rhetoric of sectarianism and violence. Project beneficiaries – Shiites, Sunnis, and Christians – worked together to reclaim public space and collectively identify community priorities and solutions to address the economic and resource strain brought on by the crisis.

Food insecurity is another heavily debated conflict trigger. Regardless of whether a lack of food supply is considered a cause or a consequence of conflict, there is no doubt that heeding warning signs of impending food shortages can help mitigate impending humanitarian crises that can be exploited by extremist groups and lead to further violence. While military units frequently lead or heavily support civilian-led efforts to deliver humanitarian assistance, USAID’s Famine Early Warning Systems Network (FEWS NET) starts at an earlier phase in an impending crisis. FEWS NET manages food security information networks and builds local capacity for information generation and dissemination in more than 30 countries. These reports assist decision makers and planners in preventing hunger-related deaths, mitigating food insecurity, and strengthening livelihoods. FEWS NET also contributes to conflict early warning by providing local communities with objective and usable data on livelihood changes that can contribute to alleviating conflict-promoting factors such as resource scarcities and lost employment opportunities.

Post-Conflict: Tools for Reconciliation and/or the Prevention of Reemergence of Violence

The interventions previously mentioned come with the advantage of being employed without “boots on the ground.” As I describe below, avoiding active military involvement in a conflict is not always realistic or even desirable. But in an effort to avoid the outbreak of violence, as well as in the aftermath of a conflict that does not include external military intervention, having a civilian face on international intervention can buy a lot of credibility among local actors on all sides. This credibility offers an opportunity to provide immediate transition assistance as well as longer term support to improving livelihoods.

Following a controversial presidential election in Kenya in December 2007, the announcement that President Mwai Kibaki had won a second term resulted in violence that left 1,300 people dead and more than 350,000 displaced.⁴ Protests that were brutally suppressed by security forces largely divided the country along ethnic lines. Once the rival political parties reached a peace accord and a power sharing agreement in February 2008, USAID’s Office of Transition Initiatives (OTI) helped reduce the political tension by mobilizing citizens’ participation around a national identity and political party platforms, rather than ethnic identities. In response to similar violence following the November 2010 presidential elections in the Ivory Coast, OTI helped strengthen public confidence in the recovery process by enhancing the capacity of community leaders and the responsiveness of governing institutions to address grievances.

Not to be mistaken with full-fledged conflict-resolution initiatives, the goals of these interventions were limited by design and meant to capitalize on windows of opportunity to address targeted political transition and stabilization needs, thus setting the stage for long-term development. An advantage of using these mechanisms in such a politically charged environment is that the U.S. government can provide on the ground assistance without bringing attention to its role in encouraging a locally driven solution. Unlike more high profile development assistance, the U.S. government in these cases often avoids taking credit or making its presence known when trying to help shore up such fragile social or political dynamics. This contrasts with even the most benign humanitarian assistance provided by the U.S. military, which usually comes with a bigger footprint and armed soldiers in uniform, making their presence unmistakable. Of course, there are also circumstances when sending the message that the United States is providing assistance in a post-conflict environment can be advantageous in realizing the benefits of peace and improving livelihoods.

Furthermore, the success of post-conflict security operations often necessitates concurrent development-focused programs. Because violence makes news, most of the attention that follows a conflict focuses on security sector training and equipping. National armies and local police usually get new uniforms, new gear, and a steady paycheck. But civilians living in the communities that violence has torn apart often complain more about cor-

rupt or non-existent governance than about threats to physical safety. Establishing accountable municipal and national governments that provide essential constituent services and increased economic opportunity is an effective way to combat the reemergence of more extremist ideologies aimed at maintaining enflamed levels of unrest. For this reason, sustained development programs in post-conflict countries often pair service delivery programs with economic growth programs. Across the Balkans and the Middle East, projects focused on public sector budgeting, financial management, and administering capital improvement projects have been able to demonstrate visible results to constituents who now advocate on their own behalf and expect results from elected officials.

Although the aforementioned examples are not easy to implement, and their success is far from guaranteed, they are meaningful steps that can be taken to mitigate the risk factors that lead to conflict or reduce the likelihood of conflict reemerging. However, in the most egregious cases, they cannot prevent conflict.

Conflict-Affected Development: Pockets of Opportunity in an Ongoing Conflict

When fighting starts, a kinetic response is often the only way to create enough space to implement civilian-led programs. The challenge to getting this right, however, is knowing how to correctly sequence the military and civilian interventions. During the wars in Afghanistan and Iraq, victory on the battlefield and a full spectrum of political and economic development programs were pursued simultaneously. Throughout both countries, civilian and military teams worked side by side in units known as Provincial Reconstruction Teams (PRTs).

As I have written elsewhere,⁵ while PRTs made sense logistically and practically — by providing development practitioners with access to areas accessible only by the military — the ambiguity between military and civilian engagement was problematic on multiple levels. At the local level, the trust that development professionals gained by working with Afghan and Iraqi professionals and beneficiaries eroded when they were seen as an extension of the military. Likewise, including development success as a factor in “winning the war” created an impression among congressional overseers that military success and development could be measured according to the same standards. Development results are never as clearly defined in time or scope as outcomes on the battlefield.

For the military, removing the enemy and providing a secure environment that enables a provincial government to deliver basic services represents a short-term win that elicits further funding to replicate that success elsewhere. Economic growth and accountable governance, however, cannot be measured in terms of immediate impact. Development assistance in Afghanistan has created numerous jobs⁶ and has trained Afghan farmers how to vaccinate livestock and strengthen local agricultural value chains

across the country.⁷ This assistance also helped facilitate the 2011 Afghanistan Pakistan Transit Trade Agreement.⁸ While the effects of these activities on gross domestic product might not yet be apparent, these projects are helping to increase household incomes in real terms.⁹

As for the development of accountable governments, despite heavy fighting across southern Afghanistan in 2011, multiple municipalities, supported with international assistance, introduced integrated financial management systems that transparently managed revenue collection, budgeting, expenditures, and automated payrolls. Many of these municipalities also established advisory boards and citizen service desks to increase the visibility, demand, and accountability for public services. In Kabul, the public began buying into the value of gas taxes and vehicle registration fees. There, and in other cities, municipal governments were able to use increased revenue from fees to improve solid waste management and other services. Similar efforts in the Iraqi province of Diyala, which is equally divided among Shiites, Sunnis, and Kurds, led to approved budgets and provincial capital improvement plans that have given residents a belief in the possibility of credible governance in the face of the brutal campaign being waged by the Islamic State in neighboring provinces.¹⁰

These modest steps would have been much harder to achieve without a military presence providing support. The consequence of trying to introduce a similar approach without military support has played out in Libya in recent months, where expatriate civilians have been forced to withdraw to neighboring countries for security reasons. In Syria, the United States is trying to provide assistance to local councils in regions of the country controlled by the moderate opposition, but in some cases schools are getting bombed before the assistance can reach them.

Policy Recommendations

Civilians and soldiers will inevitably continue to co-mingle in euphemistically named battle spaces for the foreseeable future. The point here is not to advocate for, or against, military intervention, nor to argue whether civilian or military imperatives should take the lead. The point is to recognize when and where civilians are better placed to provide meaningful development assistance and when a focus on stability operations or security sector reform should take precedence. Often this distinction depends on the nature of the threat. Whether in a pre-conflict phase or in the aftermath of war, in many fragile states a harbinger for further violence is just as likely to be a dramatic increase in the price of fuel or staple food products as it is increased troop movements. Recognizing this distinction enables policy planners to call on the most appropriate tools to help defuse the crisis. Once the fighting starts, however, development practitioners must realize that pursuing initiatives intended to improve war-torn livelihoods can make them party to the conflict, and as such a military solution may be required to achieve well-meaning outcomes that have a lasting impact.

The leverage that non-military actors bring to the exercise of national power was recognized in 2010 with the release of the first Quadrennial Diplomacy and Development Review, which states at the outset that, “to advance American security, prosperity, and values and to lead other nations in solving shared problems in the 21st century, we must lead through civilian power.”¹¹ In an era of constant, but usually non-existential irregular threats, unpredictability will largely be the rule. At the same time, with its experience operating in many of the recent conflict-affected environments, the development community has become well versed in the type of scenario planning that military planners are accustomed to undertaking. The trends on both sides indicate that going forward each can learn a lot from the other’s scenarios.

Todd Diamond is a development analyst and practitioner with more than 20 years of experience reporting on post-conflict emergencies and implementing assistance projects for USAID, the State Department, and the Defense Department. He has worked in Afghanistan, the Middle East, the Balkans, Latin America, and Africa, and he has also briefed U.S. Army units on implementing development assistance in conflict-affected environments.

1. General Charles F. Wald, “New Thinking at USEUCOM: The Phase Zero Campaign,” *Joint Force Quarterly* no. 43, (4th quarter 2006): 72-76.
2. Colonel Thomas M. Rhatican, “Redefining Security Cooperation: New Limits on Phase Zero and ‘Shaping,’” in *Short of General War: Perspectives on the Use of Military Power in the 21st Century*, edited by Dr. Harry R Yarger, pp. 111-130.
3. “Phase Zero: The Pentagon’s latest big idea.” *Center for Global Development*, July 20, 2007, <http://www.cgdev.org/blog/phase-zero-pentagons-latest-big-idea> (accessed April 24, 2015).
4. “Post Election Violence Humanitarian Assistance.” *Kenya Red Cross*, https://kenyaredcross.org/index.php?option=com_content&view=article&id=284&Itemid=156 (accessed April 24, 2015).
5. Todd Diamond, “Do the Military and Development Mix?” *Foreign Policy in Focus*, March 18, 2010, http://fpif.org/do_the_military_and_development_mix/ (accessed April 24, 2015).
6. Individual donor projects report on job creation among the outcomes measured under their grants or contracts. See “Agriculture, Rural Investment and Enterprise Strengthening (ARIES) Program in Afghanistan Final Report, September 30, 2006-December 31, 2009,” *United States Agency for International Development*, 7, http://pdf.usaid.gov/pdf_docs/pdacq819.pdf (accessed April 24, 2015).
7. See “Final Performance Evaluation Accelerating Sustainable Agriculture Program (ASAP),” *United States Agency for*

International Development, 150, http://pdf.usaid.gov/pdf_docs/pdact903.pdf (accessed April 24, 2015).

8. See “Afghanistan Pakistan Transit Trade Agreement (APT-TA),” *Afghanistan Customs Department*, October 28, 2010, <http://customs.mof.gov.af/en/page/1007/1009/1010> (accessed April 24, 2015).

For USAID assistance in negotiating the agreement, see “Trade and Accession Facilitation for Afghanistan (TAFa),” *United States Agency for International Development*, September 30, 2013, <http://www.usaid.gov/news-information/fact-sheets/trade-and-accession-facilitation-afghanistan-tafa> (accessed April 24, 2015).

9. For example, see “Evaluation Report for Alternative Development Program (ADP) Eastern Region by USAID in the Islamic Republic of Afghanistan,” *United States Agency for International Development*, 38-43, http://pdf.usaid.gov/pdf_docs/pdacs234.pdf (accessed April 24, 2015).

10. The examples from Kabul and Diyala come from author’s interview with a senior personnel advisor to the Commanding General, Command Joint Task Force - 82/101, Kabul, Afghanistan, 2007-2008, and senior city management advisor and deputy governance team leader for the U.S. State Department in Diyala, Iraq, 2009-2010. Interview was conducted in February 2014.

11. “Leading Through Civilian Power,” *The First Quadrennial Diplomacy and Development Review*, 1, <http://www.state.gov/documents/organization/153108.pdf> (accessed April 24, 2015).

The Role of Special Operations Forces in a Sustainable U.S. Counterterrorism Strategy

Moving Beyond Kinetic Targeting in the Future Operating Environment

by Anthony Gilgis



Navy SEALs conduct training in a remote area. (U.S. Navy photo/MC2 Martin L. Carey)

Introduction

For the past two decades, the United States military and the national security apparatus have focused their energy and capabilities on confronting Islamic terrorism as a kinetic target. Much of U.S. counterterrorism policy today consists of lethal raids and unmanned aerial vehicle strikes against targeted individuals. The U.S. government has come to rely heavily on the Special Operations Forces (USSOF) in particular for lethal raids, also termed “Direct Action” assaults, one of the ten “Core Activities” that Title X identifies for USSOF. Unfortunately, Direct Action has come to overshadow the broad array of missions that USSOF was originally intended to conduct. Unconventional Warfare, for example, is a core USSOF mission intended to prevent radical ideology from taking root in a society with a range of activities to build local good will towards friendly forces and animosity towards extremists. The U.S. can more effectively incorporate USSOF into a “whole-of-government” approach to counterterrorism by refocusing attention on non-kinetic, coun-

ter-ideology operations.

To move beyond the recognized battlefields of the past decade, U.S. officials must embrace a multidimensional operating environment that requires simultaneous focus along multiple lines of effort. Future warfare will include complex, adaptive systems of ideology, economy, physical infrastructure, governance, and energy — which cannot be defeated through kinetic operations alone. The USSOF will need to transform its operations accordingly.

During the last two decades of the twentieth century, a paradigm shift occurred in the realm of transnational terrorism and how nations responded to it. Shifting away from a focus on political goals, transnational terrorist groups began using religion as a motivating factor — both in their operations and in their recruitment. This new form of terrorism required a shift in response from the international community. It took the West almost a decade to recognize this shift and adjust its response to

the emergent threat. Following 9/11, the United States fully engaged Special Operations Forces and paramilitary elements to actively counter this new religious ideology. SOF and paramilitary units were tasked to conduct raids against members of radical extremist groups. However, after almost 15 years of continuous warfare, the U.S. has arguably experienced limited success with its counterterrorism efforts as groups continue to conduct attacks and grow, gaining notoriety and establishing affiliated movements around the globe. Kinetic actions have created an entire generation of potential radicals who are victims of our counterterrorism “successes.” Populations sensitive to radicalization are also vulnerable to state-level terror in the form of unexpected and unpredictable military strikes. The battle against terrorism to date leaves the question, “As the United States looks to the future operating environment, can the Special Operations community find a more effective method to counter the ideology that creates the modern Islamic terrorist?”

Since 2001, the West has increasingly focused on lethal targeting of individuals within religious-based extremist organizations. This method of conducting kinetic operations — either through direct action assaults by military or paramilitary units, or through the use of missile strikes from aerial platforms — has become the public face of the United States counterterrorism effort. While the United States military has arguably raised man-hunting of individuals from an imprecise task to a methodical science, targeted lethal actions are nonetheless perceived as little more than indiscriminate state-level terror within the populations in which the operations are conducted. Looking to the future operating environment, the current policy of countering terrorist actions with targeted killing is unlikely to sway the underlying ideology in Americans’ favor. As such, it is necessary to develop a sustainable counterterrorism strategy that considers the human domain of local opinion as the future battlefield.

The Special Operations Forces of the U.S. military will play a central role in any long-term strategy to counter violent extremist organizations; they are specifically designed to create a counter-ideology within the scope of unconventional warfare. Before looking at the role of U.S. Special Operation Forces within this emerging strategy, an understanding of the changing nature of warfare within a complex environment is necessary. Moving forward in the concept of developing a long-term counterterrorism strategy beyond the use of kinetic operations, we must understand that Islamic extremism is rooted in an ideology the West has displayed overt ignorance of and has been unprepared to counter. As stated by Patrick Sookhdeo, “Equally damaging has been the desire for a quick-fix and the reluctance to engage in a long-term struggle against the ideological struggle that nourishes and promotes Islamist terrorism.”

Looking to the Future

Guerrilla warfare, in the larger sense...is revolutionary war, engaging a civilian population, or a significant part of such a population,

against the military forces of established or usurpative governmental authority.

-Taber

The evolving nature of warfare throughout history suggests that Islamic extremists, too, will change their approach over time. Understanding how adaptation, co-evolution, change, and the non-linear nature of warfare has manifested itself, it is important to look at the Global Salafi-jihadi movement as it is in the process of shifting from a Guevarist-style kinetic insurgency to a more Maoist-style systemic strategy. The most successful Islamic extremist groups are no longer solely focused on kinetic operations to achieve their goals; rather they have proven an ability to take advantage of vulnerabilities in the local political system and use forms of social engineering to achieve long term goals. Understanding who the adversary is, why they fight, and more significantly how their concept of their warfare will change creates opportunities to successfully engage this ideology. Unconventional warfare tactics, originally designed to affect change within a society, can disrupt the formation of affiliates and acolytes before the virulent ideology can take root within an at-risk population. Moving away from an operational environment dominated by kinetic actions, USSOF are ideally suited to operate “left of the beginning.”

The Future of Warfare is Increasingly Irregular

There are many terms for the nature of non-linear warfare. Irregular Warfare dominates the space as the umbrella term to describe wars and tactics other than regular. Since the Boxer Rebellion at the beginning of the twentieth century, the U.S. military has been consistently engaged in more than 80 irregular conflicts that occur at the sub-state level. This indicates that irregular warfare, in the form of unconventional warfare, insurgency, guerrilla warfare, and modes of warfare yet to be defined are likely to be a dominate form of warfare for generations to come. It is therefore imperative that the various tactics of Irregular Warfare, and their potential impact on U.S. national strategy, be understood.

Even as the gap between developed and under-developed nations continues to widen, technology and economics are creating a tiered system within the ranks of developed countries. Governments are becoming acutely aware of the capability gaps emerging among the great powers. As the gap between the different tiers begins to widen, near-peers and adversaries at both the state and non-state levels will be forced to resort to irregular warfare as a method to express their political will short of engaging in a kinetic war. Recognizing this trend towards asymmetric use of force, it is essential to prepare for Irregular Warfare across the complete spectrum of conflict.

Insurgency as a Form of Warfare

Insurgency is the organized use of subversion and violence to seize,

nullify, or challenge political control of a region.

-U.S. Army FM 3-24

As a result of perceived inequality, sectors of the population become isolated and disenfranchised. Often, insurgencies begin long before they emerge into the public eye with groups establishing clandestine networks and shadow governments in the form of auxiliary and underground support elements. The U.S. Army's joint publication on counterinsurgency indicates that "insurgents challenge government forces only to the extent needed to attain their political aims: their main effort is not just to engage [host nation] military and other security forces, but instead to establish a competing system of control over the population, making it impossible for the government to administer its territory and people." However, this does not take into account governments who abdicate their role in these areas, leaving the population to fend for themselves without support from the central government. It is within these complex environments that insurgencies blossom, radical ideologies thrive, and where USSOF will operate deep into this century.

Insurgencies do not occur in a vacuum — they develop over many years as the direct result of the failure of the central government to provide for swaths of the population. Often faced with expansive ethnic, sectarian, demographic, and economic divides, national governments often struggle to find a balance. Regardless of the relative strength of the central government, its inability to provide stability and security throughout the country classifies it as a weak government.

Countries with weak central governments often exhibit limited control across the entire span of the country, instead seeking to control population centers and critical infrastructure. This is done as a way to consolidate security forces and maximize the number of citizens — in the form of affiliated supporters — they can protect with limited resources. This choice of governance creates vast pockets of under-governed space within their borders where the central government either does not exist, or chooses to not exercise authority. These under-governed territories, found within both the rural and urban environments of a country, become the breeding ground for civil discontent that leads to insurgency, radical ideology, or exploitation by transnational organizations.

The Role of Under-governed Space

While there are many variations of under-governed areas within a country and region, the RAND Corporation was able to identify three general typologies to use as a basis for defining these territories.

- Contested Governance, also referred to as "competing governance," is where a group refuses to acknowledge the legitimacy of the government's rule. In most cases, the groups contesting the state's authority are seeking to establish their own state-like entity.

- Incomplete Governance is when a state seeks to exert authority over its territory but lacks the resources to do so. The legitimate government cannot maintain a competent, qualified presence that is stronger than the sources of violence and order. Other forces, some tribal, some criminal, move in to fill the vacuum that results.
- Abdicated Governance is when the central government abdicates its responsibilities for poor provinces and regions where it concludes that maintaining a presence is not cost effective or where ethnic minorities with whom the government shares little affinity predominate.

These emerging countries typically have weak and corrupt central governments, high unemployment, exorbitant poverty levels, limited internal infrastructure, deep ethnic and religious divisions, and a history of humanitarian issues which make these regions ripe for radicalization. The rise of transnational non-state and sub-state actors will serve to complicate actions throughout the region of under-governed nations. Millenarian groups and illicit organizations will look to these vast under-governed areas to establish operational nodes, communications hubs, and support networks to train the next generation of terrorists. This region of the world will require continual vigilance to maintain security and will occupy the majority of nation-state investment and attention well into the next decade.

Combatting Ideology

In his work on defining a religious-based war, noted Islamic scholar S.K. Malik wrote that "terror is the viable means to conduct war, jihad is the responsibility of both soldiers and civilians." During the last two decades of the twentieth century, a new phenomenon emerged — a global insurgency tied to ideology instead of nationality. This new evolution of the transnational insurgent freed the organization to conduct spectacular attacks outside of the local supporting population. While terrorism has become the overriding focus of our National Security Strategy, it remains only a tactic in the adversary's asymmetric efforts against us.

The commitment to a long-term strategy to combat ideology will force a change in operational outlook for both conventional forces as well as USSOF. As the U.S. and its allies move into the middle of this century under the weight of overburdened economies, legacy geo-political strategies will reemerge alongside existing transnational, non-state threats.

Special Operations Forces will operate within this ill-defined battlefield and must understand that this type of conflict will include new requirements for identification and engagement of the adversary. Within this changing operational landscape, the recognized sovereignty of nations will continually be challenged by the rise of transnational non-state and sub-state organizations, and sympathetic populations connected to each other

through the global conversation.

Political Ideology

Political ideology is typically seen as affecting change within the existing government. At its roots, political ideology is focused locally and does not seek annihilation of the state, but rather the reformation of the state structure, to include a rapid return to international rapprochement. As the nature of warfare changes, or as the adversary adapts and changes, and the lines between political warfare, insurgency and terrorism blur, it remains essential that USSOF continues to operate within the seams of such chaos.

Religious Ideology

Religious ideology emerged following the Iranian Islamic revolution of 1979. Largely based on the writings of Sayyid Qutb, the Ayatollah Ruhollah Khomeini, S.K. Malik, and Abdullah Azzam, what became known as Islamic terrorism evolved from a politically-driven opposition to Western and Israeli occupation into a global effort to defend Muslim lands. The current divide within Islam, centered on the Sunni and Shi'a sects, is likely to expand beyond the Near East, continuing to trigger regional and transnational sectarian conflicts well into this century. It becomes essential to begin looking at these opposing non-state elements in the light of a global influencer — rather than as the adversary itself.

Perhaps the most effective method in both creating and sustaining an organizational goal is to immerse them in a combination of political and religious ideologies.

It is this role which makes transnational terrorism so insidious. Ideology cannot simply be destroyed; in order to effect change at this level requires the repudiation of a belief structure. “A political ideology or a set of religious beliefs readily becomes the source of truth for — and the basis for violent action by — young fanatics. Such principles can be used to transform the true believer into a terrorist and justify the acts of terrorism at the same time.”

This new-breed of extremist leaders has learned to adapt, evolve, and incorporate commercial technologies to recruit, train, and control their networks while also announcing their operations to the world. Leveraging business models and lessons learned from other licit and illicit organizations, many of these twenty-first century terrorist leaders are capable of creating and managing a covert diversified network with multiple simultaneous methods for achieving and reviving long held grievances. It is the apparently random aggregation and disaggregation of groups that complicate identifying the systemic nature of conflict.

Unconventional Warfare...the Role of Special Ops

The battle against Islamic extremism following 9/11 has further justified USSOF operational capabilities and identified the continuing need for the development of a more specialized form of warfare that transcends the spectrum of conflict. USSOF has proven their ability, flexibility, insight, and ingenuity to operate in a complex warfighting domain, employing small unit tactics to achieve relative superiority across the spectrum of conflict.

As the national combatant command for conducting traditional unconventional warfare, the U.S. Special Operations Command has played a primary role in developing the methods and tactics necessary for implementing persistent host-nation engagement to further the nation's strategic and operational objectives. As the world becomes more complex, unconventional warfare operations are becoming an integral part of an overarching strategy transcending traditional military operations and diplomatic actions. This shift of focus will place a greater emphasis on the non-linear, non-kinetic, small-unit missions of the Special Operations core competencies.

The nature of future USSOF missions will call for them to be conducted across the developing world ranging from austere, remote areas into the heart of feral megacities — often beyond the reach of conventional logistics and support infrastructure. The role of USSOF in these areas will be to support the Combatant Commander's and the Ambassador's strategy by providing tailored information campaigns designed to operate within the cognitive battle space, construction projects designed to rehabilitate the local infrastructure, as well as train, advise, assist, and when necessary, accompany host-nation security forces in “a manner similar to the insurgents themselves.” When looking at this type of warfare, it becomes essential to understand the concepts of unconventional warfare, specifically the tactics of Special Warfare.

Unconventional Warfare

Moving deeper into the twenty-first century, unconventional warfare will dominate the international battlefield. As the adversary adapts and employs increasingly non-linear forms of warfare, as the technological gap continues to divide first-world nations from the less developed and under-developed nations, as international borders and geo-strategic boundaries blur, the adversary — in its new and continually changing form — will resort to asymmetric efforts spanning the spectrum of conflict. This effort will range from leveraging proxy elements to conducting military-style operations short of war, to using economic, social, and diplomatic actions to influence and coerce other governments to achieve a desired outcome. This concept of political warfare is defined as “the employment of all the means at a nation's command, short of war, to achieve its national objectives.”

Unconventional Warfare must become a natural extension of foreign policy – something that transcends agency, national,

and geo-strategic boundaries. This special warfare is not merely a tool to be used during a U.S. centric concept of Phase Zero preparation and planning, rather it must be recognized as a strategy for preventing or mitigating the need for any “phase” of operations that they may be in. When properly utilized, unconventional warfare expertise provides the intellectual foundation to help the country-team and host-nation security forces develop strategies to counter enemy insurgent plans and actions before they mature into a local or regional security issue — operations “left of the beginning.”

Special Warfare & Surgical Strike - USSOF Core Competencies

Strikes from the air, or from long distance leave decision making in the hands of the enemy...only on land can you compel an outcome.
-LTG H.R. McMaster, U.S. Army

Special Operations Forces have become masters of non-linear warfare. In pursuing and perfecting small unit operational tactics relying on relative superiority in both direct and indirect methods of warfare, USSOF elements create effects disproportionate to the size unit they employ.

Moving into the middle of the twenty-first century, it will be essential for the U.S. to prevent conflict before it reaches into traditional phases of warfare. This realm of pre-conflict and the actions taken during this period are identified as special warfare. After thirteen years of conducting surgical strikes in support of the counter-terrorism effort, the U.S. concept of unconventional warfare has become very tactical, narrow and limited in focus. As the mission moves from reactionary to preventative, USSOF must adjust its ability to conduct a holistic and effective unconventional warfare campaign in support of a national strategy.

Special Warfare

Special warfare is the future of USSOF and is defined as “the execution of activities that involve a combination of lethal and non-lethal actions taken by specially trained and educated forces that have a deep understanding of cultures and foreign language, proficiency in small-unit tactics, subversion, sabotage and the ability to build and fight alongside indigenous combat formations in a permissive, uncertain, or hostile environment.”

The role of Army Special Operations Forces becomes most effective when employed within the gap that exists between the conventional combined arms maneuver and that of diplomatic action. Special Warfare provides the full range of military options focused on the human domain. In looking to the future, this domain will require continued expertise in asymmetric conflict, a working knowledge and application of human factors, and will increasingly require an understanding and specialization in the cognitive battle space of the adversary.

Surgical Strike

Surgical Strike is defined as “the execution of activities in a precise manner that employ Special Operations Forces in hostile, denied, or politically sensitive environments to seize, destroy, capture, exploit, recover, or damage designated targets, or influence threats.” As the war in Afghanistan, and eventually Iraq, expanded to counter-network operations, the Special Operations Forces refined their ability to conduct surgical strike operations from an art to science. With next-generation terrorist networks beginning to operate beyond the established battlefields of Iraq and Afghanistan, the counter-terrorism forces of the United States find that they are no longer operating under the umbrella of network and technological dominance, and are limited by the scope of the new enemy. This shift in the enemy’s capabilities increases the need for U.S. national security elements to be able to conduct man hunting operations across the spectrum of the operating environment.

To counter and disrupt these networks requires a different methodology — recognizing vulnerable populations early and establishing a network designed to counter virulent ideology before it takes root as well as being prepared to rapidly adjust to permutations in the adversarial network and take immediate action to counter the extremist organization’s emergence. This balance will require extensive lead time to build the necessary nodes and establish trust within the host nation. However, this effort will pay dividends, as violent extremist organizations will find it increasingly difficult to establish their ideology in areas that no longer are susceptible to their ideology.

Persistent Factors Impacting the Future Operating Environment

Today’s non-state actors represent a significant threat to regional security. In many cases, the host nation’s ability to maintain internal stability is hindered by local popular support for the non-state actor. Some government knowingly allow non-state actors to operate from within their borders.

-Marks, Meer, and Nilson

The world has increasingly devolved into a complex environment with multiple aspects of state power and non-state influence combining or becoming interchanged with each other. The inter-related nature of society complicates our efforts to close observed capability gaps within one aspect of society, and may actually create a gap in another. A key trend that reveals this environment is the emergence and proliferation of technology. Technology enables communication to occur at an exponential rate and on a global scale, linking disparate communities into a common international conversation while exposing populations to how other societies think and act. This connectivity increases individual empowerment and erodes the centrality of the state, openly challenging the traditional Westphalian concept of state sovereignty.

Moving away from the artificial limitations imposed by sovereign borders, extensive pockets of under-governed areas, controlled by non-state and sub-state actors, will transcend recognized international borders and exploit geo-strategic seams. This will place a premium on small, highly mobile forces capable of operating across the spectrum of conflict within these complex environments in support of multiple partner-nations within the region. As these areas fall beyond the abilities of host nation security forces it will become essential to conduct traditional Special Forces missions as well as engaging in special warfare in support of partner-nation elements and U.S. regional strategy. Understanding the impact of complex systems on traditional Special Operations Forces missions will become essential.

Complex Operating Environments

Complex environments will create situations that will challenge existing concepts of warfare. These future environments will encompass social, economic, physical, and virtual aspects that must be accounted for in both preparation and sanctioned operational authorities.

- **Social:** This challenge involves the close groupings of different ethnic, sectarian, or socio-economic populations who will have varying degrees of tolerance, communications, and beliefs. Social norms and mores must be understood, and taken into account, when working within these populations whether conducting unilateral operations or creating operational plans alongside host-nation elements.
- **Economic:** In their work on unrestricted warfare, Qiao Liang and Wang Xiangsui assert that future conflict will certainly involve economic actions as offensive tactics for conducting war. Used as an asymmetric weapon, economic attacks can be disruptive to the point of destabilizing an entire nation-state. This method of conflict will be used as both a solitary method as well as in combination with other tactics to conduct irregular warfare. This future battlefield will be both ubiquitous as well as ambiguous.
- **Physical:** The physical environment is the easiest to recognize and prepare for. However, it is essential to anticipate this environment in order to create systems and concepts of operation which will be effective across a diverse physical and ethnic landscape. Due to different operational lenses, the operational requirements within the physical environment will vary between maneuver elements and SOF units. The complex physical environment will require U.S. elements to be prepared to conduct the full range of diplomatic and military options in areas of dense megacities and austere hinterlands with minimal adjustments to authorities, equipment, and training.
- **Virtual:** Perhaps the most insidious and pervasive of the future operating environments, the virtual world, creates is-

sues which span the whole of government ability to react and protect against potential nefarious actors and actions. While considered outside the traditional operating environment, the virtual environment enables illicit networks to organize, plan, train, and recruit without relying on face-to-face encounters. As any conflict in this environment will occur at the speed of processing, the ability for leaders to employ considered analysis and long development cycles, in the midst of the conflict, will be virtually eliminated. Therefore, relationships and authorities must be in place before a conflict occurs in order to create space for the decision-makers. Additionally, this environment is also the most ambiguous as actions within and emanating from this realm are not entirely clear as to what constitutes an act of war.

Warfare in any of these environments proves difficult in the modern age. As each will, with varying degrees, aggregate into one complex environment, there will be significant challenges for how USSOF approaches their missions. Moving forward into the middle of this century, it can be anticipated that irregular warfare will take place in each of these environments, simultaneously, and emerge with little warning as unrestricted warfare. While the sophistication of the adversary will determine how much impact will be felt in some of these environments, the United States must be prepared to operate in degraded conditions across the entire spectrum of the complex operating environment.

Complex Adaptive Systems

As the capabilities gap increases between the developed and emerging world nations, the distance between them will mark the limitation of conventional influence. Across the developing world, complex adaptive systems will emerge in the gap to challenge local governance and regional stability. Complex adaptive systems are organizations where the individual components and relationships between those elements can “change due to continuous adaptations of disparate parts, which on their own produce certain system-wide behaviors in order to cope.” Complex adaptive systems, as an adversary, will require a force that is capable of recognizing the amorphous threat and be agile enough to operate within the same decision-making cycle as the adversarial leadership.

As violent sub-systems, and the adversaries found within them, adapt and become comfortable in their milieu, they will develop the ability to skillfully adapt to variances within their environment. This ability to implement systemic change along the breadth of their network makes these groups incredibly lethal. Elements within a complex adaptive system constantly make assessments of a given situation to determine “the correct action to take in the future based on past experience.” Understanding that complex networks can be manipulated and affected will present disruption opportunities. However, it is important to understand that this method of influence requires persistent

presence and extensive lead-time, as well as a consistent, coherent strategy for network disruption. This method of manipulating complex adaptive systems is only effective if the emerging system — and the conditions under which it formed — are understood and recognized before the network becomes a regional problem.

The Impact of Globalization

The phenomenon of globalization is increasingly driving the responsibility for national decisions further down into the population. The growing influence of sub-state and non-state groups is a clear indicator of the leadership void created by this shift in national decision-making strategy. As these sub-state groups gain support and recognition, some of them will transform into transnational armed groups. These groups will rapidly emerge from a localized domestic law-enforcement challenge into a legitimate regional or strategic security threat with little-to-no warning.

Globalization has increased the organizational effectiveness, lethality, and ability for these groups to transcend traditional Westphalian borders and truly operate on a global scale. This emergent threat will require a highly mobile, scalable force with long dwell periods and pre-existing authorities, capable of recognizing and disrupting these groups before they reach breakout capability.

Time as a Limiting Factor

A natural by-product of the move towards globalization is that the world is becoming more complex. Historically, international relations—to include war—were conducted between nation-states. Diplomacy, strategies, and even specific tactics were designed to confront rational actors who represented relatively large populations. Often correspondence between belligerents was measured in months, allowing times for considered decisions. The shift towards globalization has introduced new actors and technologies into the calculus which has simultaneously reduced the decision cycle to minutes and will eventually eliminate time as a factor in making decisions. Therefore it becomes essential to recognize this limitation and plan for it by building artificial time into the decision-making process and understand the need to create “space” in the cycle through pre-positioned authorities and approvals to the lowest possible operational levels.

Conclusion

For the past two decades, the U.S. military and the national security apparatus has focused its energy and capabilities on confronting Islamic terrorism as a kinetic target. The non-linear nature of warfare suggests that terrorism will evolve and incorporate tactics which will target systems across the spectrum of

national power. In looking at unrestricted warfare, operations against these systems will transform how USSOF operates — no longer focusing on short-term gains, but seeking a long-term strategy which deliberately targets the adversary’s ideology and influence.

Understanding who the adversary is, why they fight, and more significantly how the concept of their warfare will change, creates opportunities to engage this ideology. As the adversary adapts and employs increasingly non-linear forms of warfare, as the technological gap continues to divide first-world nations from the less developed and under-developed nations, as international borders and geo-strategic boundaries blur, the adversary will resort to asymmetric efforts spanning the spectrum of conflict. Unconventional warfare therefore must become a natural extension of foreign policy — something that transcends agency, national, and geo-strategic boundaries.

Unconventional warfare tactics can disrupt the formation of affiliates and acolytes before the virulent ideology can take root within an at-risk population. Moving away from an operational environment dominated by kinetic actions, USSOF are ideally suited to operate as an integral aspect of a sustainable counter-terrorism strategy which incorporates a unified, whole of government, approach.

Mr. Anthony Gilgis has served within the National Intelligence Community for 26 years with 16 years directly supporting Special Operations. He earned his MA in Diplomacy from Norwich University in 2015 with a focus on international-terrorism. Having conducted deployments in support strategic objectives and tactical operations around the globe, Mr. Gilgis has translated this experience into a subject matter expertise of the special operations community and the intelligence support required for these unique missions.

1. Sookhdeo, Patrick. “The West, Islam, and the Counter-Ideological War.” In *Fighting the Ideological War: Winning Strategies from Communism to Islamism*, by Katharine C. Gorka and Patrick Sookhdeo, 15-44. McLean: The Westminster Institute, 2012.
2. White, Jeffrey B. “A Different Kind of Threat: Some Thoughts on Irregular Warfare.” *Irregular Warfare* 51-59.
3. Barnett, Thomas P.M. *The Pentagon’s New Map: War and Peace in the Twenty-first Century*. New York: Berkley Books, 2005.
4. U.S. Army Special Operations Command. ARSOF 2022. Ft. Bragg: U.S. Army Special Operations Command, 2012.
5. Rabasa, Angel, et al. *Ungoverned Territories: Understanding and Reducing Terrorism Risks*. Santa Monica: RAND Corporation, 2007.
6. Gorka, Sebastian. “The Enemy’s Threat Doctrine.” MISOC

Effects Group, September 04, 2013.

7. White, Jonathan R. *Terrorism: An Introduction*. Belmont: Wadsworth Publishing, 1998.

8. Flynn, Michael T. "Sandals and Robes to Business Suits and Gulf Streams: Warfare in the 21st Century." *Small Wars Journal*, 2011: 1-7.

9. Maxwell, David. *Unconventional Warfare and Counter-Unconventional Warfare*. Washington: Georgetown University, 2014.

10. Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

11. Ibid.

12. U.S. Army Special Operations Command. *ARSOF 2022*. Ft. Bragg: U.S. Army Special Operations Command, 2012.

13. Ibid.

14. Barnett, Thomas P. M. *The Pentagon's New Map : War and Peace in the Twenty-first Century*. New York: Berkley Books, 2005.

15. Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

16. Ibid.

17. Glenn, Kevin B., *Complex Targeting: A Complexity-based Theory of Targeting and its Application to Radical Islamic Terrorism*. Maxwell: School of Advanced Airpower Studies, 2002.

18. Ibid.

Conflict in Cyberspace: How International Legal Norms Can Reduce Military Escalation in Cyberspace

by Nikolas Ott

The Current Discussion

Cyberspace is an increasingly important operational environment for surveillance, espionage, military conflict, and beyond. Offensive military operations in cyberspace especially pose a new challenge for the applicability and enforcement of public international law. Since 2013 the United Nations has acknowledged that conflict in cyberspace is a serious concern for the international community.¹ States agree that cooperation is essential to reduce risk and enhance security within cyberspace.² Given this commitment, it is fair to say that states believe that further escalation in cyberspace can be prevented through the implementation of international regimes,³ treaties,⁴ or agreements.⁵ However, when it comes to military activities, few states are currently willing or able to engage in comprehensive negotiations on treaties governing military use of cyberspace.⁶

Below the threshold of international treaties, there are norms, which have the potential to be codified or implemented through practice. The same applies to confidence-building measures (CBMs) as means to further promote this dialogue. Many international institutions are facilitating such talks at this stage.⁷ However, most of these talks are focused on law enforcement cooperation against organized cyber-crime rather than military activities in cyberspace.⁸

During the latest round of consultations of the United Nations Group of Governmental Experts on Cybersecurity (UN GGE), the group hardly addressed military activities as relevant to their discussion of norms and principles in cyberspace. Instead, in their July 2015 report to the UN General Assembly, the relevant section focused on critical infrastructure and Information and Communications Technology (ICTs).⁹

While the UN GGE reports from 2013 and 2015 demonstrate that there is a general agreement that existing international laws — such as the laws of armed conflict — do indeed apply to cyberspace, the actual scope of their application remains contested.¹⁰ Some analysts argue that the latest UN GGE report

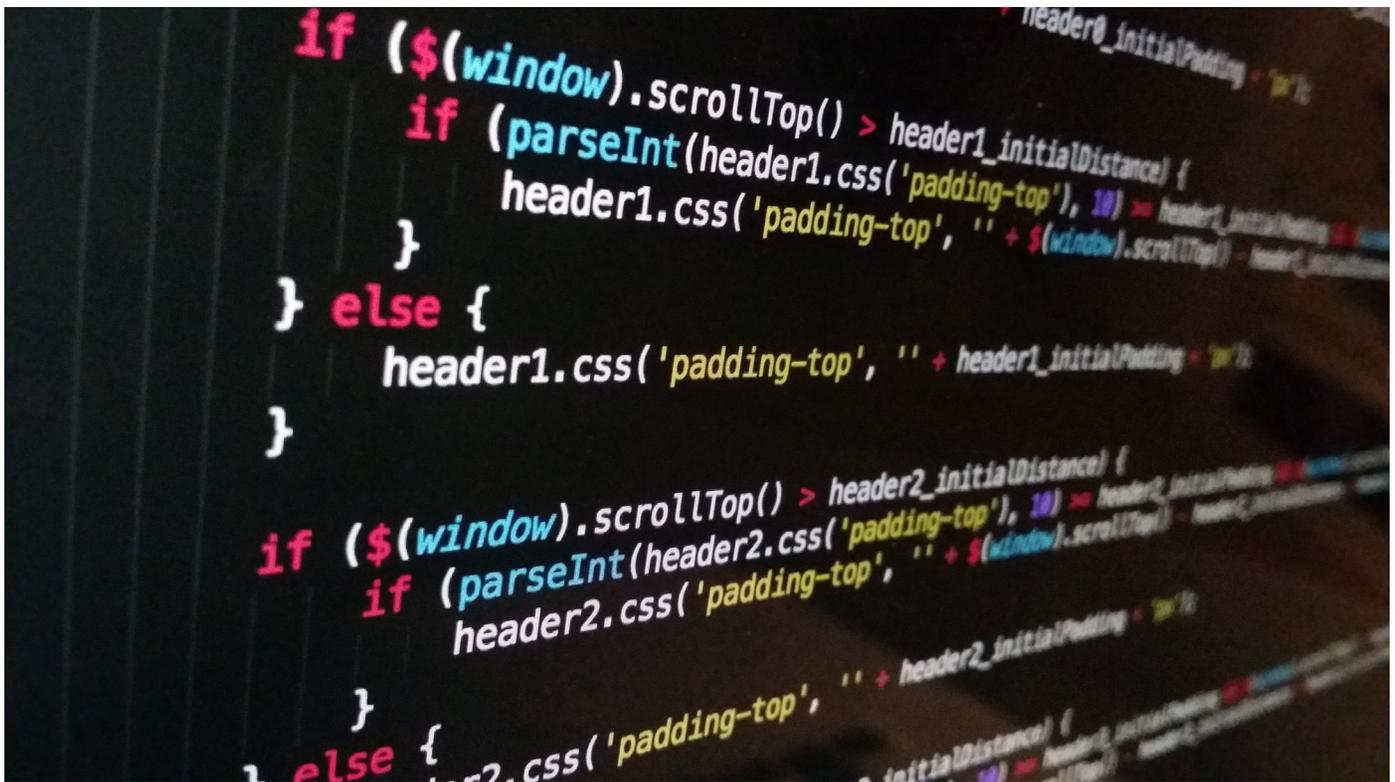
made some important steps in clarifying the applicability of the laws of armed conflict in cyberspace.¹¹ Even so, the discussion of a definition of armed attack and the use of force in cyberspace is hardly over.¹²

A dialogue on legal norms is crucial to harmonizing different interpretations among countries, and there are several key developments that try to clarify the scope and extent to which existing international law applies to cyberspace.¹³ However, the current discourse on norms, at least at the UN level, seems to be stagnant.¹⁴ With this stalemate in mind, this essay will examine under what conditions international legal norms and CBMs contribute to the reduction of military escalation within cyberspace and how this development can be facilitated. Given the scope of this paper, the analysis will be limited to the discussion of legal norms surrounding an armed attack and the use of force in cyberspace.

First, this essay will outline several important characteristics of cyberspace that are relevant for any potential methods of implementing international legal norms and CBMs. Second, it will discuss technical considerations with regard to offensive and defensive military activity in cyberspace. Third, it will review the current policy debates surrounding the use of force and armed attacks in cyberspace. Fourth, it will outline present efforts to reduce conflict in cyberspace with a focus on international legal norms and CBMs. Lastly, it will draw conclusions from the technical and policy perspectives and propose potential next steps to bridge the gap between the two.

Important Characteristics of Cyberspace

While some scholars argue that existing frameworks for analyzing the use of force and armed attacks can be applied to cyberspace as well,¹⁵ military action in cyberspace has several unique features that are important to understand when aiming to establish functioning legal norms.



Attribution in cyberspace remains a core challenge. Given the wide variety of options for acting anonymously in cyberspace, guaranteed attribution of every single attack remains technically impossible.¹⁶ The most sophisticated intelligence agencies might be able to identify the computer that was used to create a certain code or to carry out an attack, but this does not mean that they know who was actually using the computer or whether the computer was a means to carry out the attack, while the attack was actually planned somewhere else. In many situations hijacked computers around the world are used to further complicate tracing an attack back to its originator. While some experts argue that attribution in cyberspace is no longer a challenge, it remains unclear about what kind of attribution they are actually referring.¹⁷

Most security experts remain reluctant to say attribution, especially for international legal purposes, has been solved. Given the ongoing evolution of technological capabilities, experts in most cases are able to track a connection to a machine. However, as noted above, connecting this computer to the user is extremely difficult. This problem is oftentimes referred to as the “endpoint security issue,”¹⁸ effectively tying the device to the person is currently almost impossible.

The number of potential actors is significantly higher compared to other domains since the technical threshold for entering cyberspace for offensive purposes is relatively low.¹⁹ The confusion surrounding the origin of the Sony hack reflects this trend. Even weeks after the incidents, security experts were not absolutely sure who was behind the attack.²⁰ The reason for this was the

simplicity and lack of sophistication of the hack. In fact, the attack could have been created easily many by non-state actors. Ultimately, a deep review of the intent of the attackers, combined with additional intelligence was necessary to be able to determine with reasonable confidence that North Korea was behind the attack.²¹

If a few individuals with experience in hacking might be able to conduct operations similar to a highly sophisticated military of an industrialized country,²² then this leads to an erosion of (hard) power that we have not seen in recent decades. The low cost of initiating unsophisticated offensive operations in cyberspace also means that it is easier for unconventional players, oftentimes non-state actors, to enter the stage and further complicate inter-state discussions and negotiations to introduce mechanisms that could reduce conflict in cyberspace. However, experts believe that ordinary hackers are not able to create computer worms like Stuxnet, the advanced malware deployed in an attempt to sabotage Iran’s nuclear facilities.²³ Such sophisticated attacks are generally labeled as “Advanced Persistent Threats” (APT) given the significant amount of human intelligence and information that is required to deploy them.²⁴ These attacks require the attacker not only to create a malicious virus and hack into a network, but also require an intimate knowledge of software bugs, network vulnerabilities, human intelligence, and on-the-ground operations.²⁵

Given the borderless design of cyberspace, the geographical location of an attacker and its target no longer play a major role. Distance used to be an impediment for confrontation. More-

over, one could build walls, fences, or use natural borders such as mountains or water to create distance. In cyberspace, such borders do not exist by design and it is difficult at this stage to artificially create them. In fact, the entire concept of distance becomes obsolete in cyberspace. Once an attacker has access to the victim's network or computer, data extraction, surveillance or even destruction may occur almost instantaneously. It is yet to be seen how this trend will shape future geopolitical strategic thinking. Lastly, incorrect identification of the origin of an attack, commonly referred to as false flag events, is more likely to occur in cyberspace than in traditional military domains.

Technical Considerations on Legal Definitions of Offensive Activity

Based on the previously outlined characteristics of cyberspace, it comes as no surprise technical considerations play an important role in developing and implementing functional norms. It is important to acknowledge there are no absolutes in cybersecurity. There is no absolute security, no absolute attribution, no absolute detection, etc.

When one observes internet traffic, it is impossible to know immediately what a certain package of data may contain. The design of the package itself is neutral. Recent technological advancements such as deep package inspection make it easier to detect known malign internet traffic, but they cannot stop new kinds of attacks. Ultimately, intent is what distinguishes Google's testing of its own networks for vulnerabilities from outside hackers who are stealing from that same network. While Google's employees most likely have good intentions when improving their network defense capabilities, the hacker's intentions could be characterized as malign. Thus, the intent of an action is crucial to determining whether the action is offensive or defensive.

In the case of the United States, legal definitions also have an effect on the cyber-attack threshold analysis. While computer network exploitation (CNE) and computer network attacks (CNA) are technically the same,²⁶ they are treated differently from a legal perspective.²⁷ A perceived CNA might cause a significantly different response from a perceived CNE, though the technical symptoms of both activities look identical. From a technological perspective, there is no such thing as "passive hacking."²⁸ Making such a determination requires knowledge of the actor's intent.

This technical consideration creates huge challenges for the development of legal norms because almost every activity related to cybersecurity could be identified as a potential "dual use" good, depending on the intention of the actor. Moreover, cyber defense experts might not be able to distinguish immediately whether a network intrusion is done to spy on, steal, or destroy data or infrastructure. Any legal norm aimed at reducing conflict in cyberspace will have to acknowledge this reality. The U.S. Department of Commerce's Bureau of Industry and Security's latest legal effort to introduce international regulations on this is-

sue failed due to the ambiguity in the proposed legal language.²⁹

The Use of Force and an Armed Attack in Cyberspace

Scholars and experts continue to discuss what kinds of actions are necessary to constitute a conflict in cyberspace. In fact, there is no universally accepted definition of cyber warfare. Authors such as John Arquilla, Thomas Rid, Peter Singer, and many others have searched for a consensus definition, but so far no definition has been widely endorsed among states.³⁰ The lowest common denominator seems to be that the definition simply depends on the circumstances, the involved actors, the target, the intent, and the scale of the event. So far, scholars argue that we have not yet seen long-term offensive cyber activities, but we have experienced several events in which cyber attacks supplemented kinetic attacks, such as in Georgia in 2008.³¹

Agreeing on a definition for cyber warfare is important because it helps reduce ambiguity and complexities; this evolution can facilitate the reduction of conflict in cyberspace. Using Thomas Rid's narrow interpretation³² of cyber war referring to an active force compelling the enemy to your will plus a political goal or intention,³³ we are not yet living in an environment of cyber war. In fact, the 2015 Worldwide Threat Assessment of the U.S. Intelligence Community came to a similar conclusion. It stated that "... the likelihood of a catastrophic [cyber] attack from any particular actor is remote at this time. ... We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security."³⁴

But even before theorizing on the existence of cyber war, one needs to define what an "armed attack" and the "use of force" in cyberspace actually mean. Several states, international organizations, researchers, and other actors have come up with potential definitions.³⁵ While few states acknowledge this argument, most of them actually follow a very crude logic: an armed attack in cyberspace is when we say it was an armed attack.³⁶ Thus, depending on the actors' perspective, they will either observe or not observe "cyber war." Similar discussions take place around the definition of the "use of force" in cyberspace.³⁷

Generally, the UN Charter, the Laws of Armed Conflict, and subsequent legal interpretations of these documents are considered as foundational legal documents for legal analysis of an armed attack and the use of force in cyberspace. Additionally, customary international law is considered a secondary source for the legal interpretation of state practice. Article 2(4) in the UN Charter prohibits the use of force except in situations of self-defense (Article 49) or through UN Security Council approval under a Chapter VII resolution. Lastly, Article 51 refers to the "inherent right of individual or collective self-defense if an armed attack occurs."³⁸ As mentioned above, the legal discussion about the correct application of these terms for cyberspace is still ongoing.³⁹ This leaves current politicians and policy-makers with a dilemma: How do you act in a situation in which precise

legal definitions have not been generally agreed upon?

Current International Efforts to Reduce Conflict in Cyberspace

Based on the existing international legal framework, the further development of international legal norms requires a multilateral negotiation and development process. CBMs and capacity building can also be implemented on a regional level. Currently, the discussion on the scope of existing legal frameworks largely takes place within the UN GEE and regional organizations. Parallel to that analysis, a discussion on the development of new legal norms for cyberspace, such as the potential international code of conduct for information security, is also taking place within the UN.⁴⁰ CBMs and capacity building are mostly taking place within regional organizations, such as the Organization for Security Cooperation in Europe (OSCE), the Organization for American States (OAS), and the Association of Southeast Asian Nations (ASEAN). The European Union (EU) is also actively engaged in providing capacity building for its member states and its own institutions.

In 2013 the UN GGE published for the first time a consensus report in which it identified three ways to reduce conflict in cyberspace: legal norms, CBMs, and capacity building.⁴¹ While this list contains an implicit hierarchy, all three methods are crucial to improving the effectiveness of any one of them. In fact, as this paper will argue, all three are reinforcing and supporting each other. Since that report, the UN GEE has been trying to identify ways to deal with cybersecurity challenges on an international level. In July 2015, the UN GEE released its latest report proposing additional norms of responsible state behavior and the standing of international law in cyberspace.⁴² However, the new norms and principles of the 2015 report focus on ICTs and nation-states' critical infrastructure.

Sadly, the latest UN GEE report "did not reconcile the ongoing tensions over the scope of state sovereignty with respect to the Internet."⁴³ This challenge remains a core issue that cannot be addressed without extensive and constructive contributions from a variety of nation-states and non-state actors. This growing frustration on the limited power of the UN GEE, which is technically a UN working group that relies on an annual renewal of its mandate, is oftentimes reflected in calls for the establishment of a body with more authority.⁴⁴ However, it seems unlikely that key actors such as the United States, China, and Russia have a particular interest in giving away authority to influence the international agenda on cybersecurity.

Beyond the UN GGE, a variety of actors and institutions have initiated several projects in order to harmonize the different perspectives on military activities in cyberspace. The following pages will provide an overview of these efforts and draw conclusions on the necessary next steps to help codify legal norms for cyberspace, while keeping in mind the technological circumstances within which these legal norms must operate.

Dispute around Legal Norms Governing Use of Force

Norms help enter a new area of activity where existing laws are inapplicable or non-existent. They help pave the way through non-binding principles. Even if they do not give rise to a new law, norms create expectations and foster discussion among actors. In fact, norms shape expectations, which are critical for states to rationally calculate their interests and define behavior. Shared expectations through norms help avoid the cost of conflict, because they reduce friction and create greater predictability, which reduces transaction costs. However, there is no clear-cut hierarchy among the many norms that govern cyber activities; this confusion is why scholars like Joseph Nye refer to this environment as a regime complex.⁴⁵

When it comes to states' efforts to reduce conflict in cyberspace, international legal norms have received considerable attention in recent years. This is particularly true for states that believe in the value and relevance of the current international legal order (ILO). In fact, the international community largely agrees that existing international law applies in cyberspace. However, "the guidelines on how this should be done in practice are only beginning to emerge."⁴⁶ Several key state actors, such as China and Russia, disagree with the Western approach to the ILO and are making efforts to adjust it according to their preferences.⁴⁷ Their efforts to implement an international code of conduct for information security are the most prominent, but not the only example of such efforts.⁴⁸

Under current circumstances, "cybersecurity" and "information security" are the two main themes that are discussed and debated among states. For the United States, cybersecurity largely relates to the "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."⁴⁹

In contrast, China defines information security as an issue that "involves not only the risks arising from the weakness and interconnected nature of the basic information infrastructure, but also the political, economic, military, social, cultural, and numerous other types of problems created by the misuse of information technology. Both of these factors are worthy of concern when studying the issue of information security."⁵⁰ Comparing these two, one notices that while some portions of both themes have overlap, there is considerable disagreement about the very idea of security, let alone about potential definitions of an armed attack and the use of force in cyberspace.

Third parties such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE) are also contributing to this discussion. However, the CCDCoE's Tallinn Manual on the International Law Applicable to Cyber Warfare largely reflects ideas and perceptions of academics from NATO membership

countries.⁵¹ Moreover, the Tallinn Manual's definition and scope is also contested and not accepted by many non-NATO member countries.

Beyond the political disagreements among states, the technical constraints outlined above further complicate the development of effective legal norms. This implication leads to the question of whether the current emphasis on international legal norms is in fact helpful to solve the challenge of conflict in cyberspace. Do international legal norms help prevent, or at least reduce conflict in cyberspace? There is a wide spectrum⁵² of scholarly work on this topic and the key conclusion that can be drawn is that international cooperation is understood to be "essential to reduce risk and enhance security," just as the UN GGE Report stated already in 2013.⁵³ But it remains disputed what kind of cooperation is necessary, which actors will be involved, and how this cooperation can be institutionalized.

The Role of Confidence-Building Measures to Reduce Conflict in Cyberspace

Given the highly political circumstances under which international legal norms are discussed, CBMs are considered to be a good alternative to identify areas of cooperation and reduce mistrust among nation-states. In fact, CBMs between states are generally considered to be "one of the key mechanisms in the international community toolbox aimed at preventing or reducing the risk of a conflict by eliminating the causes of mistrust and miscalculation between states."⁵⁴

Norms reflect values, which are ideas that exist among actors and therefore aim at a certain end state or a goal. On the other hand, CBMs are considered to be means because they provide the process of getting to the end state that norms envision.⁵⁵

Establishing CBMs in cyberspace shares some of the challenges that face the effort to develop norms, including state sovereignty, the non-physical nature of cyberspace, and the significant number of non-state actors. The lack of reasonable attribution in cyberspace makes it difficult to implement CBMs that are based on verification, a common feature among traditional CBMs. These challenges need to be acknowledged by all involved actors before innovative CBMs for cyberspace can be developed.

Once acknowledged, CBMs have several features that cannot be accessed through pure discussions around norms. CBMs help prevent miscalculation, misunderstanding, and escalation between states. They do not require reaching consensus on everything. It is possible to work around the edges of contested issues and gradually move to a more comprehensive agreement. Generally, there are four types of CBMs that are relevant in cyberspace: collaborative, crisis management, restraining activities, and increasing engagement.

CBMs on collaboration are designed to share information, provide transparency, and build trust. They provide a platform for

dealing with the unique challenges of cyberspace. They foster trust by creating channels for communication. Collaborative CBMs also contribute to transparency, accountability, and stability. The OSCE is one of the first international organizations that implemented a first round of collaborative CBMs aimed at information sharing and regular meetings. Proposals for additional CBMs on collaboration include the establishment of a framework for joint investigations, the application of environmental law in cyberspace, and increased compliance policing through best current practices.

CBMs on crisis management are intended to manage tense moments to avoid outbreak of major wars between nation-states. In cyberspace, such efforts would require the inclusion of non-state actors as observers or policing forces. Current practical proposals on crisis management CBMs include the functional alignment of crisis emergency response teams (CERTs) to increase transparency. Actors that share the CERTs with other governments before a crisis hits know immediately whom to reach out to in a tense situation. To further promote stability, some suggest the implementation of a multilateral cyber "hotline," which should also include private and social sector actors to keep them informed about ongoing developments. Lastly, scholars recommend fostering accountability in cyberspace through the establishment of a cyber adjudication and attribution council. Such an international body should be able to investigate and assign responsibility for cyber crises that could spiral into conflict. It could also serve as local arbitration court to avoid conflict. However, the challenges surrounding attribution in the cyber domain loom over the implementation of such a council.

CBMs aimed at increasing engagement with non-state actors are also crucial in cyberspace. Stronger engagement across both sides would create leverage for international technical regimes and help develop norms. This could be done by facilitating existing regimes, such as the Internet Engineering Task Force, Internet Corporation for Assigned Names and Numbers, or the World Wide Web Consortium to work with governments to set norms. Moreover, neutral activists' entanglement and support could be fostered. This would encourage and support security researchers to collaborate across borders and thus increase the discussion and engagement of technical, scientific, and legal experts across the world.

CBMs aimed at restraining activities could help on three levels: increasing stability of the internet backbones and infrastructure by creating target restrictions and neutrality; improving accountability by asking states to declare responsibility for behavior within their territory; and enhancing transparency by joint research on the applicability of international human rights law in cyberspace.

CBMs are not designed to substitute discussions around international legal norms. In fact, the feasibility of CBMs depends on the parallel development of international legal norms. Instead of looking at CBMs as a replacement of legal norms, both should rather be considered as reinforcing methods that help

reduce conflict in cyberspace. Eventually, both paths may lead to the codification of best practices, behavior, and norms within cyberspace.

Ultimately, the main challenge that all of these proposals face is identifying clear and precise language that reflects the complexity of the technical circumstances while still being understandable by policymakers. The OSCE successfully bridged this gap in its first set of CBMs, but it remains the only international body that has made this effort.⁵⁶ Closing this bridge between technology experts, policymakers and lawyers should be at the core of any future CMB process.

Taking Stock and Moving Forward: Bridging the Gap Between Technology and Legal Norms

When considering technological considerations with the legal and political challenges, one quickly notices that the two worlds operate according to very different principles and conditions. Politics and law develop much more slowly than technology. While technological development is driven by the adoption of new features by users, politics is driven by long negotiations and concludes in compromise or agreement. In the case of cyberspace, the technological constraints are significant and pose serious challenges to policy-makers and lawyers. Worse still, in light of recent discussions about separating different parts of the Internet, introducing backdoor access to encryption standards, and forcing companies to store data within certain jurisdictions before being allowed to operate, the gap between what technologists can do and what policy makers think technologists can do seems to be growing. The most relevant example for this paper is the argument from lawyers to establish a framework that distinguishes offensive from defensive cyber operations.⁵⁷

Unfortunately, lawyers dominate the current discussion around legal norms in cyberspace. Only a few technology experts, such as Bruce Schneier, a fellow at the Berkman Center for Internet and Society at Harvard Law School, are engaged in discussions around norms. However, any discussion about legal norms in cyberspace is dependent on the technological environment in which those norms are supposed to be implemented. One good example to highlight this challenge is attribution in cyberspace. Norms in cyberspace only work if the actors believe that they can be accused of doing something wrong which requires attribution. Norms in a world without attribution are much harder to enforce because we tend to enforce norms by assigning responsibility.

Instead, many analysts look at the victims of attacks and draw conclusions about potential attackers through intuitive and non-empirical reasoning. However, given how easy it is to create false flags within cyberspace, this approach has significant limitations. Instead, the most powerful intelligence agencies, such as the NSA, are using a multitude of lawyers to assign attribution. However, such methods do not help create mechanisms for developing legal norms at the international level.

The same problem occurs with efforts to distinguish cyber espionage for intelligence purposes from cyber attacks. The two might look identical to an observer, so conveying intent can make the key difference in determining whether something is an offensive move or an intelligence operation.

These problems are crucial for understanding why it is so difficult to establish trust and confidence within the military sphere of cyberspace. Inspecting each other's military infrastructure, as was common for nuclear facilities during the Cold War, is basically useless because the intent, and not the technological design, of a cyber operation determines whether it is offensive or defensive. This key difference is not yet widely understood. So how do we move forward from here?

While states have managed to bring engineers and lawyers together in the past, the difference here is that states have not yet identified ways to deal with the truly global design of cyberspace.⁵⁸ This has led to a clash of digitalization with pre-existing norms, structures, and laws. Acknowledging this problem is an important step in the right direction. In order to close the gap between technology experts and lawyers, some of the following steps could be initiated.

First, existing international platforms such as the UN GGE need to receive a stronger mandate that is not limited to a yearly renewal through the UN General assembly. The negotiations have reached a level of complexity where internal capacity building, especially on the technological side, is crucial for further discussion. Simultaneously, such a reform should also provide nations with an increasingly large portion of cyberspace users — such as India, Brazil, and China — with more room to express their political, legal, and technological concerns through diplomatic channels.

Second, by providing the government experts with a more sustainable framework, it will also be easier to include non-state actors in the discussion. While the current framework gives some room for their voices, they are not well integrated into discussions. By opening the door to internet businesses (such as internet service providers), technology experts, and other non-state actors, future policy decisions are more likely to be technologically feasible to implement.

Third, once states accept that the inclusion of non-state actors helps reduce conflict potential and increase trust internationally, this process must be accompanied by the establishment of a database with relevant legal and technical terms. A prominent example of this idea is the New America Foundation Global Cyber Definitions Database,⁵⁹ which was supported by the OSCE. Such efforts will increase understanding of different points of view across sectorial and jurisdictional borders. Databases should also help reduce complexity from both the legal and technical sides.

Fourth, a significant increase in capacity building among cur-

rent diplomats and policymakers would help them understand the technological characteristics of cyberspace. The same holds true for information technology experts who lack a legal or policy background. Additionally, by bringing more technical experts from around the world together, a shared understanding of technical terms and knowledge can develop across countries. Such efforts exist within some countries and regions, but need additional support.

Fifth, the issue of how to avoid the disintegration of cyberspace needs more attention. The economic opportunities that a global cyberspace offers cannot be maintained in a segregated cyberspace. By raising awareness of the strong nexus between economic prosperity and cyberspace, future negotiations will generate more responsibility, hopefully furthering an even better understanding of global cyberspace. Increased awareness and contact will also promote interdependence among states in terms of managing the infrastructure and maintenance of cyberspace.

Sixth, by acknowledging the importance of this issue, not just for today but for many generations to come, it is easy to understand why efforts to train future generations of policymakers, lawyers, and technology experts about the interdisciplinary challenges of governing conflict in cyberspace are crucial. Oxford University's Center for Doctoral Training in Cyber Security⁶⁰ and the Scholarship for Service Partnership for Interdisciplinary Research and Education program at New York University Law School⁶¹ are among the first institutional programs of their kind. Hopefully we will see many more in the future.

All of the aforementioned steps would improve the conditions under which international legal norms and CBMs can contribute to the reduction of military escalation within cyberspace. It is now a matter of political will to implement these suggestions and maintain such commitments.

Conclusion

We have reason to worry about military confrontation in cyberspace. Be it in a full-scale cyberwar, or as component of a larger military activity, it seems reasonable to say that the militarization of cyberspace is on the rise. Fortunately, fora like the UN GGE, the OSCE, ASEAN, OAS, the EU, and many others are actively working on reducing conflict and setting limits for military engagement in cyberspace. However, many of these efforts are slow, or have become stuck, given their limited mandate.

Simultaneously, technological developments will continue to outpace policy and legal discussions. It is therefore important for both sides to acknowledge that they are operating in very different environments. This does not mean that either side has to fundamentally change its modus operandi. Instead, the situation highlights the importance of increased exchange of perceptions, ideas, and trends. Given the borderless design of cyberspace, these exchanges should occur on an international level,

facilitated, but not dominated, by states.

There are many possible efforts to bridge the gap between technology experts, lawyers, and policy-makers. Such efforts include expanding the mandate for the UN GGE, reducing the centrality of state governments in negotiating a framework of cyber norms, maintaining a shared database of cross-sectorial knowledge, and connecting the importance of cyberspace with the growth of global economies.

Together these measures would increase awareness of the political, legal, technological, and economic nexus in cyberspace, thus reshaping discussions of state-based military escalation using cyber capabilities. Ultimately, such efforts will foster negotiations on international legal norms and CBMs for reducing military escalation within cyberspace and create conditions in which future dialogue can be more effective, sophisticated and sustainable. Cyberspace has become a fundamental and inextricable realm of governmental activity. Maintaining a stable cyberspace is therefore not simply an interest but a necessity.

Mr. Nikolas Ott is a 2016 MALD graduate of The Fletcher School of Law and Diplomacy. He focused on international law and cybersecurity during his graduate work.

1. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/70/172, July 22, 2015.
2. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/70/172, July 22, 2015; and *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/68/152, June 24, 2013.
3. Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series*, 1, May 20, 2014, <<http://dash.harvard.edu/handle/1/12308565>>.
4. *Proposal for an International Code of Conduct for Information Security*, Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, September 12, 2011.
5. Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *The New York Times*, September 25, 2015, <<http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html>>; and Andrew Roth, "Russia and China Sign Cooperation Pacts," *The New York Times*, May 8, 2015, <<http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html>>.
6. "UN Cybersecurity Report Compromises on Self-Defense

Issue - Russian Official,” *Sputnik International*, August 17, 2015, < <http://sptnkne.ws/AYy>>.

7. United Nations 2015; Decision No. 1106: *Initial Set Of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies*, Organization for Security and Co-operation in Europe Permanent Council, 1, December 3, 2013; and *ARF Work Plan on Security of and in the Use of Information and Communications Technologies*, ASEAN, May 7, 2015.

8. Henry Rõigas and Tomas Minárik, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, NATO Cooperative Cyber Defense Centre of Excellence, August 31, 2015.

9. United Nations 2015; Rõigas and Minárik.

10. Sputnik International.

11. Joseph Marks, “U.N. Body Agrees to U.S. Norms in Cyberspace,” *Politico*, July 9, 2015, <<http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900>>

12. Keir Giles and William Hagestad II, “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English,” 2014 5th International Conference on Cyber Conflict, ed. K. Podins, J. Stinissen, M. Maybaum, 2013.

13. Sean Selin, “Governing Cyberspace: The Need for an International Solution,” *Gonzaga Law Review*, 365, 1996; Tim Maurer, “Cyber Norm Emergence at the United Nations,” Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project, September 2011; Nye 2014; Paul Meyer, “Seizing the Diplomatic Initiative to Control Cyber Conflict,” *The Washington Quarterly*, 38 (2) pp. 47 - 61; and Sean Watts, “Cyber Norm Development and the United States Law of War Manual,” *NATO Cooperative Cyber Defence Centre of Excellence, International Cyber Norms Development*, August 7, 2015.

14. Paul Meyer, “Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace,” *ICT for Peace Foundation*, September 4, 2015, <<http://t.co/ccXFDvPW4O>>.

15. Scott Shackelford, Scott Russell, and Andreas Kuehn, “Unpacking the International Law on Cybersecurity Due Diligence,” August 27, 2015, *Chicago Journal of International Law*, 2016; and William M. Stahl, “Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity,” *Georgia Journal of International and Comparative Law*, 40 (1) 2011.

16. Major Erik M. Mudrinich, “Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem,” *Air Force Law Review*, 167 2012; and Bruce

Schneier, “Attack Attribution and Cyber Conflict,” *Schneier on Security*, January 8, 2015, <https://www.schneier.com/blog/archives/2015/01/attack_attribut.html>.

17. Martin Libicki, “Would Deterrence in Cyberspace Work Even with Attribution,” *Georgetown Journal of International Affairs*, April 22, 2015, <<http://journal.georgetown.edu/would-deterrence-in-cyberspace-work-even-with-attribution/>>.

18. Robin Tatam, “Cracking the Problem of Endpoint Security,” *HelpSystems*, December 19, 2014, <<http://www.helpsystems.com/powertech/cracking-endpoint-security-problems>>.

19. Joseph S Nye Jr., “Nuclear Lessons for Cyber Security,” DTIC Document, 2011, <<http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA553620>>.

20. Bruce Schneier, “We Still Don’t Know Who Hacked Sony,” *The Atlantic*, January 5, 2015, <<http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/>>; and Bruce Schneier, “Reacting to the Sony Hack,” *Schneier on Security*, December 22, 2014, <https://www.schneier.com/blog/archives/2014/12/reacting_to_the.html>.

21. David Sanger and Martin Fackler, “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say,” *The New York Times*, January 18, 2015, <<http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html>>

22. Schneier 2015.

23. Kenneth Geers, Darien Kindlund, Ned Moran, and Rob Rachwald, “World War C: Understanding Nation-State Motives behind Today’s Advanced Cyber Attacks,” Technical report, FireEye, 2014, <<http://ver007.com/tools/APTnotes/2013/fireeye-wwc-report.pdf>>

24. Nicolas Falliere, Liam O Murchu, and Eric Chien. “W32. Stuxnet Dossier.” *Symantec*, September 30, 2010.

25. Ibid.

26. Bruce Schneier, “Computer Network Exploitation vs. Computer Network Attack,” *Schneier on Security*, March 10, 2014, < https://www.schneier.com/blog/archives/2014/03/computer_network.html>.

27. Joint Chiefs of Staff, “Cyberspace Operations,” Joint Publication 3-12 (R), Washington D.C.: Department of Defense, February 5, 2013; and Joint Chiefs of Staff, “Information Operations,” Joint Publication 3-13, Washington D.C.: Department of Defense, November 20, 2014.

28. Schneier, “Computer Network Exploitation vs. Computer Network Attack.”

29. Nate Cardozo and Eva Galperin, "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?" Electronic Frontier Foundation, May 20, 2015, <<https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation>>; and Andrea Peterson, "The Government Is Headed back to the Drawing Board over Controversial Cybersecurity Export Rules," *The Washington Post*, July 29, 2015, <<https://www.washingtonpost.com/news/the-switch/wp/2015/07/29/the-government-is-headed-back-to-the-drawing-board-over-controversial-cybersecurity-export-rules/>>.
30. John Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy*, February 27, 2012, <<http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/>>; Thomas Rid, *Cyber War Will Not Take Place*, Vol. als eBook (New York City: Oxford University Press, 2013); and P.W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York: Oxford University Press, 2014).
31. Eneken Tikk, Kadri Kaska, Kristel Rünneri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008).
32. Rid argues that: "... all acts of war are violent or potentially violent . . . , an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker's will . . . to qualify as an act of war, an attack must have some kind of political goal or intention."
33. Rid.
34. James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," (Washington D.C.: Office of the Director of National Intelligence, February 26, 2015).
35. Michael N. Schmitt, "Attack' as a Term of Art in International Law," Proceedings of the 4th International Conference on Cyber Conflict, September 7, 2012, 283-293.
36. James Stavridis, "Incoming: What Is a Cyber Attack?" *Armed Forces Communications and Electronics Association Magazine*, January 1, 2015, <<https://www.afcea.org/content/?q=incoming-what-cyber-attack>>; and Michael N. Schmitt, "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis," *Lawfare Blog*, January 8, 2015, <<https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis>>.
37. Given the scope of this paper, the author will not go into further detail about the (legal) differences between the use of force and an armed attack in cyberspace. However, it is important to note that most scholars agree that the threshold under Art. 2(4) UN Charter is lower than under Art. 51 of the UN Charter. In other words, a particular cyber attack might breach Art. 2(4) but not rise to the threshold of allowing a state to invoke self-defense under Art. 51.
38. United Nations, *Charter of the United Nations*, October 24, 1945, 1UNTS XVI.
39. NATO, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Ed. Michael N. Schmitt. (Cambridge: Cambridge University Press, 2013).
40. *Proposal for an International Code of Conduct for Information Security*.
41. United Nations 2013.
42. United Nations 2015.
43. Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict."
44. Meyer, "Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace."
45. Nye, "The Regime Complex for Managing Global Cyber Activities."
46. Patryk Pawlak, "Cyber Diplomacy," Briefing, Brussels, Belgium: European Parliament, October 2015. p. 2.
47. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, 39(3), Winter 2014/2015, 7-47; and Sophie Beach, "China and Russia Support 'Cyber Sovereignty,'" *China Digital Times*, May 11, 2015, <<http://chinadigitaltimes.net/2015/05/china-and-russia-agree-to-respect-cyber-sovereignty/>>.
48. *Proposal for an International Code of Conduct for Information Security*
49. *Department of Defense Dictionary of Military and Associated Terms*, Department of Defense, Joint Publication 1-02, 58.
50. *Submission to the United Nations General Assembly Resolution*, Permanent Representative of the People's Republic of China, A/62/98, May 15, 2007, 7.
51. Ashley Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process," *Lawfare Blog*, May 31, 2015, <<https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process>>.
52. Maurer; Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law," *Texas Law Review*, 88 (2009): 1571, <http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr88§ion=56>; Watts, "Cyber Norm Development and the United States Law of War Manual"; Selin; and Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests*, 36(5), September 3, 2014, 322-31.

53. United Nations 2013.
54. Pawlak.
55. For more general information and latest proposals on CBMs in cyberspace, see: Healey et al., "Confidence-Building Measures in Cyberspace - A Multistakeholder Approach for Stability and Security."
56. Organization for Security and Co-operation in Europe Permanent Council.
57. Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict."
58. Nye Jr, "Nuclear Lessons for Cyber Security."
59. New America, Global Cyber Definitions Database, <www.newamerica.org/cyber-global/cyber-definitions/>
60. See: <https://www.cybersecurity.ox.ac.uk/education/cdt>.
61. See: <http://www.lawandsecurity.org/ASPIRE-Scholarship>.

When War is Not Worth Winning

by Dr. Matthew Testerman

Winning a war requires the capacity to wage a war and an understanding of an end-state that equates to winning. These fundamental concepts, however, are not well defined. This essay draws from recent historical examples, contemporaneous strategy documents, and formal game theory to provide some additional degree of conceptual clarity that will enhance the debate about winning without war. In the past two decades, the U.S. has developed a demonstrated capacity to win with war. Victory in kinetic war fighting is nearly assured and can be accomplished with limited cost. Despite this, in the modern context, war has evolved to the point that war is not worth winning. It is far from the case that there are no wars to be fought, but the political and economic constraints of the international system have transformed the environment in which the U.S. operates militarily. Evidence of this is found in the strategic outlook of the U.S. military as documented in the revised U.S. naval strategy, especially when compared to earlier maritime strategy. To inform this discussion, game theoretic explanations of strategic interactions are helpful. The assumptions underlying recent U.S. naval strategy can be understood by applying the basic construct of a “game of strategic entry.” Applying this construct, one finds that war is not worth winning— a conclusion that has substantive consequences for designing, organizing, and employing naval forces.

A game of strategic entry – also conceptualized as an economic model of market entry, or a political model of challenging an incumbent – has a fairly simple structure. There are two players who move sequentially. The first player decides to attack or not attack. If the first player attacks, the second player chooses to retaliate or capitulate. There are thus three potential outcomes: the status quo (player one decides not to attack), capitulation (player one attacks and player two capitulates), or a war of uncertain outcome is fought (player one attacks and player two retaliates). In deciding what action to take, both players consider the costs of attack and retaliation as well as the chances of their winning the war. Strategies are developed based on expected rational choices of the other player. The theory of the game holds that player one will attack when there is a relatively high probability of winning and the cost of waging war is moderate-to-low. While simplistic, the game reveals the very basics of a strategic interaction and emphasizes the need for accurate information

on the likelihood of victory and the costs of war.

The lessons of the past thirty years, however, do not align quite so nicely with the underlying assumptions of game theory. The United States has fought and won kinetic wars. In these wars winning is understood as battlefield victory and either changed behavior of a regime or regime change. The removal of Manuel Noriega in *Just Cause*, the defeat of Iraq’s army in *Desert Storm*, the withdrawal of Serbian forces from Kosovo in *Allied Force*, regime change in Afghanistan in *Enduring Freedom*, the toppling of the Hussein regime in *Iraqi Freedom*, and the Qaddafi regime in *Odyssey Dawn* all affirmatively bolster assessments of America’s ability to win in a kinetic war. Furthermore, the estimates of likely costs in terms of human lives have greatly declined. Desert Storm in 1991 was the last time that pundits cautioned that the likelihood of victory was uncertain and that casualties would be extremely high. At best, the estimates of between 4,000 and 30,000 U.S. military casualties were off by a factor of ten in their predictions of this aspect of conflict’s human cost.¹ Within the context of the strategic entry game, the U.S. would be expected to develop strategies that reflect these underlying expectations of a high probability of winning and low costs for fighting. War should be a preferred method of winning.

A predisposition to war, however, is clearly not the announced strategy of the U.S. government. The recently released Navy strategy document, *A Cooperative Strategy for 21st Century Seapower: Forward, Engaged, Ready* (henceforth referred to as *CS21R*), describes multiple types of military activities short of war that shape the environment in which the Navy operates and are intended to deter conflict. In this latest incarnation of the maritime strategy, the dominant theme is that modern strategy “raises the prevention of war to a level equal to the conduct of war.”² The focus is pro-active in shaping the strategic environment beyond traditional roles of presence and deterrence. Repeatedly, reference is made to the complexities of the geopolitical and military environment, suggesting that war may be ill-suited to redressing contemporary crises.³ The role of the world’s largest Navy is to shape the environment, deter a range of potential enemies, and only in limited circumstances “respond to crisis” or “deter aggression” using kinetic force. Only in a few instances is reference made to winning wars.⁴ Certainly winning

war is only one component of the Navy's mission set, but its relatively sparse mention in *CS21R* is noteworthy in illuminating a global context in which fighting wars is not the primary emphasis of the maritime strategy. It is also noteworthy that the cost of fielding fighting forces is specifically highlighted as fiscal constraint by the Secretary of the Navy – a constraint that affects decisions in organizing, equipping, and employing the fleet.⁵ Even though the immediate costs of war are relatively low and the chance of winning high, current maritime strategy does not favor war.

These observations are perhaps more salient when contrasted with *The Maritime Strategy of 1986*. That document, reflecting the markedly different global environment of the Cold War, outlined a strategy “to bring about war termination on favorable terms” and emphasized preparation for global conflict.⁶ The spectrum of conflict is outlined as a continuum from peacetime presence, to crisis response, to global conventional war.⁷ Winning a war was understood as a achieving a decisive outcome. Conflicts were to be put out as if “brushfire” and naval forces were to “suppress or contain international disturbances.”⁸ *The Maritime Strategy*, while acknowledging the threats posed by the full spectrum of conflict by state and non-state actors and their connections to the global economy, emphasized winning through war. The then-Secretary of the Navy pressed for sustained budget growth to fund the fleet necessary for this strategy and the costs of fighting, whether in human casualties or in dollars, were not identified as a limiting factor.⁹ U.S. maritime strategy in 1986 is therefore dramatically different from that of today.

This presents a paradox. While the costs of waging war have decreased since 1986 and the likelihood of winning war has increased, today the U.S. employs a strategy that de-emphasizes winning within an environment of significant cost constraints. In part, this apparent contradiction is explained by a changed understanding of what it means to win and of what the long-term costs of war are.

It is hardly surprising that a second look at the successes of kinetic military operations of the last thirty years reveals that while winning-as-regime-change was accomplished, the subsequent peace building and peace sustainment operations have consumed significant resources and fostered global instability. The success of *Odyssey Dawn* in enabling the overthrow of Qaddafi has left in its wake a bifurcated political and chaotic security landscape in what used to be Libya. A substantive debate has also followed operations in Iraq and Afghanistan about what it means to win. Similarly, while initial military victory has been at relatively low human costs, the long-term follow-on commitments have defied predictions and drawn out both the fiscal and human costs over many years. To again apply the game theoretic outlook on war, the calculus of waging war is changed when the military victory is not as decisive as expected and the costs of war are unclear. With so much uncertainty over outcome and ambiguity in costs, the preferred action becomes maintenance of the status quo. *A Cooperative Strategy for 21st Century Seapower:*

Forward, Ready, Engaged reflects this strategic environment in which primacy is not only given to winning without war, but more accurately a world in which winning is not worth war.

The changed strategic environment requires a reexamination of the role of the Navy. Generally, the purpose of a maritime strategy is to “reassess our approach to shifting relationships and global responsibilities” in order to “design, organize, and employ the Sea Services.”¹⁰ Fundamentally, if winning is not worth war, then one has to question the relevance of and need for, in this case, a Navy that has been built over several decades to effect kinetic operations. One could argue that this kinetic force has adapted well to its predominant employment in a range of non-combat roles. Moreover, agile networks, cyberspace operations, electromagnetic maneuver warfare, and integrated non-kinetic fires are considered to be worthy of investment in equipment, infrastructure, personnel, and tactics because the conflicts in which they will be used are considered to be worth winning.¹¹ In the second decade of the 21st century, the Navy has clearly adapted to the new strategic environment.

However, shifting the design principle of the Navy from fighting wars to providing maritime security, humanitarian assistance, and all-domain access, as outlined in *CS21R*, raises the question of whether this future U.S. Navy is capable of being employed in those rare instances when it is called upon to fight wars. One questions whether the Navy's new mission areas are preparing the battlespace for a fleet at war, shaping the environment to avoid war, neither, or both. While doing both would appear to align with the strategy, this could have unknown costs to the Navy's ability “to fight and win when required.”¹²

It is clear that today's strategic environment, even with an emergent China and resurgent Russia, is substantially different from that of the mid-1980s. The acknowledgement of the complexity of what it means to win and a better understanding of the long term costs of waging war have altered calculations of the utility of war. It is encouraging to find that modern naval strategy appears to reflect this new reality. In considering this choice of strategies, however, it bears continued debate about the underlying assumptions of what it means to win with or without war in the modern era and the degree to which the remote possibility of war must be acknowledged in designing, organizing, and employing the Sea Services. Paradoxically, this leads to a reflection similar to that of the computer, Joshua, in the closing scene of a movie from that bygone era of the Cold War, where it observes that “the only winning move is not to play.”¹³

Dr. Matthew Testerman is a Commander in the U.S. Navy and a Permanent Military Professor stationed in the Department of Political Science, U.S. Naval Academy, Annapolis, MD, where he currently serves as the Department Chairman. He can be reached at his email address: testerma@usna.edu

Material contained herein is made available for the purpose of peer review and discussion and does not necessar-

**ily reflect the views of the United States Naval Academy,
the Department of the Navy, or the Department of Defense.**

1. Michael O'Hanlon, "Estimating Casualties in a War to Overthrow Saddam," *Orbis*, Winter 2003, p. 6.
2. U.S. Navy, "Maritime Strategy Fact Sheet," <http://www.navy.mil/maritime>, accessed 10 May 2015.
3. U.S. Navy, *A Cooperative Strategy for 21st Century Seapower: Forward, Engaged, Ready (CS21R)*, March 2015, p. 3 "volatility, instability, complexity, and interdependence", p. 4 "persistent instability and under-governed areas", "regional instability threatens global economic stability in a hyper-connected world."
4. *CS21R*, p. i "...continued commitment to maintain the combat power necessary to deter potential adversaries and to fight and win when required." p. 19 "The Sea Services operate in the world's oceans to protect the homeland, build security globally, project power, and win decisively."
5. *CS21R*, p. I "Our responsibility to the American people dictates an efficient use of our fiscal resources," p. 33 "...conserve capacity of limited resources in the magazine in favor of more efficient and less costly means, where available..."
6. James D. Watkins, "The Maritime Strategy," *The Maritime Strategy*, Annapolis: US Naval Institute Press, January 1986, p.3, 5.
7. Watkins, figure 3, p. 8.
8. P. X. Kelley, "The Amphibious Warfare Strategy," *The Maritime Strategy*, Annapolis: US Naval Institute Press, January 1986, p. 25.
9. John F. Lehman, Jr., "The 600-Ship Navy," *The Maritime Strategy*, Annapolis: US Naval Institute Press, January 1986, p. 38-40.
10. *CS21R*, p. I, iii.
11. *CS21R*, p. 33.
12. *CS21R*, p.i.
13. *War Games*, directed by John Bradham (1983: Beverly Hills, CA: MGM, 2008), DVD.

The Strategic Duel over Taiwan

by Ian Easton

The United States and the People's Republic of China (PRC) are firmly entrenched in what will be a long and intense strategic competition for dominance over the Pacific Rim. American strategists Andrew Marshall, Robert Kaplan, and Aaron Friedberg began foretelling of this great power struggle over a decade ago.¹ They recognized before anyone else that there are strong forces underpinning the U.S.-China rivalry. The two countries' political systems and national interests stand in fundamental opposition. This is why, despite Washington's reluctance to officially admit it, strategic competition between the U.S. and the PRC is unavoidable.

The United States, while an imperfect democracy, is an inspiration to people everywhere who yearn for the freedom and dignity that comes from having a representative government, independent legal system, and market economy. In the PRC, on the other hand, power is monopolized by the Chinese Communist Party (CCP), a political organization that is directly responsible for more human suffering than possibly any other regime past or present, anywhere in the world.² Numerous State Department reports detail the past and continuing human rights violations occurring under the watch of the CCP.³

For all its much ballyhooed economic reforms, China's economy is still largely controlled by massive state-owned corporations, making it a mercantilist country, not a capitalist one.⁴ Much of Beijing's economic power ultimately stems from its remarkable ability to lure foreign business elites with promises of access to its huge market. Once the hook is set, China pockets their investments, steals their intellectual property, and undercuts their market competitiveness.⁵

Yet it is not the PRC's unsavory political or economic practices that will ensure sustained U.S.-China competition over the coming decades, although future American presidents, like Barack Obama, will undoubtedly be tempted to paper over ideological differences for expedience sake. Rather, Beijing's insecure and aggressive nature is at the root of the problem. In recent years, China has stoked maritime tensions with Japan and the Philippines, both treaty allies of the United States; provoked border clashes with India, a democratic nation and American security partner; and enabled nuclear missile proliferation amongst its

friends: North Korea, Pakistan, and Iran.⁶ Track records tell a compelling story. The PRC's track record indicates that a growing number of geostrategic issues could eventually result in a clash between the United States and China.

Future Flashpoint

Of all the geostrategic powder kegs out there, the potential for a war over Taiwan is the largest and most explosive. Beijing has made clear that its main external military objective is attaining the ability to apply overwhelming force against Taiwan during a war, and in a manner that would keep American-led coalition forces from intervening.⁷ Chinese military strategists obsess over Taiwan because their communist party masters are deeply insecure. Beijing views Taiwan, which exists as a free and independent state known officially as the Republic of China, as a grave threat to its totalitarian grip on domestic political power.⁸ Taiwan is dangerous to Beijing because it serves as a beacon of freedom for Chinese-speaking people everywhere.⁹ Consequently, the People's Liberation Army (PLA) considers the invasion of Taiwan to be its top planning priority. It is this envisioned war that drives PLA modernization.¹⁰

Understanding a Taiwan scenario first requires some myth-busting. It has become conventional wisdom that Taiwan will eventually be pulled into China's orbit by cross-strait trade and other economic entanglements.¹¹ This view, however, is disconnected from the reality on the ground in Taiwan. The Taiwanese are fiercely protective of their hard-won freedoms and rightfully proud of their democracy. They are no more willing to compromise their territorial sovereignty for the sake of economic benefits than the Japanese or Australians. In spite of the power disparity that exists--Taiwan has a population of 23 million to China's 1.3 billion--Taipei's close defense ties with Washington means that it does not have to bow to coercion from Beijing, economic or otherwise.¹²

Another popular myth is that the U.S. will sell Taiwan out.¹³ American commitment to Taiwan though is enshrined in U.S. Law 96-8, the Taiwan Relations Act.¹⁴ This legal instrument is founded on calculations of national interests. Every professional

American strategist since Admiral Chester Nimitz and General Douglas MacArthur has recognized that Taiwan is a center of gravity in the Asia-Pacific.¹⁵ The island sits astride the world's busiest maritime and air superhighways, right in the middle of the first island chain, a defensive barrier for keeping Chinese power projection in check.¹⁶ While America does not need Taiwan as a base for its troops, planes, or ships, it is strategically interested in the island remaining in the hands of a friendly government. For this reason, any PRC attempt to gain control of Taiwan would almost certainly be regarded as an attack on the vital interests of the United States, and therefore repelled by any means necessary, including military force.

The question of how the U.S. can best deter Chinese aggression against Taiwan will be hotly contested in the years ahead. Peace and prosperity in Asia and beyond are riding on the ability of the United States to get this problem right. Some scholars have entertained notions of abandoning Taiwan, trading it away for other ends as if it were a stack of poker chips and not a democratic country.¹⁷ Policymakers in Washington, however, should ignore those views, because the dispute between China and Taiwan cannot be separated from the larger geopolitics of the region. Taiwan is critical not only for its location, but also because of its shared values with the United States.¹⁸ Historical experience shows time and time again that nations that share democratic values are the best partners and worth defending. Common values generate common interests, which are the basis for making a common cause in addressing global challenges.

Imbalance, Rebalance, Quagmire, and Elections

When it comes to strategic interaction with China, the United States has suffered from a lack of clarity, unsure of what is needed to compete effectively with China or whether the competition even exists in the first place. Since the early 1970s, many American foreign policy elites have taken the strategic importance of the PRC for granted and asserted that Washington needs Beijing's cooperation, first geostrategically as a counterweight to the Soviet Union, then economically for market access, and more recently diplomatically as a partner on global issues ranging from North Korea to the Taliban and from piracy to climate change. This view is especially pronounced among those who embrace the notion that America is in decline and that China is going to prevail over the long run. From their perspective, the best the U.S. can do is make a grand bargain that would limit China's ascendancy to its own sphere of interest.¹⁹ American policymakers, influenced by these defeatist views, have often gone to great lengths to accommodate China's communist leadership. This tendency to overvalue the strategic importance of maintaining warm U.S.-PRC relations is something that unnecessarily weakens Washington's bargaining power with Beijing, and ultimately undermines efforts to formulate long-term strategy.

America's relatively sanguine approach to China's emergence as a strategic competitor is increasingly difficult to reconcile with

events. Over the past decade, the PRC has provided Washington several indicators that trouble is lurking ahead. However, each of them has been minimized or ignored in the name of positive Sino-U.S. relations. The first wake-up call came on January 11, 2007, when China shot a ballistic missile into a target satellite in low earth orbit.²⁰ This missile test was followed by several others which as a whole clearly demonstrate Beijing's intention to weaponize space and neutralize the eyes and ears of U.S. military power in a conflict.²¹ Another warning came in 2010, when China deployed the world's first anti-ship ballistic missile, a weapon specifically designed to sink aircraft carriers, the queens of America's fleet.²² Many other unsettling developments, both diplomatic and military, followed over the course of the following five years.²³

Even in the face of these events, some scholars have clung to the false hope that mutual economic interdependence, military-to-military exchanges, and favorable diplomatic treatment will build trust and socialize China internationally, enticing it into becoming a responsible stakeholder. They often emphasize the risks of inadvertent conflict and escalation control if their policy prescriptions are not followed. Yet none of these factors have dulled China's competitive instincts. If anything, they have only served to heighten them.²⁴

Recognizing the looming storm ahead, Kurt Campbell, Assistant Secretary of State for East Asia under Secretary of State, Hillary Clinton, spearheaded the strategy of rebalancing American attention to Asia in the early years of the Obama Administration.²⁵ America's allies in Asia warmly welcomed the rebalance, or "pivot" as it became known. As part of the effort, the Pentagon established a new Air-Sea Battle office, which generated much excitement among those who recognized fresh operational concepts were needed for dealing with China's military threat.²⁶ However, when Campbell stepped down in early 2013, things began to unravel. White House leadership, characterized by a strong focus on domestic issues, the Middle East, and climate change, quickly allowed the much-anticipated rebalance to quagmire.²⁷

This inattention exacted a heavy toll in 2015 when several major events occurred which adversely affected U.S. strategic interests. The PRC systematically created a massive archipelago of artificial island bases in the South China Sea, claiming the entire area as a virtual province of China. This disrupted ongoing attempts to apply international legal mechanisms, like the United Nations Convention on the Law of the Sea, to settle disputes and greatly weakened the defensive positions of Brunei, Indonesia, Malaysia, Philippines, Taiwan, and Vietnam.²⁸ Next, it was revealed that Chinese intelligence agents had penetrated American systems and compromised the identities (including fingerprints) of over twenty million Americans who worked for the federal government.²⁹ Not long afterwards, China held a military parade in Beijing where the military rolled out a new intermediate range ballistic missile that could be used against the U.S. territory of Guam—a strategic hub in the Western Pacific.³⁰

Confidence in American leadership has declined among democratic allies across the Asia-Pacific as the result of Beijing's actions and Washington's inactions. The resultant power vacuum in the Pacific has hit Taiwan especially hard; it has no other security partners to turn to for help, and its threat-environment is the most stressing. Taiwanese officials now frequently complain about Washington's unwillingness to sell them new fighters, tanks, drones, and destroyers. Even submarine technology, promised by President George W. Bush in 2001, has proven out of reach for Taipei. The current White House, deeply fearful of rousing Beijing's ire, has instead offered Taiwan second-rate equipment, of the type provided to Mexico.³¹ Adding insult to injury, U.S. Navy ships now make port calls up and down the PRC coast, sailing past Taiwan at full steam as if it were somehow a dreadful pariah state, not a friendly democracy.³²

The landslide results of the recent presidential and legislative elections in Taipei are telling. The citizens of Taiwan chose Dr. Tsai-Ing-wen, whose political party and its supporters are widely viewed as tough on China and friendly to the United States—and therefore more likely to secure a better future relationship with Washington.³³ At the same time, they also chose a policy platform that calls for a more robust indigenous defense industry as a pragmatic hedge against continued American paralysis.³⁴ Taiwan wants to arm itself and has resolved to do so whether its “big brother” helps or not. This can-do attitude means that the small island democracy, largely ignored for the past decade, will soon be at the front of American geostrategic thinking. If the contest of the century is to be waged between the U.S. and PRC for primacy in the Pacific, then Taiwan will assuredly be at the center of the action.

Conclusion

All indications suggest that China is striving for military superiority over the United States in the Pacific, and especially in a Taiwan invasion scenario. Beijing's communist government sees its future aspirations as fundamentally incompatible with an American-led global order. The U.S. and PRC are engaged in a strategic standoff that will likely define the decades ahead. Those denying this are simply failing to be skeptical enough, or too satisfied with information—often crafted in Beijing—that conforms to their preconceptions. They are simply not giving enough weight to what Chinese leaders are actually saying, writing, and doing.

The next American president will therefore come into office during a period of shifting global power, which, if the trend is not arrested, will be increasingly adverse to American interests. Without a course correction, the U.S. and other Pacific democracies will find themselves confronted by an adversary who does not share their most fundamental beliefs and who will soon be able to threaten much of region and beyond. Much more can and should be done by America and allies to convince the PRC that a war in the Taiwan Strait—or anywhere else—would be fruitless and financially crippling. This will only be possible with

stronger and smarter American leadership.

Mr. Ian Easton is as a research fellow at the Project 2049 Institute, where he conducts research on defense and security issues in Asia. Mr. Easton previously served as a 2013 visiting fellow at the Japan Institute for International Affairs (JIIA) in Tokyo and worked for two years as a China analyst at the Center for Naval Analyses (CNA).

1. See Andrew Krepinevich and Barry Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy* (New York: Basic Books, 2015), 227-246; Aaron L. Friedberg, *A Contest for Supremacy: China, America, and the Struggle for Mastery in Asia* (New York: W.W. Norton & Company, 2011); and Robert Kaplan, “How We Would Fight China,” *The Atlantic*, June 2005, 49-64.
2. See Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Perennial, 2010); Frank Dikotter, *Mao's Great Famine* (New York: Walker & Company, 2010); and Yang Jisheng, *Mubei: Zhongguo Liushi Niandai Da Jihuang Jishi* [Tombstone: A Record of the Great Chinese Famine of the 1960s] (Hong Kong: Cosmos Books, 2008).
3. “China (Includes Tibet, Hong Kong, and Macau) 2014 Human Rights Report,” U.S. Department of State, at <http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2014&dlid=236432#wrapper>.
4. Robert D. Atkinson and Stephen Ezell, “False Promises: The Yawning Gap Between China's WTO Commitments and Practices,” *Information Technology & Innovation Foundation*, September 17, 2015; Stephen Ezell, “China's Economic Mercantilism,” *Industry Week*, July 24, 2013; Derrick Scissors and Dean Cheng, “Preparing for the New Chinese Government,” *China Business Review*, January 1, 2013.
5. Ibid. See also Dennis C. Blair and Jon M. Huntsman, Jr. (Chairs), *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (Washington, D.C.: The National Bureau of Asian Research, 2013), at http://www.ipcommission.org/report/ip_commission_report_052213.pdf.
6. See Shirley A. Kan, *China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues* (Washington, D.C., Congressional Research Service, 2015); Vivek Raghuvanshi, “India-China Border Talks Make No Headway,” *Defense News*, May 23, 2015; and Patrick M. Cronin, *The Challenge of Responding to Maritime Coercion* (Washington, D.C.: Center for New American Security, September 2014).
7. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2015* (Washington, D.C.: Department of Defense, 2015), 6 & 57-61; and *The PLA Navy: New Capabilities and Missions for the 21st Century* (Suitland, MD: Office of Naval Intelligence, 2015), 9.

8. Academy of Military Science's Military Strategy Research Department, *The Science of Military Strategy 2013* (Beijing: Academy of Military Science, 2013), 198-200; 209-212; 221-222; 230-232.
9. *Ibid.*, and Ian Easton, "The South China Sea is Not Beijing's Next Battlefield," *The National Interest*, September 19, 2015.
10. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2015* (Washington, D.C.: Department of Defense, 2015), 6 & 57-61; and *The PLA Navy: New Capabilities and Missions for the 21st Century* (Suitland, MD: Office of Naval Intelligence, 2015), 9.
11. Tom Wright and Aries Poon, "Taiwan Grapples With Closer China Ties," *Wall Street Journal*, December 7, 2014; Ricky Yeh, "Over-Dependence on China will Doom Taiwan," *The Diplomat*, August 26, 2014; Robert D. Kaplan, "The Geography of Chinese Power," *Foreign Affairs*, May/June 2010; Stephen Nelson, "Falling into China's Orbit," *CBC News*, December 18, 2008.
12. See Kin W. Moy, "U.S.-Taiwan Relations in a Changing Regional Landscape," *Remarks of Director of American Institute on Taiwan*, September 30, 2015, at <https://www.ait.org.tw/en/officialtext-ot1523.html>.
13. See John J. Mearsheimer, "Say Goodbye to Taiwan," *The National Interest*, March-April 2014; and Thalia Lin, "Don't Say Goodbye to Taiwan," *The National Interest*, February 27, 2014; and Nat Bellocchi, "Say goodbye to Taiwan, say goodbye to peace," *Taipei Times*, March 9, 2014.
14. Taiwan Relations Act, Pub. L. No. 96-8, § 2, 93 Stat. 14 (1979).
15. See Bruce A. Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979* (Newport, RI: Naval War College Press, 2012); Edward J. Marolda, *Ready Seapower: A History of the U.S. Seventh Fleet* (Washington, D.C.: Naval History & Heritage Command, 2011), and Robert Ross Smith, "Luzon Versus Formosa" in Kent Roberts Greenfield (ed.), *Command Decisions* (Washington, D.C.: Defense Department Army Center of Military History, 1960).
16. Robert D. Kaplan, "The Geography of Chinese Power," *Foreign Affairs*, May/June 2010.
17. For example, see Charles Glaser, "A U.S.-China Grand Bargain? The Hard Choice between Military Competition and Accommodation," *International Security*, Spring 2015, 49-90; and Lyle J. Goldstein, *Meeting China Halfway: How to Defuse the Emerging US-China Rivalry* (Washington, D.C.: Georgetown University Press, 2015).
18. For an excellent assessment of why Taiwan's values matter to U.S. foreign policy interests, see Mark A. Stokes and Sabrina Tsai, *The United States and Future Policy Options in the Taiwan Strait* (Arlington, VA: Project 2049 Institute, February 2016), at http://www.project2049.net/documents/160130_%20ALTER-NATE_FUTURE_POLICY_OPTIONS_IN%20THE_TAIWAN_STRAIT.pdf.
19. See Glaser, and Goldstein.
20. Shirley A. Kan, "China's Anti-Satellite Weapon Test," *CRS Report for Congress*, April 23, 2007; and Ian Easton, *The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy* (Arlington, VA: Project 2049 Institute, June 2009).
21. Brian Weeden, "Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space," *The Space Review*, March 17, 2014.
22. Andrew S. Erickson, *Chinese Anti-Ship Ballistic Missile (ASBM) Development: Drivers, Trajectories and Strategic Implications* (Washington, D.C.: The Jamestown Foundation, May 2013), 10. For further details, see Mark Stokes, *China's Evolving Conventional Strategic Strike Capability: The anti-ship ballistic missile challenge to U.S. maritime operations in the Western Pacific and beyond* (Arlington, VA: Project 2049 Institute, September 2009).
23. For example, see Robert Windrem, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," *NBC News*, July 30, 2015; Sam LaGrone, "China Sends Uninvited Spy Ship to RIMPAC," *USNI News*, July 18, 2014; Jon Harper, "Chinese warship nearly collided with USS Cowpens," *Stars and Stripes*, December 13, 2013; Madison Park, "Why China's new air zone incensed Japan, U.S.," *CNN*, November 27, 2013; Esther Tran Le, "China and Philippines in Standoff Over Resource-Rich Islands," *International Business Times*, April 11, 2012; Elisabeth Blumiller and Michael Wines, "Test of Stealth Fighter Clouds Gates Visit to China," *New York Times*, January 11, 2011.
24. Colby and Ratner.
25. Catherine Putz, "Campbell: The History of the 21st Century Will be Written in Asia," *The Diplomat*, April 15, 2015; Kurt M. Campbell and Ely Ratner, "Far Eastern Promises: Why Washington Should Focus on Asia," *Foreign Affairs*, May/June 2014; Kurt Campbell and Brian Andrews, "Explaining the US 'Pivot' to Asia," *Chatham House*, August 2013; and Hilary Clinton, "America's Pacific Century," *Foreign Policy*, October 11, 2011.
26. See Aaron L. Friedberg, *Beyond Air-Sea Battle: The Debate Over US Military Strategy in Asia* (New York: Routledge, 2014) and Jan Van Tol, *AirSea Battle, A Point of Departure Operational Concept*, (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2010).

27. Fareed Zakaria, "Whatever happened to Obama's pivot to Asia?" *Washington Post*, April 16, 2015, at https://www.washingtonpost.com/opinions/the-forgotten-pivot-to-asia/2015/04/16/529cc5b8-e477-11e4-905f-cc896d379a32_story.html.
28. "A 'Great Wall of Sand' in the South China Sea," Editorial, *Washington Post*, April 8, 2015; and Derek Watkins, "What China Has Been Building in the South China Sea," *New York Times*, October 27, 2015.
29. Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, July 9, 2015; and Ellen Nakashima, "Chinese hack of federal personnel files included security-clearance database," *Washington Post*, June 12, 2015. For an excellent study on PLA hackers, see Mark A. Stokes, *The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398* (Arlington, VA: Project 2049 Institute, July 2015).
30. Wendell Minnick, "China's Parade Puts US Navy on Notice," *Defense News*, September 3, 2015.
31. Christopher P. Cavas, "US Frigates Approved For Transfer - Finally," *Defense News*, December 19, 2015, at <http://www.defensenews.com/story/defense/naval/ships/2014/12/19/navy-frigates-ships-taiwan-china-mexico/20642841/>.
32. See Kevin V. Cunningham, "Stetham Arrives in Shanghai to Promote Cooperation with PLA (N) East Sea Fleet," *America's Navy*, November 16, 2015; Megan Eckstein, "USS Blue Ridge Pulls into Zhanjiang, China for Port Visit," *USNI News*, April 20, 2015; and Jacob Waldrop, "Blue Ridge Strengthens Cooperation with PLA(N) North Sea Fleet in Qingdao, China," *America's Navy*, August 5, 2014.
33. Andrew Browne, "For U.S., Taiwan Vote Changes Calculus over 'One China,'" *Wall Street Journal*, January 19, 2016; Dan Blumenthal, "Will the 'One China' policy survive the new Taiwan?" *Foreign Policy*, January 19, 2016; and Jeremy Page, Jenny W. Hsu, and Eva Dou, "Taiwan Elects Tsai Ing-wen as First Female President," *Wall Street Journal*, January 16, 2016.
34. Jennifer M. Turner, "DPP Plans to Enhance Taiwan Defense: Prospects and Cross Strait Implications," *China Brief*, January 12, 2016; and Defense Policy Advisory Committee, *Bolstering Taiwan's Core Defense Industries* (Taipei, Taiwan: New Frontier Foundation, October 2014).

China's Development of Space Warfare and Its Operational Applications

by Feng-tai Hwang

As early as March 2011, the journal *Aerospace America* featured an article with the title “China’s Military Space Surge,”¹ which warned that there had been a rapid increase in China’s capability to conduct warfare in space. Such capabilities would then in turn threaten and jeopardize the ability of the carrier battle groups of the United States to conduct operations in the Pacific. This article was soon translated into Japanese and published in *Space Japan Review*. This and other high profile articles highlight the anxieties on the part of the U.S. and Japan about China’s increasing ability to militarize space, and also their concerns about its implications for the peace and security of East Asia and the entire Pacific Asia region.

On December 31, 2015 China announced the creation of three new branches of armed forces to be added into the reformed People’s Liberation Army (PLA): Army General Command, Strategic Support Force, and the PLA Rocket Force. While the PLA Rocket Force replaced the old Second Artillery Corps, what is even more intriguing is the mission of the new Strategic Support Force. According to Chinese media, the Strategic Support Force will be responsible for overseeing intelligence, technical reconnaissance, satellite management, electronic warfare, cyberwarfare, and psychological warfare. It is no coincidence that Gao Jin, the newly appointed commander of the Strategic Support Force, is also an expert on rocket science, which has further fueled media speculations that the Strategic Support Force has been created for the purpose of conducting future space warfare.²

In fact, China has been increasing the focus on the military applications of space since the end of Persian Gulf War in the 1990s. During that war, the United States mobilized dozens of satellites to aid the American-led coalition forces, enabling them to defeat Iraqi forces with extraordinary efficiency and ease. The Persian Gulf War greatly shocked PLA observers at the time, and served as a reminder that the conduct of modern warfare had been transformed by the arrival of a new generation of technology. Chinese military theorists then began to study the concept of “space warfare.” The most influential was Chang Xian-Qi who categorized space warfare into three distinct phases based on his observations of U.S. planning: the “Entry into Space,” the “Utilization of Space,” and the “Control of Space.”

“Entry into Space” is represented by the delivery of a military-purpose spacecraft into its designated orbit path. “Utilization of Space” is to harness the power of existing space assets to aid military operations across the land, naval, and air domains. For example, such power can manifest in the forms of using space sensors to conduct surveillance and gather intelligence for Anti-Access/Area Denial (A2/AD) against potential foes, to provide ballistic missile early warning, satellite navigation and communications, among other purposes. The “Control of Space” phase focuses on establishing “space superiority” with the missions of: (1) increasing survivability of one’s own military satellites and systems; (2) disrupting, sabotaging, or destroying opposing countries’ satellites and their systems when necessary; and (3) directly using space-based weapons to aid in combat operations on the ground.³

China’s Space Warfare Capabilities

After years of development, China has established an operational level of space warfare capabilities. It is useful here to provide an assessment of China’s current capabilities in terms of the three different phases in conducting space warfare.

Entry into Space

Currently China’s satellite launch vehicles can be divided into two distinct series: The “Long March” rockets and “Kuaizhou” rockets.

Long March Launch Vehicles

The new series of Long March rockets currently being developed are the Long March 5 (LM-5), Long March 6 (LM-6), and Long March 7 (LM-7). Table 1 shows the payload capacity of each series.⁵

Designed as a smaller launch vehicle, Long March 6 (LM-6) made its test flight on September 20, 2015 and delivered 20 small satellites into orbit, successfully demonstrating the feasibility of a multiple satellite launch. In terms of medium

Table 1: Payload capability of newest “Long March” series launch vehicles

Rocket Type	Launch Weight (T)	Liftoff Thrust (kN)	Payload (kg)		
			LEO	SSO (700km)	GTO
Long March 5 (CZ-5-504)	N.A.	~10451	25000	N.A.	14000
Long March 6	~103.2	1177	1500	1080	N.A.
Long March 7	594	7200	13500	5500	N.A.

launch vehicles, Long March 7 (LM-7) has been under development since 2011 and is expected to make its first test flight at some point in 2016. Its primary missions will consist of launching remote sensing low-earth orbit satellites, supplying the space station, and delivering manned space missions. For heavy launch capabilities, the Long March 5 (LM-5) has been in development since 2007 and had a successful ground test in early 2015. It is also expected to make its first test flight in 2016 and to become the primary launch vehicle for China’s future space mission to the moon.

Kuaizhou Launch Vehicle

Evolved from the earlier Kaituoazhe (KT) rockets, China’s “Kuaizhou” series are solid-fuel rockets developed by China Aerospace Science and Industry Corporation (CASIC). They are capable of delivering satellites weighing between tens of kilograms to over a hundred kilograms into low-earth orbit. Satellites can be mounted on Kaituoazhe series rockets in a short amount of time, which makes them the ideal launch vehicle to serve as a type of quick-response force in space, known as “Operationally Responsive Space.”⁶

Utilization of Space

Since China first launched its Dong Fang Hong I satellite in April 24, 1970,⁷ it has made significant progress in developing a whole range of satellites with a variety of different functions. Those satellite systems that are capable of supporting ground, air, and naval military operations are listed below:

The electronic intelligence satellites, “Yaogan” remote sensing satellites, data relay satellites, and navigation satellites deserve special attention.

Electronic intelligence satellites

Electronic intelligence satellites (ELINT) can be divided into active and passive types. Active ELINT satellites use space-based radar to detect the position and nature of ships, while passive ELINT satellites rely on the detection of radar emissions from ships to pinpoint their exact position. In March

2010, China launched Yaogan 9 which consisted of three satellites with approximate orbits of 1100 km at 63.4 degrees. Because Yaogan 9 satellites have characteristics similar to the first generation Naval Ocean Surveillance System (NOSS) developed by the United States Navy, Western observers believe that they are designed specifically with ocean-based ELINT collection missions in mind.⁸ Aside from Yaogan 9, China has already launched four sets of other “Yaogan” series ELINT satellites.⁹ The newly augmented Yaogan ELINT satellites will increase the revisit frequency so that the target acquisition latency can be further reduced.

“Yaogan” remote sensing satellites

“Yaogan” satellites produce images based on the electromagnetic signatures reflected from the ground. As there are two different means of collecting such electromagnetic signatures, there are active type Yaogan satellites which utilize synthetic aperture radar, and passive type Yaogan satellites which rely on optical image sensing. Between 2006 and late 2015, China launched a total of 27 Yaogan satellites. Five of them are ELINT satellites, while the rest are remote sensing satellites. Though China officially claimed that they are designed for land surveillance, agricultural research, disaster monitoring, and other scientific uses, Western observers suspect that these satellites are in practice used for military remote sensing purposes.

Data relay satellite

Tianlian I, China’s first data relay satellite was launched in April 2008. Tianlian I-02 and Tianlian I-03 were launched in July 2011 and July 2012, respectively.¹⁰ Tianlian I satellites serve similar functions to the tracing and data relay satellites (TDRS) of the United States, they help to relay data communication between satellites and the ground. Such data relay satellites are crucial for China’s manned-space missions and any future moon exploration mission. Tianlian I-02 satellite is located around 177 East Longitude where it may serve as part of the A2/AD data link.

Table 2: China's Satellite Systems ¹¹		
Type	Series Name	Note
Reconnaissance satellite	Fanhui Shi Weixing	Not a true sun-synchronous orbit (SSO). Image data only recoverable after satellite return to Earth
	Gaofen	First Chinese low-earth orbit satellite with designed lifespan of more than 5 years
	Yaogan	High resolution optical remote sensing satellite. L-band synthetic aperture radar (SAR) satellite
	Huanjing	Capable of hyperspectral and infrared-based multispectral synthetic aperture radar imaging
	Tianhui	Capable of capturing three-dimensional pictures
Navigation satellite	BeiDou-1	Regional navigation system
	BeiDou-2	Global navigation system, expected to be operational by 2020
Weather satellite	Fengyun 1, Fengyun 3	Polar orbit satellite
	Fengyun 2	Geosynchronous orbit satellite
Communication satellite	Fenghuo	"Zhongxing-22" tactical communications satellite "Zhongxing-20" strategic communications satellite
	Tianlian	Data relay satellite with a geosynchronous orbit
Electronic intelligence satellite	Yaogan	Capable of functioning as triangulation network

Table 3: Assessment of China's Space Warfare Capabilities			
	Low	Medium	High
Entry into Space			X
Utilization of Space		X	
Control of Space	X		

Navigation satellite

To emulate the U.S. Global Positioning System (GPS) and the Russian GLONASS system, China has developed its own BeiDou navigation satellite system. Two BeiDou-1 satellites were launched in October and December 2000 respectively, and the third was launched in May 2003.¹² These three experimental BeiDou-1 satellites together formed China's first-generation satellite navigation system. However, the BeiDou-1 system covered only China and the surrounding areas, and thus only constituted a regional navigation system. BeiDou-1 also required users to transmit positioning requests first before navigation signals could be retransmitted back to them from the satellites via ground control center, as user position data had to be calculated at the ground control center. China began the deployment of BeiDou-2, its second-generation navigation system, in 2007. BeiDou-2 will consist of 5 geosynchronous orbit satellites and 30 medium earth orbit satellites, and it is expected to have complete global coverage in-service by 2020.¹³

Control of Space

The ultimate form of the ability to control space lies in the capacity to destroy other countries' satellite systems. Such destruction can be achieved by direct attack or co-orbital attack. On January 11, 2007, China launched an anti-satellite missile (ASAT) and destroyed a retired Fengyun 1 weather satellite that was orbiting at an altitude of 865 kilometers. The destruction created a huge amount of space debris in low-earth orbit that remains and endangers the safety of other satellites. Co-orbital attacks, on the other hand, rely on sending an interceptor satellite into the same orbit path and height as the intended target, with the intention of the two coming into direct contact with one another following a few natural orbits, at which point the interceptor satellite will explode and destroy the targeted enemy satellite. When China launched the manned Shenzhou 7 mission in September 25, 2008, a small satellite named BX-1 which weighed 40 kilograms was released from the Shenzhou vehicle. Four hours later it passed by the International Space Station at a distance of merely 25 kilometers.¹⁴ Another example is the rendezvous of the Shijian 12 and Shijian 6 satellites that took place soon after the launch of Shijian 12 on June 15, 2010. Although these two separate incidents did not result in actual co-orbital attack, Western observers see them as

clear demonstrations and exercises of China's co-orbital attack capability.¹⁵

It is useful here to provide an assessment of China's current capabilities in terms of the three different phases in conducting space warfare. China has proven its "Entry into Space" capabilities, as it has already developed a range of highly mature satellite launch vehicles and facilities with high launch success rates. It is able to deliver various types of satellites into low earth orbit, sun-synchronous orbit, and geosynchronous orbit. China's "Entry into Space" capability should therefore be rated as "high."

In terms of "Utilization of Space" although China possess a comprehensive fleet of satellites, its BeiDou navigation satellite system currently still only able to deliver regional navigation services. In addition, China's remote sensing satellites still lag far behind the United States in both quality and quantity. China's "Utilization of Space" capability should therefore be rated "medium."

In terms of "Control of Space," China has conducted successful tests of anti-satellite weapons, proving its possession of anti-satellite capability at least against certain low-earth orbit satellites. However, China still has a long way to go before such weapons are actually deployed and become operational, and there is currently no publicly available information that indicate that China has any plan for developing space-based weapon platforms. China's "Control of Space" capability should therefore be rated "low."

Applications of Space Systems in Anti-Access/Area Denial Warfare

Among security analysts, there has been a dramatic increase in discussions concerning A2/AD in recent years.¹⁶ Such a trend reflects the reality that A2/AD has been widely identified as the most likely strategy China would use in a conflict with the United States over the Taiwan Strait and the surrounding areas. In its most basic form, A2/AD calls for China to deploy means that can deny United States the ability to intervene in the region militarily. In particular, such strategy would focus on preventing U.S. carrier battle groups from entering the Western Pacific region in the first place. The U.S. Center for Strategic and Budgetary Assessment (CSBA) categorized A2/AD into two distinct

parts: “Anti-Access” focuses on preventing U.S. military forces (such as fighter jets) from entering large stationary bases in the region, such as Kadena Air Base in Okinawa. “Area Denial” focuses on defeating U.S. naval forces entering the region.

To actually accomplish the goals of A2/AD, China has to build a comprehensive system that is able to combine and coordinate various detection, confirmation, tracking, and strike systems into one package. The trike system in this case would be the Dong-Feng 21 (DF-21) anti-ship ballistic missile. Detection, confirmation, and tracking systems would be comprised of land-based, over-the-horizon radar and satellites in space. Hypothetically, an implementation of the A2/AD mission would look similar to the following: (1) ocean surveillance satellite systems report detected target to over-the-horizon radar via data relay satellites and communication satellites; (2) over-the-horizon radar tracks and surveils the detected target; (3) satellite systems or unmanned aerial vehicles (UAV) provide continuous updates on the detected target’s real-time location; and (4) anti-ship ballistic missiles are launched against the target.¹⁷

Ultimately the accuracy of such A2/AD attacks is interdependent on how large the circular error probability of the strike systems are and how precise the satellite sensing systems are. To increase efficiency and ease of attack, especially against moving targets such as aircraft carriers, anti-ship ballistic missiles need to be provided with continuous updates on the target’s location. It will also be useful to shorten the amount of time it takes between when sensors pick up target to the point when attack is launched, and this would involve increasing the efficiency of the individual components such as data relay, data processing, target identification, and weapon delivery.

Conclusion

Since China began development of its space program in the 1970s, it has now built up a capability in conducting space warfare that can no longer be ignored. China has matured in the “Entry into Space” phase, and it has also made significant progress in the “Utilization of Space” phase in recent years.

In terms of China’s capability in the “Utilization of Space,” attention should be focused not only on the rollout of new hardware such as satellite launches, but also the degree to which China is able to effectively integrate the various sources of data into its information downlink, processing, analyzing, and finally command and control systems. We should therefore pay particular attention to China’s newly established Strategic Support Force and whether it would make efforts to integrate space information into improving the overall command, control, communications, and computer systems and intelligence, surveillance and reconnaissance (C4ISR) capabilities of its military.

Feng-Tai Hwang received his Ph.D. in Engineering Mechanics from The Ohio State University in 2000. He joined the National Space Organization of Taiwan in 2003 and has

been working in the area of satellite mission analysis, Earth observation satellite mission planning & scheduling since then. Currently he serves as the system engineer of the Image Process System for FORMOSAT-5 program and leads the development team of FORMOSAT-5 Planning & Scheduling System. In addition, part of his effort is spent in the study of development trend for remote sensing satellite, space policy, and space industry analysis.

1. Covault, Craig. “China’s military space surge.” *Aerospace America* 49.3 (2011): 32-37.

2. Gertz, Bill. “Chinese Military Revamps Cyber Warfare, Intelligence Forces”. *Washington Free Beacon*. January 27, 2016. <<http://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces>>.

3. Chang Xianqi, “Military Astronautics”, National Defense Industry Press, 2002.

4. There are 15 types of rockets developed from Long March 1 (LM-1) to Long March 4 (LM-4) series rockets. Currently in service are Long March 2C (LM-2C), Long March 2D (LM-2D), Long March 2F (LM-2F), Long March 3A (LM-3A), Long March 3B (LM-3B), Long March 3C (LM-3C), Long March 4B (LM-4B), Long March 4C (LM-4C). Among them, Long March 2F (LM-2F) has been designed with delivering manned-space vehicle in mind.

5. For example, see:

[1] *SinoDefence*, “China’s new space boomers”, July 4, 2012. <<https://sinodefence.com/2012/07/04/chinas-new-space-boomers>>.

[2] *SinoDefence*, “CZ-5 and CZ-7 to make debut flight in 2016”, January 22, 2016. <<https://sinodefence.com/2016/01/22/cz-5-and-cz-7-to-make-debut-flight-in-2016>>.

[3] Gunter’s Space Page, “CZ-6 (Chang Zheng-6)”, February 21, 2016. <http://space.skyrocket.de/doc_lau/cz-6.htm>.

[4] *SinoDefence*, “CZ-6 launcher takes to the sky”, September 20, 2015. <<https://sinodefence.com/2015/09/20/cz6-takes-to-the-sky>>.

6. Gregory Kulacki, “Kuaizhou Challenges U.S. Perceptions of Chinese Military Space Strategy”, September 27, 2013, *Union of Concerned Scientists*. <<http://allthingsnuclear.org/gkulacki/kuaizhou-challenges-u-s-perceptions-of-chinese-military-space-strategy>>.

7. See Launch Record listed by China Great Wall Industry Corporation’s website, <<http://www.cgwic.com/Launchservice/LaunchRecord.html>>.

8. Ian Easton, Mark A. Stokes, *China’s Electronic Intelligence (ELINT) Satellite Developments: Implications for U.S. Air and Naval Operations*, Project 2049 Institute, 2011.

9. Yaogan-16, 17, 20, and 25 are ELINT satellites. See S. Chan-

drashekar and Soma Perumal, "China's Constellation of Yaogan Satellites & the Anti-Ship Ballistic Missile – An Update", *International Strategic and Security Studies Programme*, 2015.

10. See Launch Record listed by China Great Wall Industry Corporation's website, <<http://www.cgwic.com/Launchservice/LaunchRecord.html>>.

11. Feng-Tai Hwang, Hao-Chi Chang and Yen-Sen Chen, "Space Capability Technical Assessment - China Case Study", *29th International Symposium on Space Technology & Science*, Nagoya, Japan, 2013

12. Launch Record listed by China Great Wall Industry Corporation's website, <<http://www.cgwic.com/Launchservice/LaunchRecord.html>>.

13. Introduction of BeiDou Navigation Satellite system published on its official website. ><http://www.beidou.gov.cn/2011/12/06/20111206e06b16a3bd8846459b969277a3317e5b.html>>.

14. Brian Weeden, "China's BX-1 microsatellite: a litmus test for space weaponization", *The Space Review*, 2008, <<http://www.thespacereview.com/article/1235/1>>.

15. GlobalSecurity.org, "Chinese Demonstrates Satellite to Satellite Rendezvous, Inspection Test Bed for Duel Purpose Military Technology", <<http://www.globalsecurity.org/space/world/china/sj-12.htm>>

16. For example,

[1] Sam J. Tangredi, "Anti-Access Warfare-Countering A2/AD Strategies", Naval Institute Press, 2013.

[2] Christopher J. McCarthy, "Anti-Access/Area Denial: The Evolution of Modern Warfare", US Naval War College. <<https://www.usnwc.edu/Lucent/OpenPdf.aspx?id=95>>.

[3] Jonathan F. Solomon, "Defending The Fleet From China's Anti-ship Ballistic Missile: Naval Deception's Roles in Sea-based Missile Defense", Georgetown University, 2011.

17. Chen Haidong et.al., "Study for the Guidance Scheme of Reentry Vehicles Attacking Slowly Moving Targets", *Missiles and Space Vehicles*, No. 6, 2000.

China's United Front Strategy and its Impacts on the Security of Taiwan and the Asia-Pacific Region

by Michael M. Tsai / Po-Chang Huang

Evolution of Strategy from Hard Power to Soft Power

In 1949, Mao Zedong, leader of the Communist Party of China (CCP), defeated Chiang Kai-shek's Kuomintang (KMT) troops and succeeded in establishing the communist dictatorship of the People's Republic of China out of the "barrel of a gun." At the beginning of its rule, the CCP believed that the use of violent instruments as provided by the People's Liberation Army (PLA) was in and of itself sufficient to both suppress "reactionaries" at home and defeat "invaders" from abroad.

In this vein, during the Korean War of the early 1950s, the CCP regime sent a million-strong "Volunteer Army" into the Korean Peninsula and fought against the U.S.-led United Nations forces, thus cementing the political division of Korea and its complications that linger to this day. Between 1958 and 1960, PLA troops heavily bombarded the Chiang Kai-shek-controlled island of Kinmen, resulting in significant casualties on both sides. Between the 1960s and 1980s, the PLA and militia troops engaged in a series of border conflicts and clashes with the Soviet Union, India, and Vietnam. Throughout this period, the CCP regime still believed that military force alone was sufficient to serve as the primary bargaining chip and policy instrument in its dealing with other states.¹

However, from the late 1980s to 1990s, the collapse of Soviet Union and Eastern Bloc marked the end of Cold War and the confrontation between two global superpowers. The CCP's strategy in the international arena evolved from an overreliance on hard military force to one that utilizes both "soft power" and the "carrot and stick."

From the Chinese perspective, the concept of "soft power" encompasses the exploitation of any policy or tool outside the traditional definition of "hard" military power to achieve its desired political, economic, and diplomatic objectives. Such exploitation takes place via political, societal, commercial, economic, legal, psycho-

logical, cultural, and other means. Mass media and even tourist groups could all be used as a means of penetration to funnel and support Chinese agents deep inside enemy territory and to create conditions that are conducive to achieving China's desired outcome. This is the essence of China's strategy of the "United Front."

This article examines the United Front strategy and the ways in which China's deployment of this strategy impacts the national security of Taiwan as well as neighboring countries such as Japan, Vietnam, the Philippines, and even the United States.² The article concludes with proposed policy recommendations for how Taiwan can counter such strategies.

United Front Through Politics and Society

It is no secret that the People's Republic of China under the CCP regime has repeatedly declared Taiwan as part of its territory and vowed to "reunite" Taiwan by any means necessary. Starting in the 1990s, the CCP regime began to systematically invite Taiwan's politicians, legislators, businessmen, and other prominent public figures to visit China. During these trips, these "visitors" would receive extravagant receptions, which would serve as platforms for China to employ its United Front strategy against Taiwan. Many of these visitors were then asked to play an active role in opposing the Taiwanese independence movement and supporting Chinese reunification.³

In May 2000, the Democratic Progressive Party (DPP) candidate Chen Shui-bian won the presidential election and became the first non-Kuomintang Party (KMT) president of Taiwan, a milestone in the maturity of Taiwan's democratization. At the same time, however, China continued its United Front strategy by inviting disgruntled politicians such as then KMT chairperson Lien Chan, People First Party's chairperson James Soong, other legislators, public figures, and retired generals, to visit China. China then provided various forms

of support and benefits to those that cooperated with such a strategy. In doing so, China was not only able to instigate and intensify the vicious partisan divisions in the politics of Taiwan, but also succeeded in creating distrust and disunity among the Taiwanese society. In the words of Mao Zedong, the essence of China's United Front strategy is to "collude with the secondary enemy in order to defeat the primary enemy."⁴

In 2008, KMT President Ma Ying-jeou came to power. Since then China has continued to expand the United Front by recruiting more segments of the Taiwanese society, often using financial benefits as incentives. Targets for recruitment include labor, farmers', and fishermen unions, heads of local villages, college students, Taiwanese aborigines and tribes, businesses of all levels, academics, singers, actors/actresses, volunteer police officers, firefighters, and others. It is estimated that the number of people that have been systematically recruited to "visit" China through such officially-arranged trips have reached upwards of 50,000 people a year. These recruits, who include representatives of various broad segments of the Taiwanese population, are then intended to serve as "Trojan Horses" to inject pro-China/pro-unification sentiments and political messages into Taiwanese society. Such manipulation constitutes what the CCP terms "psychological warfare on enemy's politics and society" and is a cornerstone of China's strategy of the United Front.⁵

United Front Through the Economy

Since the handover of Hong Kong to China in 1997, China has been advocating that the same "one country, two systems" model be applied in Taiwan. To increase Taiwan's economic reliance on China, CCP leaders from Jiang Zemin to Hu Jintao have adopted the same "economy first, politics later" policy, with the priority placed on incorporating Taiwan, Hong Kong, and Macau into a "One China" common market and economic sphere. This process of economic integration would then leave Taiwan with no alternative but to accept China's political control.

As part of the economic strategy of the United Front, the CCP has in the past decade passed a series of laws designed to attract Taiwanese businesses and high-tech sectors to invest in China. Today, there are approximately 1.5 million Taiwanese investors, managers, and technical experts, along with their spouses and children, settled across China. In the past years, around 40% of Taiwan's annual total export volume have relied on China (this figure includes Hong Kong).⁶ Furthermore, 70% of Taiwan's overseas investments are directed to China,⁷ and a large portion of the foreign manufacturing contracts received by Taiwanese businesses are outsourced

to factories based in China before being exported again. These numbers serve as a painful reminder that China is succeeding in its attempt to incorporate Taiwan into its "One China" common market with serious side effects and consequences for Taiwan's own economic diversification and trading relations with the rest of the world.

United Front Through Law

In 2005, the National People's Congress of the People's Republic of China passed the Anti-Secession Law,⁸ which includes a clause stating that, "Taiwan is part of China. The state shall never allow the 'Taiwan independence' secessionist forces to make Taiwan secede from China under any name or by any means." With this piece of legislation, the CCP sought to fabricate a legal justification to use force against Taiwan.⁹

The Anti-Secession Law provoked outrage among the majority of the Taiwanese people. In effect, this law altered the perceived status quo across the Taiwan Strait that had existed for decades, where both sides were relatively at peace with the other's existence and independence. The law explicitly denies Taiwanese people the right to maintain their democratic way of life, and directly contradicts the United Nations Charter, which upholds the principle of equal rights and self-determination of all people. At the time of its enactment, the Anti-Secession Law was condemned by various states, including the United States, Japan, and the European Union.¹⁰ Few states today recognize PRC's claim in the Anti-Secession Law that Taiwan is part of its territory, as the People's Republic of China clearly does not exercise sovereign control over Taiwan, nor does it have any legal basis to make such a claim.

United Front Through Mass Media

The CCP leadership understands that the majority of the people of Taiwan want to maintain their existing democratic way of life and to maintain their political independence from the PRC.¹¹ To overcome this, the CCP makes use of a "carrot and stick" strategy in which they rapidly develop and deploy various military capabilities such as ballistic missiles that threaten Taiwan, while at the same time developing "soft power" means that employ propaganda methods to recruit Taiwanese supporters for unification.

One of the most effective means of propaganda that China has developed is the control and manipulation of mass media in Taiwan to disseminate information conducive to China's strategy of the United Front. By covertly or overtly buying out and controlling the ownership of newspaper, television channels, and internet

media in Taiwan, China is able to control a significant portion of Taiwan's mass media and to use them as a means to alter Taiwanese people's popular perceptions of the CCP government and its unification agenda.¹²

Over the past few years, a number of high profile cases have occurred in which Chinese companies or Taiwanese businessmen purchased several major Taiwanese mass media companies with close connections to the Chinese government.¹³ The purchases are notable not only because through them the CCP appears to be targeting the ownership of media that are politically neutral or lean toward supporting unification, but also media that are traditionally considered pro-independence. Media owners, managers, talk show hosts, well-known journalists, and writers are often lured with monetary incentives to switch sides and to adopt pro-China positions on political issues. Those with business involvement in mainland China are also constantly pressured to censor material critical of the CCP regime. In the CCP's view, buying off Taiwan's media is a much cheaper and more effective use of its resources than spending them on building weapons to conquer Taiwan by force.

United Front Through Tourism and Education

China's rapid economic growth in the past two decades and the resulting increases in its per capita income have enabled increasing numbers of Chinese citizens to travel and study abroad. China's increased openness to the rest of the world is something that should be celebrated and encouraged. However, evidence has surfaced in recent years indicating that a number of the Chinese tourists and students coming to Taiwan have been given "missions" by the Chinese government beforehand, assigning them to various activities associated with China's United Front strategy against Taiwan.¹⁴ Specifically, many of them have been tasked with propaganda missions to disseminate pro-China, pro-unification, and anti-Taiwan independence messages. Some have been tasked with intelligence gathering missions and instructed to spy on Taiwanese military installations and other sensitive areas related to national defense.¹⁵

Since 2008, the pro-China Taiwanese President Ma Ying-jeou has introduced a series of policies that greatly eased the restrictions previously placed on Chinese tourists, students, and short-term workers. There is no longer an annual quota on the number of Chinese tourists and students that can enter Taiwan. In 2015, there were 10.4 million international tourists visiting Taiwan, of which 5.5 million came from mainland China. In 2015 there are 33,288 Chinese students, including short-term exchange students, studying in Taiwan, which comprises 38% of the total number of international students in Taiwan.¹⁶

The CCP is likely to attempt in Taiwan similar activities that have been part of the long-established policies toward China's ethnic minorities, systematically encouraging and injecting more Chinese migrants into the local areas of Tibet, Xinjiang, and Inner Mongolia. By doing so, the Chinese migrants help to dilute the percentage of local population that are ethnic minorities, and in turn help the CCP government gain greater control over the region.¹⁷

In the case of Taiwan, it is foreseeable that the CCP would exploit any available opportunity to increase the migration of mainland Chinese citizens into Taiwan. If successful, this scheme would increase the number of residents in Taiwan that are more receptive to China's influence, and who are less likely to oppose the CCP's unification strategy.

United Front and its Impacts on the Security of the Asia-Pacific

Ancient Chinese military strategist Sun Tzu believed that winning the hearts and minds of the enemy was more important than attacking their castles.¹⁸ Following this line of thinking, the classical Chinese military tradition stresses that one must first cripple the enemy's desire and will to fight before one attempts to attack the enemy's position. Today, the CCP leadership has clearly attempted to follow Sun Tzu's teaching by spending considerable efforts in exploiting the so-called "soft power" approach to neutralize Taiwan's resistance to the United Front strategy.

China's United Front through the economy has succeeded in attracting massive amounts of capital, resources, technology, and skilled workers from Taiwan in the past two decades.¹⁹ This strategy has also helped to accelerate China's own rapid economic growth, which has helped China's nominal GDP surpass Japan and the European Union. The Chinese economy is now second only to the United States. With over three trillion USD worth of foreign-exchange reserves, China also possesses the largest currency reserves in the world.²⁰

This growth in soft power in the form of economic wealth and foreign-exchange reserves has also enabled China to invest an increasing amount of its resources towards the development of its military, thus converting soft power into hard power. China's military spending has grown at almost double digits in the past 15 years. In 2015, it reached 145 billion USD in published figures alone, which exclude auxiliary or covert expenses such as the upkeep of militia or the research and development of strategically crucial military projects such as stealth technology.²¹ Moreover, with its rapid expan-

sion in military hardware from ballistic missiles to submarine forces, China now poses a huge security threat to the Taiwan Strait and those countries to which it is strategically important, including United States, Japan, Vietnam, and the Philippines, among others.

China also exploits its newly acquired wealth and economic power to purchase large quantities of national debt from the United States, United Kingdom, and other European nations. In acquiring foreign government debts, China potentially gains powerful bargaining leverage over these governments on economic, diplomatic, and strategic issues. For example, China has repeatedly pressured the United States not to include advanced fighter jets and submarines in its arms sales to Taiwan.²² Until recently China has also frequently opposed or blocked attempts by the United States to curb the North Korean nuclear weapon program. All of this demonstrates China's exploitation of the benefits of the United Front strategy in pursuit of its goal of becoming the regional hegemon of the Asia-Pacific.

The experience China has acquired through the implementation of the United Front in Taiwan has helped it to formulate and apply similar operations in the United States.²³ Over the past 15 years, the Chinese government has invited U.S. Congressional members and staffers, retired U.S. Generals and senior officers, business leaders, think tank researchers, and scholars to visit China. As with those from Taiwan, these trips were often generously funded by the Chinese government. The American "guests" would receive lavish receptions so as to foster their positive impressions of the CCP regime, potentially helping influence the foreign policies of the United States.

Another well-documented example of China's use of the United Front strategy targeting the United States is the large number of Chinese-funded "Confucius Institutes" attached to many of the top universities and colleges in the U.S.²⁴ These institutes offer a variety of scholarships and funding to American students who pursue studies in Chinese culture, language, politics, and other related areas. They also actively recruit American teachers, academics, and think tanks to help disseminate messages that are favorable to the CCP through conferences, research, and speeches under the guise of academic activity. It is all just one part of China's extended use of the strategy of the United Front on the global stage.

As mentioned above, the essence of CCP's United Front strategy as conceived of by Mao Zedong is to "collude with the secondary enemy in order to defeat the primary enemy." The CCP also borrowed from ancient Chinese strategic teaching in "befriending the distant enemy while attacking a nearby enemy,"²⁵ a pattern which can be observed from China's behavior in the international

sphere during the Cold War. During the 1970s, China made numerous secret diplomatic overtures to the United States, a country that was at one time its primary ideological enemy. Hoping to recruit Chinese help in containing the Soviet Union in the Far East, the U.S. government provided China with much-needed assistance in developing its own economy and technology. To this end, China allowed the United States to build secret signal intelligence (SIGINT) stations in Xinjiang to monitor Soviet military activities in Afghanistan and Central Asia.²⁶

It is therefore no surprise that in recent years China has made numerous overtures to Ma Ying-jeou's government in Taiwan, seeking to recruit Taiwan to join its United Front against Japan in the dispute over the sovereignty of the Senkaku Islands.²⁷ Similarly, China has also attempted to recruit Taiwan to form an alliance against Vietnam, the Philippines, and United States in territorial disputes in the South China Sea. In most cases, the Taiwanese government has rejected the Chinese proposals and has not yet been entrapped into participating in the United Front.

Policy Recommendations and Conclusion

This article recommends that the Taiwanese government actively reevaluate most, if not all, trade and investment agreements that have been signed and are currently in effect between Taiwan and China.²⁸ Efforts should be made to reduce Taiwan's overreliance on China's market and to reduce trade relations. It must avoid falling into the trap of the "One China common market" that is part of the economic aspect of China's strategy of the United Front. Furthermore, Taiwan should also actively pursue diverse trade and commercial relationships with international partners such as Europe, the United States, Japan, and the ASEAN nations.

The Taiwanese government should seek to renegotiate agreements with China that have been identified as unfair, unjust, and negatively impacting Taiwan's society and economy. For example, Taiwan should consider lowering the number of Chinese tourists that are allowed to enter Taiwan each year, and limit Chinese investments in Taiwan's sensitive industries such as mass media and high tech sectors. With effective enforcement, these regulations can reduce or neutralize China's efforts to control Taiwan's freedom of the press and freedom of speech, and to help mitigate the negative effects of Taiwan's economic reliance on China.

Random security checks and investigations should be imposed on visiting Chinese officials, tourists, family relatives, students, and short-term workers. This will make it more difficult for Chinese agents to infiltrate

Taiwan and conduct covert operations detrimental to Taiwan's society and national security, including intelligence activities or terrorist plots. In the aftermath of the September 11 attacks, the United States has implemented a screening system for incoming foreigners administered by the Department of Homeland Security. Taiwan should consider adopting similar system.

The Taiwanese government should also hold public hearings and conferences to gather useful policy recommendations and advice on national security from experts, NGOs, think tanks, government officials, and bipartisan leaders and representatives. To defeat China's United Front, it is crucial for Taiwanese society as a whole to come together in forming effective responses and defenses against hostile takeover. Open forums will help to forge public consensus and support for policies designed to counter national security threats making Taiwan more resilient in the face of China's United Front strategy.

It is in Taiwan's best interest to preserve freedom of navigation in the Asia Pacific and to maintain peace, prosperity, and stability in the region. Taiwan should therefore work to settle existing sovereignty disputes in the East and South China Sea by actively communicating and cooperating with neighboring countries including the United States, Japan, Vietnam, and the Philippines. Taiwan should also work with these international partners to form effective cooperation on issues such as piracy, terrorism, and humanitarian aid. Doing so will deny China room for manipulation and agitation, thereby neutralizing the negative impacts from China's strategy of the United Front.

Ultimately, a successful defense against China's United Front requires the people of Taiwan to understand what is at stake and to make a concerted effort in preventing further encroachments by China. The international community also has a lot to learn from Taiwan's experience as China increasingly exploits the same stratagem to divide and weaken countries that it perceives as being its strategic rivals. China's United Front is difficult to counter as it seeks to dominate its opponent without firing a shot, but at the same time it also means that a counter-strategy does not require the use of force for it to be effective. As the old saying goes "united we stand, divided we fall." It is time for Taiwan and the countries in the Asia-Pacific to start working together and adopt appropriate defensive measures so that China's United Front will not succeed in dividing and conquering the region.

Ming-shian Tsai (Michael) served as the Minister of National Defense of Taiwan in 2008. Prior to that he had also served as the Vice Minister of National Defense and Deputy Secretary-General of the National Security Council of

Taiwan. Former Minister Tsai was also elected and served as a Legislator for Taiwan's Legislative Yuan for two terms.

Po-Chang (Paul) Huang is a Master's candidate at the Fletcher School of Law and Diplomacy, where he focuses on security issues related to East Asia. Before coming to the United States, Paul worked for The Epoch Times in Taiwan as the Chief Web Editor, where he covered news related to defense and international affairs. He has worked in the policy sector in Taiwan and has also served in the Taiwanese Army.

1. For an analysis on the pattern of China's use of force during this period, see Allen S. Whiting, "China's Use of Force, 1950-96, and Taiwan," *International Security*, 2001, p. 103-131.
2. For a detailed discussion about China's to use of United Front strategy against the United States, see Michael Pillsbury, *The Hundred-year Marathon: China's Secret Strategy to Replace America as the Global Superpower*. Henry Holt and Company, 2015.
3. See Yimou Lee and Faith Hung, *Special Report: How China's shadowy agency is working to absorb Taiwan*, Reuters, Nov 26, 2014, at <<http://www.reuters.com/article/us-taiwan-china-special-report-idUSKCN0JB01T20141127>>.
4. The Chinese catchphrase, "collude with the secondary enemy in order to defeat the primary enemy," has now become a universally recognized quote commonly attributed to Mao, which derived its core idea from his writing in the 1939 article *The Communist*.
5. For an excellent analysis on China's attempts at fostering and colluding with pro-China elements in Taiwan (even inside the pro-independent camp and the DPP), see Parris H. Chang, *Beijing's strategy to 'buy' Taiwan: Coerced unification without firing a shot*, *World Tribune*, Feb 19, 2014, at <<http://www.worldtribune.com/10-beijings-strategy-buy-taiwan-coerced-unification-without-firing-shot>>.
6. 39.7% of Taiwan's total export volume and 18.1% total import volume in 2014 came from China, according to Data from Ministry of Economic Affairs, Taiwan. Cited in Executive Yuan, March 23, 2014. <http://www.ey.gov.tw/state/News_Content3.aspx?n=1DA8EDDD65ECB8D4&s=8A1DCA5A3BFAD09C>
7. Data from Investment Commission (MOEA), Ministry of Economic Affairs, Taiwan. Cited in United News Daily, Feb 21, 2016. <<http://udn.com/news/story/7334/1514633>>
8. For full text of the Anti-Secession Law see <http://english.peopledaily.com.cn/200503/14/eng20050314_176746.html>
9. Article 8 of the Anti-Secession Law specifically stipulates the use of "non-peaceful means" and "other necessary measures" to "protect China's sovereignty and territorial integrity".

10. See European Union's Resolution adopted in April 2005 in response to China's "Anti-Secession Law" at paragraph 33, p. 6, TA(2005)0132, <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2005-0132+0+DOC+PDF+V0//EN>>.
11. 2015 survey done by a Taiwanese think tank that found across-the-board support for eventual independence reached an all-time high of 70.9%. July 2015. P. 42. Taiwan Brain Trust. <<http://www.braintrust.tw/userfiles/files/20150612.pdf>>.
12. Hsu, Chien-Jung. *China's Influence on Taiwan's Media*. Asian Survey 54.3 (2014): p. 515–539.
13. Ibid., p. 532-537.
14. Shiping, Fan. "A political-economic analysis on the impact of the mainland Chinese tourists traveling to Taiwan on the cross-strait relations". 2010, p. 245-290.
15. For example, see a 2015 Taipei Times report by Pan, Jason. "Chinese espionage at military bases increasing." Nov 11, 2015. Taipei Times. <<http://www.taipetimes.com/News/front/archives/2015/11/11/2003632174>>.
16. Hsin-Cheng Li, "90,000 - Record number of international students in Taiwan, mostly from China", Feb 6, 2015, The News Lens. <<http://www.thenewslens.com/post/123283>>.
17. For example, see Ohno Aikra, *Genocide on the Mongolian Steppe: Oral History of the Chinese Cultural Revolution*, Bachi Publishing, 2014, Taiwan.
18. Relevant quote from the Section III of Sun Tzu's *The Art of War*: "...skillful leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field."
19. For example, see Hung, Chia Ko. Taiwan business people's contribution to China's economic development 1979-2008. 2009. Quote: "From 1979 to 2008, Taiwan business people's total direct investment amounted to USD 122 billion, accounted for 14.34% of China's same time total direct foreign investment."
20. Kujundzic, Petar. "China central bank deflects concerns over forex reserves", Reuters, February 28, 2016. <<http://www.reuters.com/article/us-china-forex-idUSKCN0W10PA>>.
21. See National Defense Report 2015 published by Taiwan's Ministry of National Defense (MND). <<http://report.mnd.gov.tw>>. P. 49.
22. For a detailed list of PRC oppositions to US-Taiwan arm sales in recent decades, see a joint report by U.S.-Taiwan Business Council and Project 2049 Institute: *Chinese Reactions to Taiwan Arms Sales*. April 16, 2012. <https://project2049.net/documents/2012_chinese_reactions_to_taiwan_arms_sales.pdf>.
23. See Michael Pillsbury, *The Hundred-year Marathon: China's Secret Strategy to Replace America as the Global Superpower*. Henry Holt and Company, 2015.
24. For an overview of the controversies associated with Confucius Institutes and its connection to China's United Front strategy, see Steven W. Mosher, *Confucius Institutes: Trojan Horses with Chinese Characteristics*, March 28, 2012, Population Research Institute, at <<https://www.pop.org/content/confucius-institutes-trojan-horses-chinese-characteristics>>.
25. As one of the renowned "Thirty-Six Stratagems".
26. John C. K. Daly, *Feature: U.S., China - intel's odd couple*. UPI, Feb. 24, 2001, at <<http://www.upi.com/Archives/2001/02/24/Feature-US-China-intels-odd-couple/6536982990800>>.
27. Dolven, Ben, Shirley A. Kan, and Mark E. Manyin. "Maritime Territorial Disputes in East Asia: Issues for Congress." Congressional Research Service, Library of Congress, 2013. p. 25.
28. The incoming Democratic Progressive Party (DPP) administration has promised to push for a stricter evaluation process and legislative oversight for future Taiwan-China agreements, but remains ambiguous as to the fate of existing agreements.