Global Security and Intelligence Studies
Volume 2, Number 1 - Fall 2016

Table of Contents

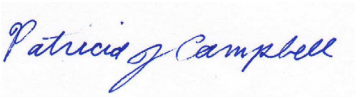
Editorial Welcome

Global Security and intelligence Studies aims to publish high-quality and original research on contemporary security and intelligence issues. The journal is committed to methodological pluralism, and seeks to help bridge the gap between scholars and practitioners engaged in security and intelligence issues by publishing rigorous research, book reviews, and occasional think pieces that are relevant to both communities. We will, on occasion, also seek to publish special issues on timely intelligence and security topics, and welcome proposals that fit with the scope and aims of the journal. The journal actively encourages both former and current intelligence and security practitioners to participate in important scholarly and policy debate, and invites them to contribute their research to the journal. As a result, we hope that the journal will become a vibrant platform for informed, reasoned, and relevant debates on the most important intelligence and security issues of our time.

This issue of GSIS touches on a number of these debates. In *Academic Intelligence Programs in the United States: Exploring the Training and Tradecraft Debate*, Michael Landon-Murray and Stephen Coulthart explore the value of academic intelligence programs to the intelligence enterprise in the United States, and examine what aspects of training and tradecraft can be appropriate for such programs. In *Anonymous Versus ISIS: The Role of Non-state Actors in Self-defense*, Andrew Colarik and Rhys Ball explore the role of non-state actors in cyberspace, and seek to apply Just War principles to the realm of self-defense in cyberspace. Chris Dolan and Alynna Lyon's article, *Calculation of Goodwill: Humanitarianism, Strategic Interests, and the U.S. Response to Typhoon Yolanda*, examines the various rationales behind the American response to Typhoon Yolanda, and offers insights into how the United States gets involved in humanitarian responses to natural disasters. In *An Assessment of Lone Wolves Using Explosive-Laden Consumer Drones in the United States*, Matthew Hughes and James Hess examine the potential impact of the advent of commercially available drones on lone wolf terrorism in the United States. Finally, in their article, *Is China Playing a Contradictory Role in Africa? Security Implications of its Arms Sales and Peacekeeping*, Earl Conteh-Morgan and Patti Weeks assess the contradictory nature of China's peacekeeping efforts and arms sales on the African continent.

Publishing an academic journal is a collaborative process. The editorial team would like to extend its gratitude to the authors, to our peer reviewers for their feedback and commitment, and the members of the editorial board for their support and input.

On behalf of the editorial team,



Yoav Gortzak
American Public University System

Patricia J. Campbell
American Public University System

doi: 10.18278/gsis.2.1.1

Academic Intelligence Programs in the United States: Exploring the Training and Tradecraft Debate

Michael Landon-Murray[A] & Stephen Coulthart[B]

Academic intelligence programs in the United States have grown markedly in the past 15 years. Their value to the U.S. intelligence community (IC) has received some attention in the literature, as has the role of training and tradecraft in those programs. The inclusion of such content has been identified and characterized as a new function of U.S. higher education in support of intelligence. Varied but limited views have been offered on the appropriateness of this sort of instruction in academic programs, a part of the value-added these programs may offer. To address this gap, we interviewed 10 intelligence educators and program directors so that a more inclusive picture of views and practices could be sketched. With their input, which certainly demonstrated variation, and consideration of current IC practice, we explore what facets of training and tradecraft can be appropriate for academic programs and offer recommendations accordingly. The article concludes that the delineation between intelligence education and training may not be so stark, largely because of the educational and social science underpinnings of analytic tradecraft and competencies, as well as various issues in IC training and tradecraft. By better connecting professional practice with social science foundations, academic intelligence programs can help create a better transition from education to training.

Key words: *intelligence education, intelligence analysis, training, tradecraft, professionalization*

Introduction

In the past 15 years, the number of civilian U.S. intelligence degrees has grown tenfold to roughly 30 programs along with dozens of minors and certificates. Before the establishment of these programs, would-be intelligence practitioners tended to come from political science, international affairs, history, regional studies, and other liberal arts programs. Many still do, which points to a key question in the

[A] Assistant Professor, School of Public Affairs, University of Colorado, Colorado Springs
[B] Assistant Professor, National Security Studies Institute, University of Texas at El Paso

[1] For a discussion of curricular facets of academic intelligence programs, see Stephen Coulthart and Matthew Crosston, "Terra Incognita: Mapping American Intelligence Education Curriculum," *Journal of Strategic Security* 8 (3) (2015): 46–68.

doi: 10.18278/gsis.2.1.2

literature and the field: are the new degree programs value-adding features of the U.S. higher education system? Some early research does suggest that the programs are a valuable addition to existing liberal arts programs, but others argue that intelligence agencies may not want to hire applicants with specialized intelligence backgrounds, preferring instead conventional academic backgrounds (Spracher 2009). This latter view is predicated on the assumption that analysts can develop the more technical facets of intelligence analysis through training and professional development.

A closely related issue is the role of training and tradecraft—namely analytical techniques—in U.S. academic intelligence programs. Given the professional orientation of some civilian intelligence curricula, it seems that a blending of training and education might prove to be part of the contributions these newer programs can make. Efforts to better harmonize education and training will require close examination of what facets of analytic tradecraft—and in what measure—could enhance the value-added of academic intelligence programs.

That academic intelligence programs in the United States have incorporated what would be considered training and tradecraft has been observed in the literature (Marrin 2009). This study will drill down into that "blurring" to get a sense of how broadly it is occurring and what form(s) it is taking. It is informed by interviews with 10 U.S. intelligence educators, several of who established and now direct intelligence programs. This is a group that has not been asked to comment on these specific issues, despite their wealth of knowledge and experience. We discussed with interviewees whether or not they feel this sort of content is useful in preparing students for intelligence careers, what instructional areas they offer in this realm, what they consider to be the more unique approaches taken in their programs, and what key facets differentiate academic intelligence programs.

We found that intelligence educators and program directors in U.S. higher education take differing views and approaches regarding training and tradecraft instruction. Some put the role of training at the center of their mission, while others disavowed it quite strongly—though often with exceptions and qualifications, which we will explore. When asked about the presence and nature of training and tradecraft in their programs, study respondents frequently cited structured analytic techniques (SATs). The article concludes that the delineation between intelligence education and training need not be so stark, largely because of the educational and social science underpinnings of analytic tradecraft and competencies, as well as various issues in IC training and tradecraft. By better connecting professional practice with social science foundations, academic intelligence programs can help create a better transition from education to training. It is important to note that our findings speak only to the U.S. context and are not definitive conclusions, although certainly the output of a diverse sample. Future research will need to determine whether these observations are present in other countries.

Before moving to the findings section, the relevant literature will be surveyed. This entails the views and opinions registered to date on the teaching of intelligence tradecraft in academic programs, as well as related empirical findings. What training and tradecraft mean, in practice, in the IC will then be briefly explored, as well as

related training and tradecraft issues and shortcomings. This will help us to frame the findings and discussion sections that follow. Having explored the parameters of training and tradecraft in various ways, we then consider what specific facets are and/or can be addressed by academic programs. This is informed by our interviews and more general considerations about the educational underpinnings of intelligence tradecraft. Some recommendations will also be made.

Literature Review

Perspectives and Findings on Intelligence Training in Higher Education

The growth of intelligence degrees in the United States has been rapid in the post-9/11 era. Currently, there are roughly 30 such programs in existence, based on a search done by the current authors. This number seems to have continued growing in recent years and through the present (Coulthart and Crosston 2015). Given the central place the study of intelligence practice and process has taken in academic degree programs, more space is afforded for specialized content. It is this content that degrees in political science, international affairs, regional studies, and other areas cannot focus on in as much depth.

To be sure, there are critics of these programs. Mark M. Lowenthal, for example, has voiced the opinion that intelligence should not be a major, only a minor (Lowenthal 2013a). Similar sentiments were found in William C. Spracher's interview research (Spracher 2009). For example, Arthur Hulnick commented that intelligence studies should not be a "distinct program," but instead "integrated with other liberal arts subjects" (Spracher 2009, 103). Others have suggested that the analytic profession requires degrees with an explicit focus on intelligence analysis (Hendrickson 2013). Such programs emphasize a generalist approach, intending to produce graduates who have the ability to move in and out of different intelligence accounts.

These perspectives suggest a practitioner-oriented skill set, on the one hand, and a broader academic approach, on the other hand. How the more applied and practical facets of academic programs bleed into the realm of training and tradecraft remains to be explored, both conceptually and empirically. Broadly conceptualized, tradecraft, a term now used in both operational and analytical contexts, refers to the tools and methods used by intelligence practitioners to execute their responsibilities. Our focus here is on the analytical, as the tools of espionage are surely beyond the domain of higher education.

In the IC, the tools and methods of tradecraft are developed through professional experience, socialization, and development and, as we will see shortly, increasingly training. Distinguishing intelligence training and education, Stephen Marrin has made the following observation:

> In terms of intelligence analysis, the term "training" is usually associated with internal government programs intended to provide specific instruction for the implementation of job-related tasks, while the term

> "education" is normally associated with academic courses or programs geared to provide more conceptual and theoretical frameworks having less immediate effect on performance, but layering the foundation for improved performance over the longer term. (Marrin 2009, 131)

Varying—though limited—views have been registered on the issue of incorporating training into academic programs, as we will see. But, regardless of these differing views, Marrin suggests a fundamentally new facet of intelligence education has emerged: the introduction of training and tradecraft into academic programs (Marrin 2009).

Some, including Jennifer Sims and Martin Rudner, have commented that tradecraft is not well-advised to be in the purview of intelligence studies programs and is best addressed through professional training (Rudner 2009; Spracher 2009). Sims has observed, "We definitely should not be teaching tradecraft and professional practice," though does see a role for professional schools (Spracher, 2009, 118). Martin Rudner has similarly written

> What are the objectives of Intelligence and National Security Studies in higher education? Certainly not to provide training in actual intelligence tradecraft. That is something best left to the national Intelligence and Security Community itself. (Rudner 2009, 116)

Others have discussed perspectives and practices that seem more in line with training and instruction in tradecraft. Spracher found that intelligence curricula and courses do a relatively good job of addressing intelligence core competencies, as laid out by the Office of the Director of National Intelligence (ODNI) (Spracher 2009). These competencies include engagement and collaboration, critical thinking, personal leadership and integrity, accountability for results, technical expertise, and communication. The programs Spracher examined did not speak equally well to the different competency areas, however—engagement and collaboration, personal leadership and integrity, and accountability for results did not receive as much treatment as the others.

Spracher also surveyed newer IC analysts to investigate how well their academic preparation helped them to meet IC core competency standards. Respondents said that their academic backgrounds were less effective in preparing them in the competency areas of engagement and collaboration, and technical expertise (which includes professional tradecraft). Recognizing the difficulty of learning some of the core competencies in the classroom, Carl J. Jensen has suggested the IC consider establishing a university-based intelligence training corps similar to the military's Reserve Officers' Training Corp (ROTC) model (Jensen 2011).

Both Spracher and Jensen see a place for training and tradecraft in academic intelligence programs. Similarly, James G. Breckenridge has suggested that, when properly prepared, new graduates of intelligence degree programs

> [M]ay be able to test out of or spend less time in basic courses offered by the IC, and resources can be redirected to advanced and career IA [intelligence analysis] courses. The question then becomes how best to prepare students for eventual work in the IA community and, at the same time, reduce the burden of training for the IC? (Breckenridge 2010, 320–321)

What such content can and should be remain quite open questions, and this article will give a better, if preliminary, sense of what university intelligence educators do, and feel comfortable doing, in the realm of training and tradecraft.

Training and Analytic Tradecraft in the U.S. Intelligence Community

As William C. Spracher observes, intelligence tradecraft can mean quite different things to different stakeholders and organizations (Spracher 2009). In his 2005 ethnographic study of analytic culture and practice in the U.S. IC, Rob Johnston found analytic tradecraft to be a "catchall" term for a wide range of "idiosyncratic" techniques (Johnston 2005). In fact, Johnston objects to the use of the term tradecraft to describe analytic methods. To him, such terminology suggests mysterious, inscrutable techniques—and perhaps an effort to bolster prestige vis-à-vis intelligence collection and operations. But rather than an opaque process not accessible to outsiders, analytic tradecraft shares many creative features of social science research, such as hypothesis generation and refutation (Johnston 2005).

While analytic tradecraft could in some ways be a misnomer, it should probably not be surprising that analytic techniques were so divergent in the IC that Johnston studied (it seems they still are). Formal analytic training in the IC is still a surprisingly new phenomenon, with the Central Intelligence Agency (CIA) first introducing more extensive approaches in just the last two decades (Marrin 2003). As of 2003, CIA analytic training stressed critical thinking, writing and briefing, collaboration, the business of intelligence, organizational issues, and agency history and values. It provides introductions to other intelligence functions and emphasizes the works of Richards J. Heuer and Sherman Kent. Kent's "Principals for Intelligence Analysis" include a number of facets that would connect rather comfortably to the IC's current Analytic Tradecraft Standards, including efforts to bolster intellectual rigor, avoid bias, consider alternative judgments, and recognize personal and analytical shortcomings (Marrin 2003).

Other agencies have certainly followed suit (Campbell 2011; Marrin 2003) and the National Intelligence University has expanded its offerings (Spracher 2016). However, regarding the various IC programs in this area, James B. Bruce and Roger Z. George have commented:

> Individual agency-developed training programs vary enormously in scope, depth, duration, and quality; some agencies support new analyst training for several months and some shorter mid-career courses in

> advanced analysis that qualify analysts for more senior positions, while other agencies offer almost none or very tailored training that does not directly support a well-rounded, "complete" analyst. Such professional development seems at best implicit and ad hoc. (Bruce and George 2015, 7)

In addition to more formalized, extensive analytic training, the IC has increasingly stressed a range of techniques—generally labeled SATs—as well as new analytic standards and competencies. These efforts have essentially been part and parcel of the introduction of the ODNI. The Analytic Tradecraft Standards, a core facet of Intelligence Community Directive (ICD) 203, require analysts and agencies to address issues of quality, credibility, and uncertainty; make assumptions explicit and consider the implications of those assumptions being incorrect; differentiate assumptions from information; explain conditions of change and continuity; apply alternative analyses; and present products that employ likelihoods, are customer relevant with key information upfront, and contain logical, accurate judgments.

ICD 203 is intended to "govern the production and evaluation of analytic products" in the IC (Office of the Director of National Intelligence 2015, 1). The standards represent the "core principles of intelligence analysis and are to be applied across the IC" (Office of the Director of National Intelligence 2015, 1). They are also meant to inform IC approaches to analytic education and training.

The SATs devised for use in the IC can generally be categorized as contrarian, imaginative, or diagnostic techniques (Central Intelligence Agency 2009). These techniques include the following: brainstorming, key assumptions check, devil's advocacy, quality of information check, brainstorming, team A/team B, indicators and signposts of change, high-impact/low-probability analysis, what if analysis, analysis of competing hypotheses, outside-in thinking, red team analysis, and alternative futures analysis (Central Intelligence Agency 2009). The use of SATs seems to vary across the IC. Federal Bureau of Investigations analysts are required to demonstrate some use of SATs for promotional advancement (Gentry 2015) while other IC elements use SATs very minimally (Coulthart 2016).

The ICD 610 series sets out core competencies across a range of intelligence occupations and positions. The baseline set, used by Spracher in his study of academic intelligence curricula, was presented above. The competency set for analysis and production include understanding collection systems capabilities and customer operations and requirements (Arant Kaspar 2014). Processing and exploitation, research, and tools and methods round out this competency set (Arant Kaspar 2014).

Criticisms and Concerns: U.S. Analytic Training, Tradecraft, and Standards

Some have voiced skepticism about current IC analytic training, and the tradecraft that training tends to focus on, as well as propositions relating to analytic professionalization. Matthew Herbert has suggested that contemporary intelligence analysis, specifically in the U.S. context, is so varied as to defy efforts at a clean, uniform

professional model (Herbert 2013). To Herbert, such efforts are more connected to academic compulsions and excesses around precise definitions than meaningful avenues to improved intelligence analysis. John A. Gentry has observed

> The concern about analyst professionalization seems related to the reasonable perception that many contemporary analysts do in fact need the basic training provided by entry courses on 'tradecraft,' including SATs. My conclusion is that the professional credentials and tradecraft skills of the analyst corps have deteriorated appreciably in recent years, leading to a perceived need to address deficiencies with unorthodox techniques of questionable utility. (Gentry 2015, 651)

As it stands, "No codified process for entry into the profession, standards in terms of educational requirements, professional development processes, or ways to accumulate and transfer knowledge from generation to generation currently exist" (Marrin 2009, 139). Bruce and George similarly observe that the IC is only in the most rudimentary stages of establishing intelligence analysis governing bodies, institutionalizing robust education and training, developing certification requirements, standardizing analytic methods, managing knowledge, and cataloguing best practices (Bruce and George 2015).

Chang and Tetlock are critical of IC analytic training that they characterize as focusing on certain analytic issues (at the expense of others) and the SATs intended to address those issues (Chang and Tetlock 2016). They write, "The *Psychology of Intelligence Analysis* was groundbreaking for its time, but revisions are now necessary" (Chang and Tetlock 2016, 3). Contemporary IC training and tradecraft are seen as overly concerned with countering analytic over-confidence and rigidity, while essentially ignoring other biases, such as under-confidence and volatility.

As alluded to above, SATs are also seen as lacking scientific, empirical demonstration, and likely to introduce new issues and problems (Chang and Tetlock 2016; Gentry 2015). John A. Gentry has suggested that SATs may have their best application in helping junior, inexperienced analysts avoid basic mistakes, some of which stem from a lack of social science foundations (Gentry 2015). To Gentry, SATs are largely social science methods in disguise—a view our intelligence educators reiterated below. In his view, SATs can be seen as a stealth effort to "address an anti-intellectual streak in the analyst corps that finds academics and academic methods unattractive" (Gentry 2015, 651).

Chang and Tetlock also point to the limited evidence available relating to the successful transfer of training to on-the-job performance (Chang and Tetlock 2016). They conclude, "For too long the intelligence community has shackled itself to a system of training that it never tested – and that almost certainly does not deliver promised performance benefits" (Chang and Tetlock 2016, 14).

James Marchio has found that the IC has used many of the analytic standards and tradecrafts set out by the Intelligence Reform and Terrorism Prevention Act and the ODNI, including ICD 203, dating back to the early Cold War era (Marchio

2014). While this use has been intermittent and thus sometimes limited, Marchio demonstrates that most of the ICD 203 analytic standards were present in analytic products from the early years of the IC through the 1990s. While the IC does have a history of establishing groups to evaluate the value and accuracy of analytic products (Marchio 2014), John A. Gentry has noted that the current IC does not, in a systematic way, evaluate the accuracy standard (Gentry 2015). Thus, analysts can meet all other standards while still falling short, and not being measured, on perhaps the key standard. Doing so would no doubt be extremely challenging, to be sure. Mark M. Lowenthal has similarly commented that ICD 203 and sourcing requirements can place more emphasis on process than content, putting sometimes unhelpful requirements and restraints on analysts (Lowenthal 2013b).

Study Methodology and Data

We do not think of our sample as representative—though our sampling was designed to include diverse perspectives and programs—but more as a "roundtable" of educators who, to date, have not been queried in a focused way on this important topic. We do not offer definitive conclusions to these questions and issues, but rather seek to move the dialogue forward in a more inclusive, empirical fashion. The intelligence educators and program directors we interviewed come from graduate and undergraduate programs, online and brick-and-mortar schools, programs with minors to standalone degrees, and the east and west coasts—and several places in between. Our purposive sampling was intended to make our group of 10 as diverse in perspective as possible, asking each participant to name individuals who approach and view intelligence education differently than they do. It is also important to note that we are focused only on the U.S. context, and findings about practice and perspectives would surely vary in other parts of the world.

Training and Tradecraft: Views and Practices from Higher Education

In our conversations, each of the 10 intelligence educators and program directors were asked, among other questions, what aspects of their program's approach or offerings could be characterized as training or tradecraft. Many respondents asked what we meant by those terms. Prior to beginning our interviews, we made the decision to defer to their views and examples, allowing them to set the terms rather than us. We felt that this would allow for a more organic picture to emerge. Respondents also discussed the role of training and tradecraft more generally, the unique approaches found in their programs, and what attributes distinguish different types of academic intelligence programs.

Not surprisingly, interviewees from various kinds and levels of programs stressed the educational role of their programs, while often also assigning training a role, be it large or small. Some said that as a matter of policy, they do not engage in training or instruction on analytic tradecraft, though often with caveats such as providing introductions to or needed methodological foundations in analytical

techniques. The following quotes demonstrate variations or points along this spectrum, with some fully disavowing training and others fully embracing it.

> *We make it specific that we don't do training.*

> *We really don't [do training]…I'm a firm believer in education, not the training side…We tend to stray away from the training aspect because… that piece is far less enduring than…the educational piece.*

> *We don't want to be, and we're not good at, training them to do exactly what the CIA does in certain analytic tradecraft…So we expose them to it, but, really the emphasis is getting back to the liberal arts, social science methodology type emphasis we have.*

> *No, we're very academic-oriented…they get real-time work, there's a training aspect in that they learn the important things, the basics, and the advanced techniques for analysis and research…they do learn about writing for intelligence…otherwise it's a full academic program…the graduate program, purely academic.*

> *Our program is an academic program, but it still has that practical, what I would call training, aspect to it. I find it to be, I would say, a very good combination of traditional training and academics.*

A number of respondents viewed certain (other) programs as being heavily, even fundamentally, training-oriented, and as the quote immediately above demonstrates, some openly took on that identity. These programs were described as focusing on analytic tradecraft to be applied to "hands-on," "hard" security issues and problems, a key distinction some interviewees noted between different kinds of academic intelligence programs. Some of our respondents praised this approach, though more were critical. Some called this a philosophical difference and were also skeptical about how the IC viewed such programs. Along these lines, some of our respondents said:

> *Unlike many, my impression is most programs, we are not following, "let's pump out fully trained intelligence analysts out the other side"…that was done strategically, the notion being that that doesn't go over super well with employers.*

> *Theirs is far more hands-on, OJT [on-the-job-training] type stuff. They're just going to get you ready to start the job…we resist that tendency, that push.*

Most of the intelligence educators we spoke with would not suggest that their program is intended to produce immediately job-ready intelligence professionals.

Some respondents told us that "bottonology" is more perishable than educational and social science foundations and that their students will be more employable if they also specialize in a substantive area (meaning regional or functional). These educators seek to inculcate skills and mentalities that will transcend specific agency training and culture. To be sure, some programs do introduce their students to explicit analytic methods and tools, such as the software program Analyst's Notebook, as early as their freshman year. Others "specifically look at, how does one perform the functions of an intelligence officer, at the undergraduate level." And even those who were skeptical of the role of training and tradecraft cast some of their programs' aspects in those terms. One such respondent, speaking about a graduate-level course in intelligence analysis, commented it had

> *[S]trong elements of both training and education to it. There is a lot of discussion of secrets versus puzzles versus mysteries…and let's do it in groups because that's how things work in the real IC…that is probably our most directly, training-like…no-kidding practical course.*

Our discussions about specific curricular facets that intelligence educators considered to be training- or tradecraft-centered frequently turned to SATs, often coupled with critical thinking and/or social science methodology. So, while the efficacy of such techniques remains something of an open question, among other noted issues, SATs (with caveats) have been incorporated into some civilian intelligence education programs. For example, one graduate-level faculty member told us

> *The closest we get to training is, we teach structured analytic techniques… but it's not so much to train them to use it, as it is to complement what we do. We do research methods, so, social science methodology. I do a lot of critical thinking…in my courses.*

Similar to the above quote, several other respondents highlighted teaching the fundamental social science methods or theory underlying SATs and critical thinking. The emphasis on social science frames more than practical application was seen to some as a key difference between intelligence education and training programs. This addresses an issue that has been noted by many in recent years, namely that intelligence programs and professionals lack needed social science foundations (Collier 2005; Gentry 2015; Landon-Murray 2011; Marrin 2012). The emphasis placed on social science methods by our interviewees suggests that academic programs are addressing these competencies, certainly a positive indicator. A couple educators suggested that SATs really fall into social science and educational domains. Along these lines, other respondents added:

> *We certainly do talk about SATs and the methodologies related to intelligence analysis, but we're not talking about specific software packages…I guess you could argue that some of the specific techniques…*

could be construed to some degree as training. But I think at the end of the day, because those are problem-solving skill sets, they really still are pretty much in the education basket.

They [methods courses] are somewhat related to stuff that's in Structured Analytic Techniques…but, for example, hypothesis testing is a course, and it's not ACH [Analysis of Competing Hypotheses], it's hypothesis testing, it's a more fundamental approach...

I don't…consider [any offerings] training in nature only because we can't teach tradecraft in our open source courses…they'll teach of course critical thinking techniques…these are all things that are all open source and nothing specific to tradecraft training.

We go into the theoretical side of critical thinking…we teach critical thinking almost as if it's the scientific method…they get that background and then when they're doing the case studies that we teach them, we're always adding different material that has a theoretical basis that you wouldn't see in a training course.

An educator from a university that had received Intelligence Community Centers for Academic Excellence (ICCAE) funding told us that while their program began teaching SATs on their own, they received signals and guidance from the ICCAE program office on the inclusion of SATs in academic courses. The respondent found the ICCAE workshops and seminars extremely helpful. Other ICCAE events for intelligence educators served to encourage the establishment of additional academic programs.

Writing and communicating competently for a professional intelligence context was another area that a number of our respondents addressed, in some cases with the IC explicitly stating its importance to program directors. One respondent told us simply that intelligence agencies want people who know how to write well—a challenge many educators are probably well aware of. The building of these competencies was a frequent focus across programs. This included a current intelligence briefing club explicitly modeled on IC practice (this became a course), an express focus in each class on intelligence writing, and the completion of "real intelligence type work" that can include written and oral briefings for actual consumers in various sectors. Some of those we spoke with differentiated academic programs on the basis of the role accorded to writing for professional intelligence uses.

A number of other instructional areas were identified when we asked what programmatic aspects were considered to be associated with training and tradecraft. This included coursework in open source intelligence, security operations and management, counterintelligence, financial investigations, intelligence collection and collection management, and cyber operations. But, these areas, like SATs and critical thinking, were often mentioned with similar caveats.

Discussion

Now that we have discussed training and tradecraft as conceptualized and practiced in the IC, as well as the views and practices of intelligence educators in U.S. colleges and universities, we will discuss what facets of training and tradecraft academic programs can address. We are guided by intelligence educators' input and more generally what comfortably seems to fit in the educational realm. In this way, the new class of U.S. intelligence programs may move closer to realizing their full contribution to higher education and the IC. By considering what facets, and in what measure, can be broached in an academic setting, we also move closer to populating the instructional areas that may be used to transfer some content from IC training to higher education, as James G. Breckenridge has suggested.

As we have seen, analytic tradecraft, in practice, has been found to be idiosyncratic (Johnston 2005) and more extensive analytic training in the IC is still a relatively recent, limited, and flawed phenomenon (Bruce and George 2015; Campbell 2011; Chang and Tetlock 2016; Marrin 2003; 2009). Additionally, the practice of intelligence analysis shares key characteristics with social science methodology (Johnston 2005; Office of the Director of National Intelligence 2015). This all suggests that analytic training and tradecraft may not be so specialized, or frankly, special, and not necessarily beyond the capacity of academic programs. And as we have seen, some programs and educators have embraced training and tradecraft, and several in our sample said some programs have fully crossed into that territory. As one educator told us, exemplifying what was certainly one of the most training-oriented approaches:

> *The idea is that what we wanted to produce was somebody who had the skills to actually produce intel…it's like an engineering program…we provide our students with the tools that they need for their toolkit, we give them the practical experience, and when they graduate they walk out the door and they're ready to build intelligence…*

SATs seem to have taken on a noticeable role in academic intelligence programs, often with an emphasis on the social science techniques that underpin them. This seems like an especially ripe area for the IC and higher education to cooperate around in order to design a more purposive approach to teaching students these techniques and their foundations. This would not only promote a deeper understanding of SATs, and continually reinforce that understanding, but could also help support a better shared understanding of SATs and address issues that both trainers and educators find problematic. On this latter point, IC trainers will, in certain cases, be apprehensive about the tradecraft instruction students are receiving, and could be well-served by a voice in that instruction. This may be somewhat attenuated by the reality that many instructors in intelligence programs and courses are former intelligence professionals (Smith 2013). Conversely, the shortcomings and blind spots of SATs can be more explicitly recognized and covered. This would—and does—also afford an opportunity to demonstrate and teach the practical importance of rigorous social science methods, countering both the

limited knowledge of social science methodology (Gentry 2015; Marrin 2012) and the perceived anti-intellectualism in the IC's analytic corps (Gentry 2015; Lowenthal 2013b).

There are several other skill sets and competencies found in IC training and tradecraft that would seem to fit well into the purview of academic education. These include grappling with uncertainty in assessments and findings, the explicit recognition of assumptions (and their limits, contingencies), separating those assumptions from information, working to manage personal and analytic shortcomings, thinking carefully about the quality of information and methods, and thinking about alternative views and possibilities. It is hard to imagine any educator suggesting it would be acceptable for students to graduate without these skills, regardless of their discipline and career intentions. However, the broad value and impact of higher education for students and society has come under increased scrutiny in recent years (Arum and Roksa 2010; Berg and Seeber 2016; Ginsberg 2011). Perhaps the most common concern is that the "administrative bloat" of higher education has diminished in different ways the role of faculty members, with important implications for students (Berg and Seeber 2016). If students are leaving academic intelligence programs with these competencies well-developed, however, they will have a head start on key IC tradecraft and standards and will be better positioned to learn others and practice them in the longer term.

These types of skills and competencies—and mindsets, really—are not always expressly reflected in the current standards of the International Association for Intelligence Education (IAFIE). IAFIE standards are largely the same for graduate and undergraduate programs, with standards for the former increasing "depth and rigor in the instruction of" undergraduate outcomes (International Association for Intelligence Education 2011). Thus, as academic programs seek guidance or certification from the association, such outcomes and objectives may not be given a central role in intelligence curricula. And while US IC-emphasized competencies and practices should, of course, not drive IAFIE academic standards, they can contain rather basic guidelines for the improved conduct of intelligence analysis. IAFIE members and officers might, over time, arrive at additional standards by engaging stakeholders on an international basis. Any such standards could deviate from professional intelligence communities when those competencies or practices are found to have important limits or not to be appropriate for academic programs. Examining those limits can also be important, helping future practitioners identify potential pitfalls. These standards might be revisited somewhat regularly as knowledge grows.

A number of additional initiatives could be pursued, or extended, to help integrate this and other content into academic programs in a broad, successful way. The IC could expand its reach to schools outside of the ICCAE program, providing guidance and even training to academic intelligence educators. Our respondents involved in ICCAE spoke positively of ICCAE (and other IC) events and trainings. An expanded, more inclusive approach of this kind may also prove successful. Additionally, the IC could certify intelligence educators to indicate their ability to teach to IC standards and practices. Likewise, the IC, perhaps via the ODNI, could help establish or certify certain courses—for example, pre-professional training in analytic methodologies, writing, and sourcing practices.

Measures of this kind would seem a necessary step for the sort of waiver system promoted by James G. Breckenridge (Breckenridge 2010). Such steps would also be a good complement to what Carl J. Jensen has suggested on a collegiate intelligence corps (Jensen 2011). One can imagine practical limits and reasons not to do these things—for example, many enrolled students would not likely end up in the IC. However, such measures could help those students who do go on to intelligence careers better develop and retain key skill sets, while also inculcating the shared language, understanding, and identity that initiatives like Analysis 101 are meant to accomplish (but may not, for example, if intelligence agencies opt not to participate).

However, there will likely be instances when intelligence educators resist the teaching of certain analytic tradecraft, even if it is endorsed by the IC. As Chang and Tetlock have pointed out, IC training may not reflect the most current, complete understanding of analytic process and related insights (for example, from psychology) (Chang and Tetlock 2016). Thus, intelligence curricula and educators can likely maintain instruction and coursework more continually up-to-date than their professional counterparts. This will raise awareness and skills in intelligence analysts that may be missing in IC-wide and agency-specific training. Speaking to this sort of independence, one of our respondents told us that their approach to instruction on intelligence analysis is "not drawn from the IC's understanding of how to do intelligence analysis."

Even across specific INTs and analytic positions, there are unifying frameworks and techniques that are applicable. It may be in the successful use those frameworks and techniques that more robust analysis will emerge—or not, in their absence. These, for example, could include the IC's Analytic Tradecraft Standards, which certainly have some critical roots in social science methodology. It is a possibility that the particulars and technicalities of the specific INTs could serve to obscure the use of the more broad, underlying facets of analytic tradecraft. And as Bruce and George have written, analytic training is quite varied in the IC and could be prone to underemphasizing certain content and approaches (Bruce and George 2015).

A key, then, is finding an appropriate middle ground between training and education, and then within training and tradecraft, in academic programs. It is toward this middle ground that this article has sought to help us move; although as more specialized intelligence degrees emerge in areas like geospatial and cyber intelligence, this navigation and balance will be further challenged. Again, the full realization of the benefits afforded by academic intelligence programs will depend on how these programs are designed. It is very difficult to imagine a graduate degree in geospatial intelligence analysis that does not get heavily into training and tradecraft.

We believe that conventional education and training can be melded in ways that do not erode either, but in fact strengthen both. Other professions employ such an approach (Finckenauer 2005), and a more purposive combination should come with long-term professional development and performance benefits. The input from the 10 intelligence educators we spoke with, on net, tended to agree. Of course, there were different views about the degree to which programs should take on a more professional coloring, with some seeing their role as providing needed foundations and others as

getting a jump on IC training. Several of our respondents noted an aversion to training but still described training-like program features.

Conclusion

This article has been an effort to clarify the views and practices of those teaching in civilian intelligence curricula in the United States regarding the role of training and tradecraft in their (and other) programs. As we built our sample, we purposefully sought out varying viewpoints based on asking interviewees who they think views and approaches intelligence education differently than they do. So, although comprising 10 interviewees, our sample was constructed to be inclusive of the constructs and views of the broader intelligence education community.

This study has confirmed that in concept and in practice, the delineation between intelligence education and training may not be so stark. It has also argued that there is good reason for this. As has been discussed, analytic tradecraft and competencies sometimes fit into the "education basket" and have important foundations in social science. There are also noted limits and gaps in IC training and tradecraft, and academic programs can provide a venue for future intelligence practitioners to get sensitized to such issues. When academic programs take on appropriate facets and fundamentals of training and tradecraft, they can more explicitly connect professional practice with social science foundations, counter the uneven nature of IC training, and make explicit key issues and problems in contemporary tradecraft (such as those identified by Chang and Tetlock 2016). In general, colleges and universities can help create a more seamless transition from intelligence education to training.

A number of possible steps that might help academic intelligence programs better prepare graduates for careers in the IC have been outlined, and some represent a complement to the current ICCAE program. But more than anything, our hope was to offer a somewhat inclusive empirical look at a topic that has thus far received only passing comments in the literature. Ours is just a single set of findings, but one capturing the views of 10 intelligence educators—including what could be considered thought or industry leaders. It is our hope that such conversations will continue and help keep important issues out front and out in the open. This will propel the continual enhancement and refinement of academic programs meant to prepare America's next generation of intelligence professionals.

Acknowledgments

We would like to share our deep appreciation to those who spent time talking with us for this study, and thanks to the anonymous reviewers who helped us to improve this article in important ways.

References

Arant Kaspar, Wendy. 2014. "Information Survival Skills for Students in Intelligence Studies and International Affairs." *International Security Studies Section of the International Studies Association Annual Conference*, Austin, TX, November 14–16, 2014. http://web.isanet.org/Web/Conferences/ISSS%20Austin%202014/Archive/695023c0-10b5-481c-b625-22c442428931.pdf

Arum, Richard, and Josipa Roksa. 2010. *Academically Adrift: Limited Learning on College Campuses*. Chicago, IL: University of Chicago Press.

Berg, Maggie, and Barbara Seeber. 2016. *The Slow Professor: Challenging the Culture of Speed in the Academy*. Toronto: University of Toronto Press.

Breckenridge, James G. 2010. "Designing Effective Teaching and Learning Environments for a New Generation of Analysts." *International Journal of Intelligence and CounterIntelligence* 23 (2): 307–323.

Bruce, James B., and Roger George. 2015. "Professionalizing Intelligence Analysis." *Journal of Strategic Security* 8 (3): 1–23.

Campbell, Stephen. 2011. "A Survey of the U.S. Market for Intelligence Education." *International Journal of Intelligence and CounterIntelligence* 24 (2): 307–337.
Central Intelligence Agency. 2009. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence.

Chang, Welton, and Philip E. Tetlock. 2016. "Rethinking the Training of Intelligence Analysts." *Intelligence and National Security* 31 (6): 903–920.

Collier, Michael W. 2005. "A Pragmatic Approach to Developing Intelligence Analysts." *Defense Intelligence Journal* 14 (2): 17–35.

Coulthart, Stephen. 2016. "Why Do Analysts Use Structured Analytic Techniques? An In-depth Study of an American Intelligence Agency." *Intelligence and National Security* 31 (7): 933–948. doi:10.1080/02684527.2016.1140327.

Coulthart, Stephen, and Matthew Crosston. 2015. "Terra Incognita: Mapping American Intelligence Education Curriculum." *Journal of Strategic Security* 8 (3): 46–68.

Finckenauer, James O. 2005. "The Quest for Quality in Criminal Justice Education." *Justice Quarterly* 22 (4): 413–426.

Gentry, John A. 2015. "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and CounterIntelligence* 28 (4): 637–661.

Ginsberg, Benjamin. 2011. *The Fall of the Faculty: The Rise of the All-Administrative University and Why it Matters*. New York: Oxford Press.

Hendrickson, Noel. 2013. "Intelligence Analysis as an Academic Discipline: A National Security Education and Recruitment Strategy for a Long-Term Environment of Limited Resources." *American Intelligence Journal* 31 (2): 23–27.

Herbert, Matthew. 2013. "The Motley of Intelligence Analysis: Getting over the Idea of a Professional Model." *International Journal of Intelligence and CounterIntelligence* 26 (4): 652–665.

International Association for Intelligence Education. 2011. "Standards for Intelligence Education." http://c.ymcdn.com/sites/www.iafie.org/resource/resmgr/docs/iafie_intelligence_education.pdf.

Jensen, Carl J. 2011. "The Intelligence Officer Training Corps: An ROTC-style Program for the IC." *International Journal of Intelligence and CounterIntelligence* 24 (4): 733–746.

Johnston, Rob. 2005. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. Washington, DC: Center for the Study of Intelligence.

Landon-Murray, Michael. 2011. "Social Science and Intelligence Analysis: The Role of Intelligence Education." *Journal of Applied Security Research* 6 (4): 491–528.

Lowenthal, Mark M. 2013a. "Intelligence Education: Quo Vadimus?" *American Intelligence Journal* 31 (2): 7–11.

Lowenthal, Mark M. 2013b. "A Disputation on Intelligence Reform and Analysis: My 18 Theses." *International Journal of Intelligence and CounterIntelligence* 26 (1): 31–37.

Marchio, Jim. 2014. "Analytic Tradecraft and the Intelligence Community: Enduring Value, Intermittent Emphasis." *Intelligence and National Security* 29 (2): 159–183.

Marrin, Stephen. 2003. "CIA's Kent School: Improving Training for New Analysts." *International Journal of Intelligence and CounterIntelligence* 16 (4): 609–637.

Marrin, Stephen. 2009. "Training and Educating U.S. Intelligence Analysts." *International Journal of Intelligence and CounterIntelligence* 22 (1): 131–146.

Marrin, Stephen. 2012. *Improving Intelligence Analysis: Bridging the Gap Between Scholarship and Practice*. London: Routledge.

Office of the Director of National Intelligence. 2015. *Intelligence Community Directive 203: Analytic Standards*. Washington, DC: Office of the Director of National Intelligence.

Rudner, Martin. 2009. "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand." *International Journal of Intelligence and CounterIntelligence* 22 (1): 110–130.

Smith, Jonathan. 2013. "Amateur Hour? Experience and Faculty Qualifications in U.S. Intelligence Courses." *Journal of Strategic Security* 6 (3): 25–39.

Spracher, William C. 2009. "National Security Intelligence Professional Education: A Map of U.S. Civilian University Programs and Competencies." Doctoral dissertation, The George Washington University, Washington, DC.

Spracher, William C. 2016. "Intelligence Education as Envisioned by the National Intelligence University: Emerging Certificates, Concentrations, and Offsite Academic Centers to Complement Accredited Degree Programs." *International Studies Association Annual Conference*, Atlanta, GA, March 16–19, 2016. http://web.isanet.org/Web/Conferences/Atlanta%202016/Archive/e5737ddb-dba0-4e29-a78d-01f03efdff1c.pdf.

Anonymous Versus ISIS: The Role of Non-state Actors in Self-defense

Andrew Colarik[A] & Rhys Ball[B]

The use of cyberspace by terrorist organizations for command and control activities, recruitment and the dissemination of training materials is of ongoing concern for state actors. This is especially true because the nature of cyberspace makes efforts to limit and/or eliminate it exceedingly difficult. With the emergence of non-state actors such as the Islamic State of Iraq and Syria (ISIS) openly using cyberspace to spread its ideology and activities, other non-state actors such as the hacktivist group Anonymous have declared their intention to attack them anywhere they find them in cyberspace. This paper initially examines the cyberspace activities and capabilities of ISIS and Anonymous, and their roles and relationship as non-state actors. We then explore the notion of applying just war theory to non-state actors in self-defense, and propose a number of likely outcomes from our analysis.

Key words: *Terrorist, Cyberspace, Islamic State of Iraq and Syria, Anonymous, Non-state Actor, Just War Theory*

Introduction

> *The ultimate goal of stratagem is to make the enemy quite certain, very decisive, and wrong.*
>
> Barton Whaley, *Stratagem: Deception and Surprise in War,* 1969, p.135.

> *I call this whole thing the rise of the chaotic actor… [but] whoever fights monsters, should see to it that they themselves don't become one.*
>
> Joshua Gorman in *How Anonymous Hackers Changed the World*, May 2014.

The composition of actors who affect the national security of a nation-state can be both numerous and complex. The interaction between entities such as government agencies, nongovernmental organizations, citizen militias, media,

[A] Senior Lecturer, Centre for Defence and Security Studies, Massey University, Auckland, New Zealand
[B] Lecturer, Centre for Defence and Security Studies, Massey University, Auckland, New Zealand
doi: 10.18278/gsis.2.1.3

insurgencies, and other influential actors can affect how states operate in this global space. Additionally, this interaction between entities within the nation-state is making it increasingly more difficult for state actors to interact with other state actors in a cohesive and consistent manner. The influence of non-state actors on national security both within and without the state is becoming more problematic in an increasingly globalized space that challenges our traditional understandings of Just War Theory.

The role of information and communications technology and its resulting contribution to globalization is facilitating the rise of non-state actors in asserting themselves in ways that were once reserved for state actors alone. Technology increasingly enables the movement of non-state actors into multiple state jurisdictions and cross-border activities. The use of cyberspace by terrorist organizations for command and control activities, recruitment, and the dissemination of training materials is of on-going concern for state actors, and creates a new battlespace outside traditional state borders and jurisdictional lines toward interventions. With the emergence of non-state actors such as the Islamic State of Iraq and Syria (ISIS) openly using cyberspace to spread their ideology and activities, other non-state actors such as the hacktivist group Anonymous have declared their intention to attack them anywhere they find them in cyberspace.

In this paper, we examine how non-state actors are beginning to compete with other non-state actors in cyberspace, and consider how the Just War Theory of self-defense might apply to this domain. We consider this emerging phenomenon of non-state actors in conflict with each other by paying particular attention to the recent confrontation between ISIS and Anonymous and ask what implications can be derived from the emergence of competing non-state actors who consider themselves beyond the sovereignty of state actors. In conclusion, we further ask whether it is reasonable that they be allowed to conduct battle in the cyberspace domain within the previously established rules of Just War Theory or whether states should create new rules and adapt these into their respective national security strategies.

Just War Theory and Non-state Actors

The international system that emerged out of the Peace of Westphalia in the mid-seventeenth century has relied on state actors and their willingness to recognize sovereign territory and borders. There have been challenges to these states and borders since then, but recent conflicts enabled by emerging cyber capabilities present further obstacles to conventional paradigms and the historic legacies like the Sykes-Picot agreement of the last century (Dodge 2014). In the world of cyber-conflict, the question of cost in blood and treasure are terms that still apply even though the cost is not necessarily a physical one. The mass violence seen in previous wars as well as its impact at home is certainly not as severe in contemporary conflicts, but its proportionality and probability of success remain significant to the affected populations.

Just War Theory consists of *Jus ad Bellum*—the acceptable justifications for going to war in the first place, and *Jus in Bello*—the standard of conduct and activity during that period of conflict. Jus ad bellum contends that for any resort to war to be justified, a state must have the right reasons for war (Dipert, 2010). Just-war theorist Brian Orend (2008), in the *Stanford Encyclopedia of Philosophy* states that some of the

most frequently mentioned right reasons—or "just causes" include "self-defence from . . . attack; the defence of others from such; the protection of innocents from brutal, aggressive regimes; and punishment for a grievous wrongdoing . . .". Orend adds:

> *An important issue in just cause is whether, to be justified in going to war, one must wait for the aggression actually to happen, or whether in some instances it is permissible to launch a pre-emptive strike against anticipated aggression.*

The remaining Just War Theory requirements contend that motivations for war or conflict must be morally appropriate; war can only be embarked on if the decision has been made by those who have the authority to do so, has been done by a proper and acceptable process, and publicly announced. As opposed to *Jus ad bellum*, *Jus in bello* may cause some real problems for the international community of states and numerous non-state actors. Just how one might hold those in breach of these principles accountable—especially when anonymity applies? Even more difficult in the cyber battle space context, how can we discriminate those innocent users caught up in any escalation from those legitimate targets through the use of "weapons" such as a Distributed Denial of Service (DDOS) or a disseminated malware attack? A deliberate DDOS attack would be taking "deliberate aim at civilians." That being said, Orend (2008) importantly tells us that "almost all wars since 1900 have featured larger civilian, than military, casualties." In the twenty-first century cyber-domain, while ethically unjustifiable, this is still likely to remain true.

Cyber conflict is becoming increasingly more attractive as a method of "first resort" and a real challenge to the just cause question becomes whether "first strike" cyber-attacks could or should be considered an act of defense from aggression? Targeting critical infrastructure that is managed or controlled via computer networks is now a very real "first strike" option. If we take their efforts and capabilities to date, as well as their language, Anonymous certainly believes that targeting ISIS is worth an effort. And, in particular, where do the likes of Anonymous sit with this dilemma? The use of weapons in cyberspace in a conflict may challenge the proportionality component to Just War Theory. Posner and Sykes (2004) suggest that a just war may proceed only if the benefits are proportional to the costs incurred. In a cyber-war between Anonymous and ISIS, the limits of proportionality may become too big when a nonviolent stratagem is employed against an extremely violent opponent. There may be a kinetic response to a digital attack or disclosure that results in loss of life and is clearly out of proportion. Just how far is a nonviolent non-state actor prepared to go in a war of self-defense? What sacrifices are they willing to make for their cause? Is this the "red line" that distinguishes whether a state actor actively or passively sides with the nonviolent non-state actor? Further examination of some of the activities conducted by Anonymous to date might provide a glimpse of what the organization might, or might not, be capable of doing if it engaged in a full-blown cyber conflict with ISIS.

Non-state Actors Versus Non-state Actors in the Cyber Battle Space

Definitions abound to exactly what cyber-war looks like. The concept is increasingly considered, challenged, debated, accepted, rejected, and embraced. However, some parties are not convinced that war, which is essentially destructive and leads to widespread loss of life, can be waged in cyber-space, nor can cyber-conflict ever be described as "cyber-war" until such time as there is direct and real "loss of life." Others contend that cyber-war, or cyber-conflict, is confined to what has been described as cyber-intelligence, cyber-espionage, cyber-disruption, and cyber-sabotage; activities which can be—and are—undertaken independently or in the context of a war. There are parties that claim that the effect of cyber-warfare is not destructive in the real world and therefore not war like (Wisniewski 2013, Valeriano and Maness 2012, Singel 2010). While cyber-attacks thus far have not directly killed people or significantly damage property, it can be a vehicle for such results. Economically, cyber-attacks may be able to cripple a nation in such a manner that it may have a similar effect to a sustained physical attack upon its industrial base or other facets of the economy (Ruus 2008). In that sense, cyber-war can have similar outcomes or impacts upon a nation as a real war would, and therefore an impact on non-state actors as well.

In 2008, the U.S. National Intelligence Council posited that by 2025 "Cyber and sabotage attacks on critical US economic, energy, and transportation infrastructures might be viewed by some adversaries as a way to circumvent US strengths on the battlefield and attack directly US interests at home" (DNI 2008, 97). Thus, squeezing or negating resources available to, or used by, non-state actors is a method which is used to degrade the economic—and therefore political—capacity of those particular actors. Traditionally, such action requires multistate actor collaboration. For example, there is some obvious reluctance for airstrikes to target ISIS-controlled oil installations. The environmental impact of such was there for all to see during the 1991 Gulf War. Most of the ISIS-controlled oil sold on the open market is smuggled through Turkey. Challenges for Ankara are numerous; porous borders, economic interdependence, political weakness, fear of reprisal, sectarian and ethnic divisions all contribute to Turkey being unwilling and/or unable to comply (Snyder 2014, Akyol 2014, Crompton 2014, Hawramy et al 2014, Giglio 2014, Hager 2014, and Sullivan 2014). Water resources in the region can also be used as both a source of revenue or bargaining chip for state actors and non-state actors alike. Again, Turkey plays a major role here. Turkey closed the Ataturk dam on the Euphrates in August 2014 and reduced water supplies to Syria and Iraq, which led to threats from ISIS. ISIS itself has used water and electricity as a weapon, cutting off the Euphrates water supplies to the Anbar Province in Iraq and electricity to parts of the Damascus region in Syria (Halevy and Yashar 2015). Activities such as the above are founded in the physical realm. However, the

[1] The question of Prisoners Of War (POWs) must surely fill the likes of Anonymous with dread. We have already seen that ISIS does not abide by the rules—certainly not Geneva Convention standards—in relation to management of prisoners and "enemy combatants." Having said this, an equal response by the hacktivists' were they to do so, would, of course, violate *Jus in Bello* and the question of reprisal action.

vulnerability vector for disruption and/or destruction is available via the cyber battle space. More precisely, physical reprisals may provoke additional cyber-triggered responses such as a Stuxnet-derived virus that disables the Supervisory Control and Data Acquisition (SCADA) system supporting these infrastructures (Matrosov et al 2010).

Known ISIS Cyber Capabilities

Outside of revenue sources, communications are considered by many to be critical infrastructure. The use of social media assists ISIS to spread its message and gain support and recruits (Klausen 2015 and Bakke 2014). Tens of thousands of foreign fighters are thought to have immigrated to ISIS strongholds; many have come to fight directly as a result of enablers like social media, Internet chats, and other online news and propaganda systems. This online recruitment has both reached and appealed to all demographics, irrespective of gender, status, and location (Taylor 2015). It has also delivered a strong and highly compelling message. As a result, many have gone and more will go (Wood 2015). In an effort to counter such foreign fighter flows, a number of Western countries have enacted legislation to make such activity illegal, and engaged in various programs to identify those who intend to travel, as well as those contemplating such, and stop both. The results have not been altogether effective (Sengupta 2014). Additionally, human rights advocates like Deputy Human Rights Watch director Andrea Prasow opine that such surveillance not only denies the very right to travel, but more importantly may promote a situation where citizens of a state might be "prosecuted for their thoughts and their beliefs, but not their actions" (Lynch 2014).

The use of cyber space by terrorist or extremist organizations for command and control activities, recruitment, and the dissemination of training materials is of on-going concern for state actors. This is especially true in that the nature of cyberspace makes efforts to limit and/or eliminate its use by such group exceedingly difficult. With violent non-state actors like ISIS openly using cyberspace to spread its ideology and activities, other non-state actors such as Anonymous have declared their intention to attack those actors anywhere they can be found in cyberspace. But just what are the capabilities for this battle —and can Anonymous really go "mano a mano" with ISIS in this sense?

When reviewing the reported hacking incidents by ISIS and its supporters, it appears that their capabilities are primarily in the areas of compromising password security for publically accessible accounts and any associated databases used to support them (Gorman 2015, Keys 2015 and AFP 2015). Other reported hacking consisted of webpage defacement and small-scale denial of service attacks against government websites (Akbar 2015). Finally, and more significantly, there are reports that ISIS has been deploying digital surveillance tools within its geographic domain. The use of keyloggers and IP sniffers at Internet cafes, and the creation of an email malware used in an attempt to reveal IP addresses have been reported (Scott-Railton and Hardy 2014, Stormark 2014). It is understood that the ISIS "religious morals" police force called

"*Hisba*" has been using such technologies to counter the use of the Internet's anonymity in protesting the on-going brutality (March and Revkin 2015).

To accomplish the above attacks requires only moderate computer expertise when combined with existing hacking tools available throughout the World Wide Web. On the basis of these reports, it would be easy to conclude that ISIS does not appear to have the required computer skills to pose a serious threat to those outside their geographic domain. However, given this base of knowledge and the resources to recruit and employ more sophisticated tools and people, one must not disregard the potential for ISIS to become a clear and present danger in cyberspace. There are many anarchists, mercenaries, and states with the skills needed to do great harm in cyberspace. Given the condition that their interests align or worse that their ideological foundations find common ground, the prospect of ISIS fully utilizing cyberspace to commit widespread harm is very real. Therefore, the outstanding prevailing issues would be:

- What is the learning curve for existing ISIS supporters in the cyber domain and how long would it be before their capacity to harm individuals and infrastructures reaches a tipping point?
- To what degree can ISIS leverage its occupied geography to identify and conscript those with cyber capabilities?
- What is the possibility that state actors provide training and support to further cyber conflict?

We agree that there is significant concern over ISIS' use of the Internet to disseminate its mission and promote global recruitment. More importantly, as it consolidates more and more of its regional position, it will have the ability to put resources into accelerating its cyber capabilities. This will likely result in the recruitment of cyber-savvy "foreign fighters" to provide the skills with which to launch large-scale distributed attacks on infrastructures throughout the world (Radio Free Europe/Radio Liberty 2015).

Anonymous Cyber Capabilities

Largely composed of users from numerous Internet forums and chat rooms, Anonymous is currently the most well-known "hactivist" group. Utilizing its "do-ocratic" membership approach to identify what it believes to be just causes, its members employ a wide-range of attacks on a wide range of targets, from official government websites to corporate email servers belonging to low-profile criminal organizations, high-profile groups, and individuals. Most research suggests that the group was first established in the mid-2000s, bringing together the first "hackers" of the 1980s with those of the twenty-first century generation (Singer and Friedman 2014, 83). Anonymous' anonymity and notoriety have also, paradoxically, increased its profile. The efforts of Anonymous since 2007 to right–wrongs and to bring misdeeds to light have evolved exponentially.

In August 2011, a group of local Mexican Anonymous hackers launched Operation PAPERSTORM, an effort to "out" those members of the local Veracruz government that

the "hacktivists" knew were in collusion with the Los Zetas narco-traffickers. Following the murder of an internet blogger by Los Zetas in another Mexican state, Anonymous launched a DDOS attack against websites linked to the state government of Veracruz in protest of the "soft-response" from local officials, but also threatened to publish a vast archive of emails detailing the corrupt relationships between the cartel and various network partners online. In response, Los Zetas hired cyber-experts to help "reverse hack" Anonymous in order to identify some of its members. One such hacktivist was ultimately identified, kidnapped, and threatened with execution. This real Mexican "stand-off" was resolved when Anonymous agreed not to release the material, and in exchange, the kidnap victim was freed with an accompanying warning from Los Zetas that they would kill 10 people for every name Anonymous should subsequently chose to publicize (Singer and Friedman, 84–86 and Rexton Kan 2013, 40). Paul Rexton Kan, who wrote extensively of the exchange, described the stalemate as one of ". . . two clandestine non-state groups [who] stared each other down in the digital domain" (40). More importantly, he highlights the different benefits and values non-state actors see in the Internet and the information age:

> *The members of Anonymous see cyberspace as a type of commons that should be accessible to all.… Los Zetas, on the other hand, do not view cyberspace through an ideological lens but through an operational lens*

With the Anonymous–Los Zetas "stand-off" firmly in mind, we turn to the question of how vulnerable might Anonymous see itself—real or perceived—because of ISIS' very existence? Anonymous has a number of options that it might use in a nonviolent or nonkinetic manner, in order to defend the Anonymous "state". Anonymous published a "Declaration of War" because ISIS strikes at the very heart of what those in Anonymous believe in; that of freedom of expression and freedom of speech (Makuch 2014 and Chen 2014). While the conflict continues to progress and evolve, perhaps the real issues to be considered are as follows:

- Can Anonymous maintain this nonviolent approach (denial of service, release of information, etc.) and how far could they go?
- How effective could Anonymous be and is this the way forward?
- Should states embrace such action from nonviolent non-state actors, encourage such activity even, or is it opening up a "Pandora's box" of interpretations, debates on thresholds?
- What constitutes an "enemy," control of resources, or are we far too early into this "battle in the cyber domain" construct for us to get anywhere near beginning to understand what we are dealing with now?

Escalation Options: How Far Can Anonymous Go?

Largely as a result of the incident with Anonymous, Los Zetas embarked on a greater effort to increase their cyber capabilities by recruiting and coercing computer engineers and university students to assist with their cyber-crime efforts. This,

combined with surveillance technology provided by Los Zetas' stable of government, law enforcement, and military co-optees and collaborators, enabled the group to counter the threat presented by Anonymous. Known for its ruthlessness, the cartel responded by carrying out actions that would ensure the Anonymous threat would not present itself ever again. The hacktivists backed down because to follow through with their actions was not worth the potential cost in lives. Singer and Friedman (118-126) suggest that this particular incident make us think about cyber-war theory, especially the limits of state actors in dampening or preventing such conflict from escalating. Rexton Kan (41-43) adds that cyber conflict presents a paradigm within the cyber-world and without the state. Both authors express concern about the evolving iteration of nontraditional actors in this far more asymmetric twenty-first century.

For example, in 2007, the Department of Homeland Security (DHS) put together a team of "hired hackers" and conducted an experiment to destroy a large generator via cyber-attack (East et al 2009, 67–81). Four years later, the experiment, known as the "Aurora Generator Test", was declassified and the impressive video footage released, showing how a cyber-attack could destroy a large diesel generator that was linked to a mock electricity grid. The attack, using a computer program to modify circuit breakers, was enough to see the generator self-destruct. Might the oil infrastructure that ISIS controls be vulnerable to such attacks—covert sabotage? And if the state, or state actors, for whatever reason be unable or unwilling to carry such activity, then might the likes of Anonymous be prepared to "step up to the plate?"

In early February 2015, a Five-Country Ministerial Communique was released after a meeting of top government ministers from the "Five-Eyes" nations of the United States, Great Britain, Canada, Australia, and New Zealand (Five-Country Ministerial Communiqué 2015). The single emphasis of the Communique concerned the shared efforts necessary to counter the threat from violent extremism. Ministers identified the need to develop proactive strategies to address these groups and their "use of . . . internet and social media platforms" and stressed the importance of a "sustained and aggressive approach" to counter such challenges.[2] The Ministers suggested that opportunities to work with commercial companies might achieve this end. Could we add other non-state actors to this new twenty-first century coalition?

History tells us that engagement like this has been done in the past and, in all likelihood, continues today. During the 1980s, as computers started to form connected networks, accessing such networks via clandestine means gave intelligence services an opportunity for further methods of penetration. An early example was the KGB-sponsored German hackers who penetrated several hundred computer systems connected to the U.S. Military's MILNET networks (Price 2014, 55). And it seems that state actors recruiting third-party experts or specialists in order to access, deny, and disrupt adversaries and national security threats have not changed. Investigations into the FBI's use of one of Anonymous' very own—Hector "Sabu" Monsegur, ultimately discovered that this informant and third-party hacker who had been working for the government since his arrest in 2011 was responsible for coordinating several hundred computer attacks and penetrations against Anonymous members themselves, as well

[2] Five-Country Ministerial Communiqué, released February 6, 2015.

as websites operated by the governments of Iran, Syria, Brazil, and Pakistan (Mazzetti 2014).[3]

In an opinion piece in ForeignPolicy.com in early March 2015, commentator Emerson Brooking (2015) suggested that the very people who should be charged with countering ISIS, "dispersed, rapidly regenerative online presence," should be digital natives themselves. Brooking considered that Anonymous was perfect for the job, and should be supported with resources to do so, including paying those individuals with the online currency "Bitcoin." He added "As a rule, hacktivists despise bullying, hypocrisy, and fundamentalism. The Islamic State couldn't present a clearer target." The prevailing concern is the means by which non-state actors such as Anonymous might be co-opted into serving national and international interests to do what state actors cannot or would not do. Coercion or monetary incentives are probably to go against the social tenets that Anonymous' member espouse and may have serious future sustainability consequences for the group. In an interview with a member of the Anonymous collective known as "Nix," who also provides legal support for those being prosecuted for hacking, the authors were told that "one of the main attractions to being a part of Anonymous is a sense of empowerment to right wrongs."[4] Having turncoats or hired guns greatly diminishes this sense of shared social activism. If we return to Anonymous' first principles, it is their unrelenting moral stance on issues and rights and its ability to disclose massive amounts of information on associations and activities that has propagated its renown. Thus, Nix added "In response to Anonymous' disclosures that directly benefit society, perhaps a Cyber Samaritan Law would benefit a nation state's efforts to limit wrongful prosecutions" (2015). Such a law would limit an activist's liability; allow government deniability; conserve judicial resources; and provide better targeted prosecutions. Could state actors embrace such a direction?

Conclusions

In his article, Brooking (2015) mentions that engaging in such activity, or sanctioning the recruitment of hacktivists like Anonymous, would challenge what we would consider to be the "international norms." But things have changed. Surely these rules are not necessarily applicable in the non-state actor realm? Can we embark on a new set of rules that takes us back before Westphalia, to the days when Indian strategic thinker Kautilya first introduced the "Mandala theory" of state security—"the enemy of my enemy is my friend"(Rangarajan 1992)? Rexton Kan concludes that the Anonymous versus Los Zetas "stand-off" was not anticipated and suggests that cyber-conflict and the future of cyber-warfare is only limited by the human imagination. At some stage, he adds, it is likely to transition from online embarrassment and discomfort, to off-line and real—death and destruction. Clearly should such novel methods be utilized by non-state actors, they must be met with equally creative policies and strategies from security agencies.

[3] Monsegur had been partly responsible for the penetration and theft of information belonging to the Texas-based Stratfor Global Intelligence provider. Interestingly, neither Monsegur, nor any of the Anonymous felons was charged with cyber-attacks on any of these foreign websites.

[4] Nix interview conducted with authors on April 12, 2015.

Whether we like it or not, non-state actors are now a part of a new and emerging battle space. Where the state's power was near absolute, cyberspace has enabled a means for non-state actors to effect change in the physical world. Because of this, non-state actors are increasingly becoming problematic to state actors unless their interests align. Perhaps this is precisely the reason why states might wish to task non-state groups with activities that allow a significant degree of deniability while furthering shared goals. So, what if the state were to sponsor such activities? Between the 1970s and 1990s we saw the concept of state-sponsored terrorism—could the same apply in a state-sponsored cyber-sense? What we are seeing today might be a way in which Superpowers use non-state actors to carry out operations against each other—deniability, clandestine or covert operations—if they are not doing so already. In its targeting of ISIS' cyber presence, what would be the outcome if Anonymous were to become more robust and aggressive, and have an element of "deniable protection" from a supporting state actor in its cyber activities? Providing incentives for aligning interests is something worthy of further examination but we must also consider the fallout such actions may bring as well.

There is a likely but unknown degree of escalation in this battle space that is about to emerge, and creative policies and strategies should be the carefully developed to mitigate unexpected outcomes. To this we add that there must be "bold" and "novel" approaches to addressing the threat that other non-state actors might make in these cyber-conflicts. But there are some limitations, or tolerances, to this aggressive, pro-active imagination that must be considered, and these challenges to existing legal, ethical, and moral practices within the security space must be equally considered now. In the words of former British intelligence "Mandarin" Sir David Omand "providing for public security is an exercise in risk management, not risk elimination" (Omand 2010, 250). We believe that the paradigm of state actor reliance for self-defense is one that is already evolving into another form, and as such, the time for considering the role of non-state actors in self-defense is upon us.

References

AFP. 2015. "French TV Channel Restarts Full Operations After 'Unprecedented' ISIS Hack." *The Straits Times*, April 10.

Akbar, Jay. 2015. "'Death to France. Death to Charlie': Pro-ISIS Hackers Launched 'Unprecedented' Wave of Cyber-Attacks on 19,000 French Websites." *MailOnline*, January 15.

Akyol, Mustafa. 2014. "The Truth About Turkey and Islamic State Oil." Al Monitor, September 22.

Anonymous. 2014. "How Anonymous Hackers Changed the World." [Video file], May 29. https://www.youtube.com/watch?v=Q6o7lEKloJc (accessed March 29, 2015).

Bakke, Kristin. 2014. "Help Wanted? The Mixed Record of Foreign Fighters in Domestic Insurgencies." *International Security* 38 (4): 150–187.

Brooking, Emerson. 2015. "The U.S. Government Should Pay Anonymous in Bitcoin to Fight ISIS." *ForeignPolicy.com*, March 3.

Chen, Adrian. 2014. "Anonymous No More: The Celebrated Hackers Represent the Worst of Techno-Utopianism." *The Nation*, December 1/8.

Crompton, Paul. 2014. "Sales of Black Market Oil Surge in Middle East." *Al Arabiya News*, July 29.

Dipert, Randall. 2010. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9 (4): 384–410.

Dodge, Toby. 2014. "Can Iraq Be Saved?" *Survival: Global Politics and Strategy* 56 (5): 7–20.

East, Samuel, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. 2009. "A Taxonomy of Attacks on the DNP3 Protocol." In *Critical Infrastructure Protection III*: 67–81

Giglio, Mike. 2014. "This is How ISIS Smuggles Oil." *BuzzFeed News*, November 4.

Gorman, Ryan. 2015. "Alleged ISIS Cyber Terrorists Infiltrate Media Twitter Accounts, Post Sensitive Information and Documents." *Aol.com*, January 6.

Hager, Emily B. 2014. "ISIS' Dark Oil Trade." *New York Times*, December 1.

Halevy, Dalit and Ari Yashar. 2015. "ISIS's War of Water and Electricity." *Israel National News* February 18.

Hawramy, Fazel, Mohammed Shalaw, and Luke Harding. 2014. "Inside Islamic State's Oil Empire: How Captured Oilfields Fuel Isis Insurgency." *The Guardian*, November 19.

Keys, Matthew. 2015. "Exclusive: 'Cyber Caliphate' Unmasked as Lone Algerian Hacker." *The Desk, Journalism and Social Media by Matthew Keys*, February 10.

Klausen, Jytte. 2015. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism* 38 (1): 1–22.

Lynch, Colum. 2014. "The Islamic State Makes Electronic Surveillance Respectable Again." *ForeignPolicy.com*, September 24.

Makuch, Ben. 2014. "Anonymous-Affiliated Hackers Have Declared War on the Islamic State." *Motherboard.vice.com*, June 30.

March, Andrew F. and Mara Revkin. 2015. "Caliphate of Law: ISIS' Ground Rules." *Foreign Affairs*, April 15.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. 2010. "Stuxnet Under the Microscope." *ESET Internet Security* LLC, September. https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

Mazzetti, Mark. 2014. "F.B.I. Informant Is Tied to Cyberattacks Abroad." *New York Times*, April 23.

New Zealand Government. 2015. *Five-Country Ministerial Communiqué*. February 6.

Omand, Sir David. 2010. *Securing the State*. London: Hurst.

Orend, Brian. 2008. "War." In Edward N. Zalta, eds, *The Stanford Encyclopedia of Philosophy* (Fall 2008 Edition). http://plato.stanford.edu/entries/war/

Posner, Eric A. and Alan O. Sykes. 2004. "Optimal War and Jus Ad Bellum." *U Chicago Law & Economics, Olin Working Paper No. 211*.

Price, Douglas R. 2014. "Guide to Cyber-Intelligence." *The Intelligencer, Journal of U.S. Intelligence Studies* 21 (1) (Winter 2014–2015): 55-60.

Radio Free Europe/Radio Liberty. 2015. "Foreign Fighters in Iraq and Syria." *Radio Free Europe/Radio Liberty*, January 29.

Rangarajan, L.N. 1992. *Kautilya: The Arthashastra*. New Delhi: Penguin Books.

Rexton Kan, Paul. 2013. "Cyberwar in the Underworld: Anonymous Versus Los Zetas in Mexico." *Yale Journal of International Affairs* 8 (1) (Winter 2013): 40-51.

Ruus, Kertu. 2008. "Cyber War I: Estonia Attacked from Russia." *European Affairs 9 (1-2)* (2008). Columbia International Affairs Online.

Scott-Railton, John and Seth Hardy. 2014. "Malware Attacks Targeting Syrian ISIS Critics." *The CitizenLab*, University of Toronto, Munk School of Global Affairs, December 18. https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/.

Sengupta, Somini. 2014. "Nations Trying to Stop Their Citizens from Going to Middle East to Fight for ISIS." *New York Times*, September 12.

Singel, Ryan. 2010. "White House Cyber Czar: 'There Is No Cyberwar.'" *Wired Magazine*, March 4.

Singer, P.W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Snyder, Stephen. 2014. "ISIS is Selling Cheap Oil to its Enemies — From Syria's Government to the Kurds." *Pri News*, September 16. Stormark, Kjetil. 2014. "Hunt for America's Spies." *Hate Speech International*, December 1.

Sullivan, Paul. 2014. "The Energy-Insurgency Revolution Nexus: An Introduction to Issues and Policy Options." *Journal of International Affairs* 68 (1) (Fall/Winter 2014): 117-148.

Taylor, Adam. 2015. "Gun-toting Women Sell Jihadist Recruitment Message." *Washington Post*, March 28.

United States National Intelligence Council (DNI). 2008. *Global Trends 2025: A Transformed World*. Washington DC: National Intelligence Council.

Valeriano, Brandon and Ryan Maness. 2012. "The Fog of Cyberwar; Why the Threat Doesn't Live Up to the Hype." *Foreign Affairs*, November 21.

Whaley, Barton. 1969. *Stratagem: Deception and Surprise in War*. Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology.

Wisniewski, Chester. 2013. "Comment: There's No Such Thing as Cyber War." *Infosecurity Magazine*, August 1.

Wood, Graeme. 2015. "What ISIS Really Wants." *The Atlantic*, March.

Calculation of Goodwill: Humanitarianism, Strategic Interests, and the U.S. Response to Typhoon Yolanda

Chris J. Dolan[A] & Alynna J. Lyon[B]

U.S. participation in the global response to Typhoon Yolanda (Haiyan) was compelled by both humanitarian concerns and strategic interests. U.S. action can be understood as a product of domestic and global discourse, historical milieu, logistical factors, and domestic political determinants highlighting the importance of Asia and the Pacific in U.S. foreign policy. Consistent with previous engagements, it is apparent in this case that humanitarian concerns aligned with strategic interests in shaping the extent of U.S. involvement. Our examination begins with a conceptualizing the determining factors in humanitarian operations. This provides specific focus on the degree with which historical milieu and larger episodes of previous engagements, media coverage and public support, human security and humanitarian concerns, and strategic interests enter into considerations. Our study then applies these concepts to understand the decision-making calculus in Operation Damayan. We conclude that the prevailing literature should focus more on a comprehensive understanding of interactive concepts and dynamic factors that include state actors, norms, domestic determinants, global factors, and historical milieu..

***Keywords**: Typhoon Yolanda, Operation Damayan, historical milieu, human security, strategic interests*

The goal of this examination is to assess the complexities of U.S. participation in humanitarian relief operations in response to Typhoon Yolanda, which made landfall in the Visayas region in the Philippines on November 8, 2013. Not only did the humanitarian mission, dubbed Operation Damayan, garner significant media coverage and public influence, it underscored the strategic importance of the Philippines in the Obama Administration's foreign policy "pivot" or rebalance to Asia and the Pacific. It was also not the first time the United States participated in a large-scale humanitarian mission with strategic implications in the region. In 2004, when the Indian Ocean Tsunami killed hundreds of thousands of people, the United States participated in relief and recovery efforts that ultimately reestablished order, reconstructed economic institutions, and led to peace in Aceh Indonesia. In 2011, in response to the tsunami that triggered nuclear disaster in Fukushima Japan, the United States moved quickly to bolster its most important ally in the Western Pacific. Therefore, in Operation Damayan, the U.S. role was shaped by several interactive determinants that co-evolved as part of a broader historical episode of humanitarian engagements and strategic considerations.

[A] Professor, Lebanon Valley College
[B] Associate Professor, University of New Hampshire

doi: 10.18278/gsis.2.1.4

Determinants of Involvement in Humanitarian Operations

U.S. involvement in humanitarian operations is determined and shaped by media coverage, public support, historical milieu, as well as strategic interests and human security concerns.

Historical Milieu and Larger Episodes

To examine one humanitarian operation without considering previous engagements and interventions is to ignore or downplay the complexity and dynamism of each case of human suffering. For example, the large-scale U.S.-led humanitarian involvement in multilateral operations in response to Super Typhoon Yolanda cannot be divorced from the 2004 Indian Ocean Tsunami or the 2011 tsunami and nuclear disaster in Japan as well as other efforts to alleviate human suffering. This dynamic can be conceptualized in terms of policymaking and decision-making processes shaped by comprehensive, interconnected relationships determining policy outcomes across cases of human suffering. Previous cases of human suffering can be perceived through historical milieu and seen as larger episodes of strategic and humanitarian involvement (Oliver and Myers 2002). Historical milieu can be used to explain how the 2004 Indian Ocean Tsunami and 2011 tsunami and nuclear disaster in Japan shaped and interacted with the 2013 Super Typhoon Yolanda, two tragedies that prompted far-reaching U.S.-led humanitarian responses.

U.S.-led humanitarian actions also coevolve within a broader context of shifting normative and strategic conditions that demand responsive adaptation strategies by policy elites (McGowen 1974; Rosenau 1970, 36; Thorson 1974). The degree of foreign policy adaption is shaped and determined by an interactive and diffuse set of dynamics functioning on both institutional (policy elites operating in political authority structures) and ideational (policymaker perceptions and images of domestic and global contexts) levels (Rosenau 1992). Our framework captures the idea of "linkage politics" in demonstrating how humanitarian missions launched in response to natural disasters are characterized by both global and domestic forces (Putnam 1988; Rosenau 1969; Wilkenfeld 1973).

Humanitarian operations involve actions and reactions that function in response to altering circumstances, historical narratives containing moral evaluations, and as broader responses to systemic and nonlinear continuity and change. Put simply, historical milieu might increase public and elite confidence in specific operations. This "halo effect" might result in humanitarian relief operations garnering at least the same level of success as past missions (Jentleson 1992).

Media Coverage and the Public

We believe that it is reasonable to suggest that media coverage, public perceptions and awareness, and policymaker decisions within the foreign policymaking process are filtered through humanitarian action. To understand historical milieu and

humanitarian actions, we observe the intensity of news coverage and the role of the public and public perceptions in Operation Damayan in relation to the 2004 Indian Ocean Tsunami and the 2011 tsunami and nuclear disaster in Japan.

Decisions to address human suffering are not only shaped by historical milieu and seen as larger episodes of involvement; they are also shaped by media coverage and the public (Mueller 2005; Page, Shapiro, and Dempsey 1987; Shirky 2011). Livingston (1997) postulates that the media can enhance the role of the public in inducing or impeding an intervention. Media can serve as a "force multiplier" and induce an intervention by shortening the time in which decision makers form their policy responses or act as an "emotional inhibitor" and impede an intervention by covering events with a focus on casualties (Frizis 2013; Livingston 1997). Buzan (2004, 17) argues that the potential for humanitarian action increases when nonstate actors encourage media to raise awareness of a natural disaster, emergency, or armed conflict. Media are likely to exercise more influence and persuasion within foreign policy decision-making circles when there is significant uncertainty and disagreement among policymakers (Bob 2005; Gowing 1994; Minear, Scott, and Weiss 1996, 73; Strobel 1997).

Instances of human suffering are likely to become news events with both traditional and social media outlets intensifying coverage and raising the level of human interest. This ebb and flow contributes to a "media attention cycle," in which degrees of news reporting and public coverage shape and determine media coverage of human suffering (McPhail, Schweingruber, and McCarthy 1998). These norms influence governmental interests and policy action, especially since different forms of media create perceptions and images of suffering and crisis at particular moments (Finnemore 1996, 2–3; Ignatieff 1998). Research demonstrates public empathy tends to rise and fall when human suffering and crises occur around the world, resulting in so-called compassion fatigue (Belloni 2005; Dean 2003; Minear, Scott, and Weiss 1996). Digital media have the potential to tap into public sympathy by capturing and sharing stories and images of human suffering (Shirky 2011).

Social media coverage has tested conventionally understood boundaries between formal and informal modes of covering global crises while at the same time enhancing citizen journalism (Palen and Liu 2007; Williams 2013). Although the connection between the increase in the number of persons accessing the Internet and social networking sites with political engagement is tenuous at best, one study finds that individuals who seek out information on social networking mediums lead to greater levels of civic and political participation and awareness (Gil de Zúñiga, Jung, and Valenzuela 2012; Shirky 2011).

The public can play an influential role in shaping policy responses to human suffering by limiting the range of options available to policymakers and making decisions to use military resources politically risky (Feaver 1998). However, intensity of public awareness is determined by the extent of news coverage of human suffering and public opinion. Elites are likely to be influenced by public attitudes prior to or in the wake of foreign policy actions, especially with regard to the use of military force in response to armed conflicts and natural disasters (Baum 2002; Burstein 2003;

Sobel 2003). One study suggests public support for humanitarian interventions can help Congress and the presidency overcome and transcend partisan opposition and ideological constraints (Hildebrandt et al. 2013). The general orientation of the public may lead policymakers to shield themselves from mass public opinion on foreign policy (Jacobs and Page 2005).

Yet, the level of public attention or degree of support for humanitarian operations is unclear. Some assume a policy-driven approach and discuss the notion of human costs, risk and cost-aversion (Ehrlich and Maestas 2010; Feaver and Gelpi 2004; Gartner and Segura 1998; Kam and Kinder 2008). According to Donnelly (1993), governments recognize that the political benefits of humanitarian interventions are low, even if pursued within a multilateral context. Howell and Pevehouse (2005) contend greater levels of public support could increase the probability of a successful mission. On the whole, this literature maintains that public support is largely a function of outcomes (Berinsky 2009; Gartner 2008; Gelpi, Feaver, and Reifler 2005/2006; Klarevas 2002; Mueller 1994).

Human Security

With the end of the Cold War, humanitarian action became an important normative pillar in the emerging new world order. In 1991, the United Nations Security Council passed Resolution 688 after the Persian Gulf War to assist in the crisis facing the Kurds in Northern Iraq. The operation did not seek authorization from the Iraqi government and altered the terms under which states acting through inter-governmental organizations may intervene. Although this was reinforced by the U.S.-led mission in Somalia one year later, aid and relief operations in the war-torn East African country highlighted the risks of intervention (Chopra and Weiss 1992).

State-centric approaches tend to downplay the significance of human security (Ashley 1983; 1988). Mack's (2004, 366–367) conceptualization defines human security in terms of fear of war and violence. Thakur (2004, 347) puts forth a broader interpretation in arguing that "human security is concerned with the protection of people from critical life-threatening dangers," such as natural disasters or structural conditions. Paris (2001, 87–102) observes that human security seems for some to be an emerging paradigm that "encompasses everything from substance abuse to genocide."

Natural disasters can involve significant loss of innocent human life, damage critical infrastructure, and destruction of social, political, and economic systems, leaving people vulnerable to hazards and jeopardizing their human security (Bankoff, Hilhorst, and Frerks 2004; Pelling 2003; Wisner et al. 2003). Strong and effective humanitarian operations should provide physical and logistical assistance and mitigate suffering from natural disasters and armed conflicts. These missions are based on the norm of the right to receive help and the obligation of actors with means and capabilities to deliver aid to victims (ICRC 1977).

Research demonstrates that normative and ideational factors shape the material resources and physical capacities of states (Biersteker 1989; Linklater 1998). As Wendt (1995, 71–81) states, "material resources only acquire meaning for human action

through the structure of shared knowledge in which they are embedded." Finnemore (1996, 2–3) adds, the "normative context also changes over time, and as internationally held norms and values change, they create coordinated shifts in state interests and behaviour across the system." Claude (1966, 367–379) emphasizes the significance of legitimate action and Wheeler (2000, 4) observes that since "legitimacy is constitutive of international action," norms and beliefs can either constrain states or force them to set criteria for humanitarian operations. Commonly-held beliefs serve as the basis for understanding global norms regarding sovereignty, humanitarian action, and human suffering (Acharya and Buzan 2010; Bellamy 2003; Buzan 2004; Gibbs 2009; Kuperman 2008; Orford 2003; Reus-Smit 2001; Wheeler 2000). Consequently, human security must be incorporated into an understanding of how global actors respond to natural disasters, recover from catastrophe, and help rebuild in the wake of destruction (Cox 1999; Shaw 2000; Sinclair 1996).

Humanitarian action rests on assumptions that people possess rights and freedoms that states and global institutions must protect regardless of social and economic condition (Butler 2001; Devetak 2007; Janse 2006). Shared notions of morality define human rights and sustain a mutual humanity (Fixdal and Smith 1998). Failing to address physical security and basic protections of people suffering from natural disasters would constitute a deprivation of human rights and human security (Coates 2003; ICRC 1977).

Several international legal instruments establish guidelines for minimum standards of humanity. Common Article 3 of the Geneva Conventions sets out binding standards by maintaining that states should treat persons humanely, prohibit violence and assaults on human dignity, and must treat the injured and sick. Moreover, a state's failure to consent to the delivery of humanitarian aid within its borders threatens the survival of the civilian population (Stoffels 2004). If states block humanitarian assistance, they would be in violation of international statutes in the Geneva Conventions (Henckaerts and Doswald-Beck 2009, 105, 193). However, the need for the afflicted state to consent to humanitarian operations within its borders is not clearly established. While human security provides a principled basis for humanitarian operations, state sovereignty is a powerful force that limits intervention (Devetak 2007).

Strategic Interests and State Sovereignty

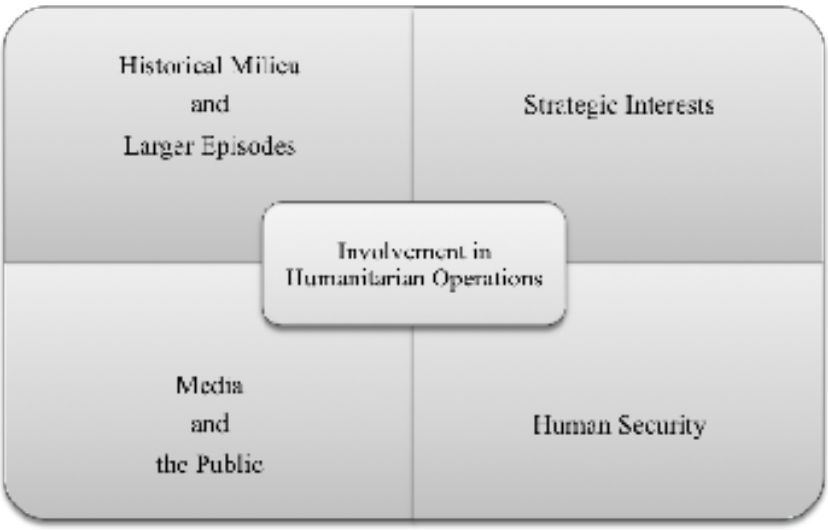
The role of strategic factors, such promoting economic prosperity and balancing against challengers, means that state sovereignty and jurisdictional exclusivity are key to whether states become involved in humanitarian operations (Chayes and Chayes 1996). International statutes reinforce these. The Charter of the Organization of American States (OAS 1967, Article 18) states that "No State or groups of States has the right to intervene, directly or indirectly, for any reason what so ever, in the internal or external affairs of any other State." Article 2 (7) in the U.N. Charter raises the right of state sovereignty, preventing powerful states from violating the territorial integrity of weaker states. Pham (2004) contends that the shroud of humanitarianism might

conceal state interests while Franck and Rodley (1973) emphasize that humanitarian norms provide great potential for major powers to engage in self-interested pursuits.

Others caution against state utilization of economic and military resources for pursuing anything short of national interests defined as self-interested motivations. Bellamy (2003) suggests realists oppose humanitarian interventions because military activities to simply aid others do not work and are not vital to the national interest. Wheeler (2000, 30) explains that "states will not intervene for primarily humanitarian reasons because they are always motivated by considerations of national self-interest." While some caution against using foreign policy for philanthropy, others might accept intervention in order to help those in need as long as it does not challenge state security interests, impose high financial costs, or result in loss of life (see Wheeler 2004).

Humanitarian operations may be interpreted through a long-term strategic perspective. States might take part in humanitarian actions if they promote efforts to balance against a rival, attain economic goals, or to enhance regional stability. A state might be able to safeguard or improve its image or even build goodwill and trust with other states in a region deemed vital to the national interest (Farer 2005, 228). However, as we observe in the next section of this article, human security concerns converged with strategic considerations in Operation Damayan. Consequently, we cannot separate self-interested state motivations from humanitarian considerations (see figure 1).

Figure 1: Interactive Framework

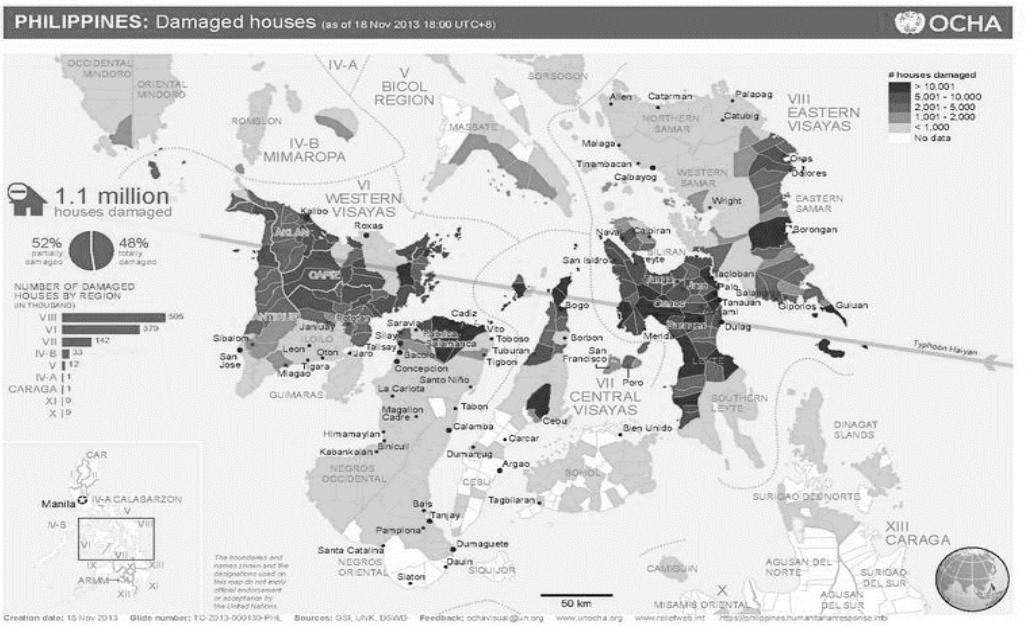


Operation Damayan

On November 8, 2013, for 16 hours, Category 5 super Typhoon Yolanda swept through six provinces in the Philippines, killing more than 6,000, displacing 670,000, affecting roughly 11.3 million people, and causing between $6.5 billion and $15 billion in damages (see figure 2) (Agence France-Presse 2013; Gladstone 2013;

UNOCHA 2013). In the coastal communities of Eastern Samar, and Western Leyte, there was little to no defense against Yolanda. In six provinces, the typhoon destroyed the power and telecommunications infrastructure, disrupted water supply lines, cut-off food provisions, demolished pharmacies, damaged airports, and blocked roads (de Leon and Zavis 2013; Fisher 2014). Although advanced warnings saved many lives and the speed of the storm limited flood damage, the humanitarian crisis hampered relief efforts. The United States responded with Operation Damayan, which allocated military and civilian resources to bolster the Philippines, an important strategic ally.

Figure 2: Residential Damage from Typhoon Yolanda



Source: UN Office for the Coordination of Humanitarian Affairs: http://reliefweb.int/sites/reliefweb.int/files/resources/TC-2013-000139-PHL_house_damaged_20131122.pdf

Humanitarian Catastrophe and the Multilateral Response

The lack of available personnel made it difficult for the Philippine government to quell looting and reestablish order (Fisher 2014). Aid workers feared even greater desperation in poorer and more remote areas beyond the cities where there was little or no communication. To save lives, humanitarian assistance offered by the International Red Cross, the United Nations, governments, and private groups needed to reach the victims quickly, especially given the 1,096 evacuation centers near the strike zone could only hold 240,800 people. Although it took 10 days for relief supplies to reach the most devastated areas, especially in Leyte province, the most remote islands and areas received little to no immediate assistance (Jacobs 2013).

Food insecurity was an immediate concern, since the rural population depends on agriculture inputs before the growing season ends in January. Also, 1.1 million

homes were destroyed and tens of thousands were reported missing, raising concerns about human trafficking. In response, the U.N. Population Fund (UNFPA) supplied assistance and protection to the displaced and the U.N. Children's Fund (UNICEF) assisted families separated by the storm. Although the widespread devastation prompted a number of states to pledge aid (see table 1), a much larger effort was required to coordinate emergency assistance and provide clean drinking water, sanitation, food, shelter, management of the dead and medical treatment to survivors to stave off diseases and infections.

Table 1: Global Relief Efforts and Action Plan in Response to Typhoon Yolanda (Haiyan)

Top 10 Donors to the Emergency	**Amount ($US millions)**
Private individuals and organizations	159
United Kingdom	104
U.N. Un-earmarked funds	87.4
United States	87
Japan	51.7
Australia	38.7
Norway	26.6
Central Emergency Response Fund	25.3
Canada	19.1
Sweden	16.6
Global Action and Strategic Response Plan (November 2013–October 2014)	
Private individuals and organizations	Amount ($US millions)
U.N. Un-earmarked funds	87.4
United States	40.2
United Kingdom	39.5
Center Emergency Response Fund	25.3
Japan	24.1
Australia	19.6
Norway	15.8
Canada	12.7
European Commission	11.7

Source: United Nations Office for the Coordination of Humanitarian Affairs: http://www.unocha.org/crisis/typhoonYolanda (Haiyan)/funding

In order to coordinate rescue and relief efforts, the United States sent military personnel and deployed its advanced logistical capabilities. It dispatched 50 naval ships to the hardest hit areas and aircraft-dropped supplies and equipment from the *U.S.S. George Washington* carrier to remote locations. Efforts focused on reopening critical links throughout the archipelago, especially on Panay Island where Roxnas

and Tacloban airports are located, so food and water, medical supplies, and other humanitarian assistance could be delivered. The U.S. Agency for International Development (USAID) and the Office of Foreign Disaster Assistance (OFDA) in collaboration with the U.S. Embassy, Philippine government, nongovernmental organizations, and U.N. agencies released funds to implement the first stage of the emergency response, deployed disaster assistance teams to assess humanitarian needs, positioned emergency relief supplies, and determined levels of aid. Also, the State Department established a crisis response task force to facilitate coordination with other agencies responsible for managing assistance requested by the U.N. Humanitarian Country Team (USAID 2013).

Prior to the typhoon, multilateral assistance to the Philippines remained relatively low from 2000 to 2008 but more than doubled from $40 million to $107 million between 2008 and 2009. The level of assistance increased at a slower rate to roughly $113 million in 2010 and $123 million 2011 (see table 2). The increase was made in response to disasters from earthquakes and other typhoons, as well as to contain the conflict in Mindanao. Disaster assistance largely went to relief and preparedness, which increased from 2.5% in 2007 to 39.2% in 2011 (GHA 2012a).

Regarding U.S. bilateral aid, USAID delivered $65.3 million for disaster relief, recovery, and preparedness to the Philippines; in 2013 alone, it provided over $7 million in aid. Much of this assistance helped with the formulation of a disaster risk reduction program and the adoption of an incident management system aimed at enhancing the capacity of national and local governments by managing the causal factors of disasters and lessening the vulnerability of people and property. The program was implemented in response to Tropical Storm Ketsana (Ondoy) in 2009, Typhoon Megi (Juan) in 2010, Tropical Storm Washi (Sendong) in 2011, and Typhoon Bopha (Pablo) in 2012 (USAID 2014).

Complicating the humanitarian response was the government's armed struggles with rebel groups operating in the impacted areas. In Mindanao and adjacent islands, conflicts raged between government forces and the Moro Islamic Liberation Front (MILF), Abu Sayyaf, and the Moro National Liberation Front (MNLF). This was exacerbated by violent attacks by Jemaah Islamiyah (JI), Bangsamoro Islamic Freedom Fighters (BIFF), and the New People's Army (NPA).

In the immediate wake of the typhoon, the Philippine government reached out to armed Communist rebels to cooperate with humanitarian relief operations and help the government with reconstruction (Philips 2013). Just one month after the typhoon struck, the government and MILF rebels signed a peace agreement, ending a decades-long insurgency that killed tens of thousands. Although MILF gave up its demand for independence, they won greater autonomy in Bangsamoro in Mindanao (Marszal 2013).

Table 2: Multilateral Aid to Philippines, 2005–2011 ($ millions)

2005	$	2006	$	2007	$	2008	$
EU	3.9	Australia	7.1	EU	8.3	EU	13.1
Germany	1.9	EU	4.6	Sweden	3.1	Spain	8.1
United Kingdom	1.2	Saudi Arabia	2.4	Spain	3.0	United States	4.8
Australia	0.9	Spain	2.4	the Netherlands	2.8	Germany	4.1
Canada	0.9	Germany	2.0	Germany	2.4	Australia	3.1
United States	0.8	Norway	1.9	Italy	1.7	Italy	2.8
France	0.8	United Kingdom	1.8	United Kingdom	1.7	France	2.6
Norway	0.5	the Netherlands	1.6	France	1.6	United Kingdom	2.3
Sweden	0.4	Canada	1.4	Japan	1.5	Sweden	2.1
Spain	0.3	Korea	1.2	Denmark	1.0	the Netherlands	1.8

2009	$	2010	$	2011	$
Spain	17.2	Japan	48.1	Japan	59.4
EU	16.2	EU	23.1	EU	14.8
Japan	11.6	United States	19.5	Australia	14.6
Germany	9.0	Germany	6.4	United States	9.8
Australia	8.1	Spain	6.1	Sweden	5.3
Canada	6.0	Sweden	5.4	United Kingdom	4.6
Sweden	5.6	France	4.5	Germany	4.1
United States	5.4	Australia	4.0	Spain	3.8
United Kingdom	5.2	United Kingdom	3.8	Norway	3.8
Italy	3.8	Italy	2.7	France	2.6

Source: Development Initiatives based on Organization for Economic Cooperation and Development, Development Assistance Committee, and the United Nations Office for the Coordination of Humanitarian Assistance data, Financial Tracking Service; Reports and data be found at: http://www.globalhumanitarianassistance.org/countryprofile/philippines

Strategic Considerations

Following the U.S. drawdown in Iraq and Afghanistan, the Obama Administration placed the Asia-Pacific region at the center of its foreign policy agenda with its so-called pivot or rebalance to Asia (Clinton 2011). Therefore, the U.S. response was not only immediate; it was designed to express support for an important ally and reinforce an already strong bilateral relationship.

The United States imports more goods and services from Asia than any other zone and is now one of the largest export markets in the world. In 2010, 61% of U.S. goods and 72% of agricultural exports went to states in Asia and the Pacific (USTR 2011). East Asia is expected to surpass NAFTA and the Euro zone as the world's largest trading zone as the region adds 175 million more people by 2030 and expects to transport and consume more oil and raw materials (IMF 2011, 31). The widespread destruction of the typhoon had the potential to cause regional economic instability.

Furthermore, Philippine leaders have suggested the U.S. response strengthened the case for a more active and increased military presence in the country (Quismundo 2013; Romualdez 2013). Prior to the typhoon, the United States maintained a considerable air and naval presence in the Western Pacific and stationed thousands of troops in South Korea, Japan, and Guam. The Philippines, in addition to Japan, South Korea, and Taiwan, has sought a greater U.S. military presence to check and balance both China and North Korea and to ensure freedom of navigation and commerce.

In addition, the disaster provided the Obama Administration an opportunity to show the region the good it could do, especially in relation to China. Although China did pledge aid to the Philippines, its initial donation totaled just $100,000, but increased its pledge to $1.6 million and dispatched a hospital ship following global media criticism (Perlez 2013). The total package was a small percentage of the overall amount given by governments. China's response was probably shaped by tensions with the Philippines over disputed islands in the South China Sea and with Japan over the Senkaku/Diaoyu islands, resulting in a buildup of naval forces and air defense zones.

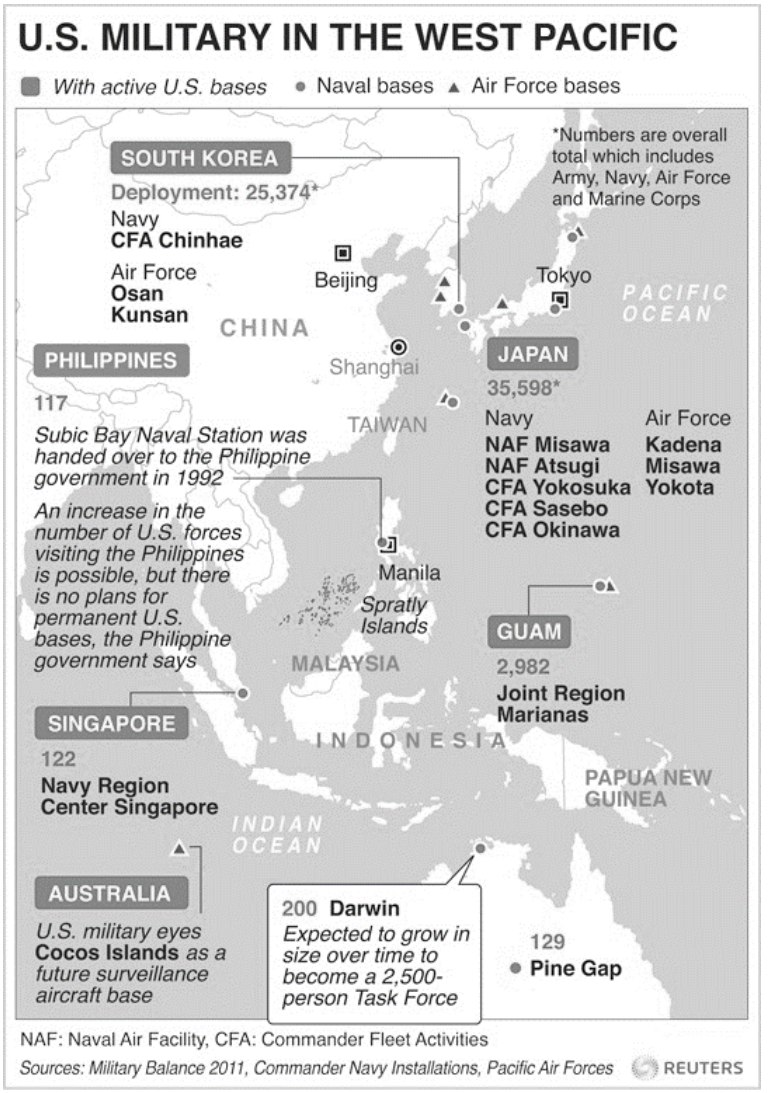
A more powerful and assertive China will probably shape the region in ways that run counter to U.S. interests (Cohen 2010; Fackler 2013; Nathan and Scobell 2012; Swaine 2011). The worry is that China will seek to alter norms and rules in the region, thereby complicating U.S. efforts to maintain the strategic balance of power (Inboden 2011). U.S. concern was most visibly expressed with its decision to increase its military presence to 2,500 Marines deployed to Darwin, Australia. For years, the United States sought to enhance its ship and aircraft access to Philippine military stations, especially at Subic Bay. While U.S. humanitarian assistance to the Philippines was an expression of goodwill, it helped pave the way for the United States to legitimize and expand its military presence in Southeast Asia and rebalance against China in the region (see figure 3). According to Thayer, "It is not that the United States used assistance to promote rebalancing, but that rebalancing enabled the U.S. to respond so decisively" (Mogato and Belford 2013).

Historical Milieu, Media, and the Public

Historical milieu and the roles of the media and the public in the foreign policymaking process determined and shaped the extent of the U.S. response to the typhoon. Previous natural disasters informed the range of options available to the policy elites formulating the U.S. response to the human suffering; however, the type of media coverage and the degree of public engagement with the disaster varied in relation to previous catastrophic events (Oliver and Myers 2002). The case of Typhoon Yolanda is interactive with previous policies and experiences, especially when it comes to the strategic importance of Asia and the Pacific in U.S. foreign policy as well as efforts to address the image of the United States.

Following the 2004 tsunami, U.S. humanitarian assistance and aid to Indonesia helped build goodwill and appreciation and bring about a significant revival following the tsunami by providing it with aid for childhood immunization and to fight corruption and abuse of women, promote human rights, and to train for disaster relief

Figure 3: U.S. Military Force in the Pacific



Source: Military Balance 2011, Commander Navy Installations, Pacific Air Forces, Thomsonreuters: http://blog.thomsonreuters.com/wp-content/uploads/2012/04/military-west-pacific.jpg

and recovery missions. There were also significant military-to-military contacts, such as joint defense operations and the sale of weapons systems (Denmark, Sukma, and Parthemore 2010; Gates 2008; Haseman and Lachica 2005; Rice 2006).

The massive humanitarian operation and subsequent cooperation between the two governments helped improve the image of the United States in Indonesia where anti-U.S. sentiment was strong since the beginning of the Iraq War. Following the March 2003 invasion of Iraq, the percentage of favorable views of the United States fell to 15%, but after the United States participated in humanitarian operations that number jumped to 79%. U.S. assistance improved their impression of the United States

with positive views increasing from 15% in 2003 to 38% in 2005 (Pew Research Global Attitudes Project 2005). At roughly the same time, U.S. public opinion polls revealed that 83% of Americans approved of the U.S. relief mission (ABC News/Washington Post 2004). Favorable views of the United States from Indonesians did not return to pre-Iraq War levels until 2009. According to Blank (2013), "The goodwill the tsunami relief brought the U.S. is incalculable. Nearly a decade later, the effort may rank as one of the most concrete reasons Southeast Asian nations trust the long-term U.S. commitment to a strategy of Asian re-balancing."

The 2004 tsunami was one of the first natural disasters in which global news organizations relied on images and video from individuals in locations where waves crashed onto coastal areas (Macmillan 2005a). The human suffering depicted online and delivered by television served as the foundation for citizen media coverage of subsequent natural disasters and armed conflicts (Handwerk 2005; Macmillan 2005b; Pottinger 2005; Regan 2005; Schwartz 2005). However, it was difficult and challenging for media networks to determine the accuracy and veracity of the overall coverage and extent of the damage.

For the United States, Indonesia is important in maintaining stability in Southeast Asia given its strategic location within maritime transport lines (Caryl 2005; Sullivan 2004). Moreover, the country has experienced terrorism, sectarian violence, and armed conflict. According to former Secretary of State Colin Powell, "This is an investment not only in the welfare of these people; it's an investment in our own national security" (see O'Lery 2005). Given the significance of Indonesia in Asia and the Pacific, the leading government donors of humanitarian assistance committed $717.5 million in 2005 before falling to $184 million in 2011 with U.S. bilateral aid increasing from $43.3 to $82.2 during this same time (GHA 2012).

Then, the United States moved quickly in Japan following the disaster at the Fukushima Daiichi nuclear plant on March 11, 2011. The catastrophic failure of three nuclear reactors occurred when the facility was struck by a tsunami triggered by the Tōhoku earthquake leading to what became the worst nuclear catastrophe since the 1986 Chernobyl disaster. The U.S. responded with Operation Tomodachi to shore up the Japanese Self-Defense Forces (SDF) responding to the disaster with the deployment of roughly 24,000 U.S. military personnel, a carrier group off the coast of Miyagi Prefecture, 19 naval vessels, and 140 aircraft (Wada 2011). U.S. forces aided SDF with the rescue and evacuation of survivors, delivery of meals and safe drinking water, medical assistance, and with repairs to infrastructure (Mizushima 2012). Operation Tomodachi was considered a successful joint humanitarian operation that "validated years of bilateral training, exercises, and planning" and promoted regional economic stability (Mizushima 2012).

Tomadachi was positively received by broad segments of the Japanese population with support for the United States soaring in the wake of the humanitarian operation. Japan's perception of the United States was already positive prior to the nuclear disaster with 66% expressing favorable views of the United States in a spring 2010 poll. One year later, after the tsunami struck Fukushima, that number skyrocketed to 85%, which was the highest positive rating among the 23 nations included in the

poll of the U.S. global image (see table 3) (Pew 2013). A similar survey conducted at the end of 2011 found that 82% expressed a "friendly feeling" toward the United States (Wike 2012).

Table 3: Favorable Views of the United States

Country	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Indonesia	61	15	–	38	30	29	37	63	59	54	–	61
Japan	72	–	–	–	63	61	50	59	66	85	72	69
Philippines	90	–	–	–	–	–	–	–	–	–	–	85

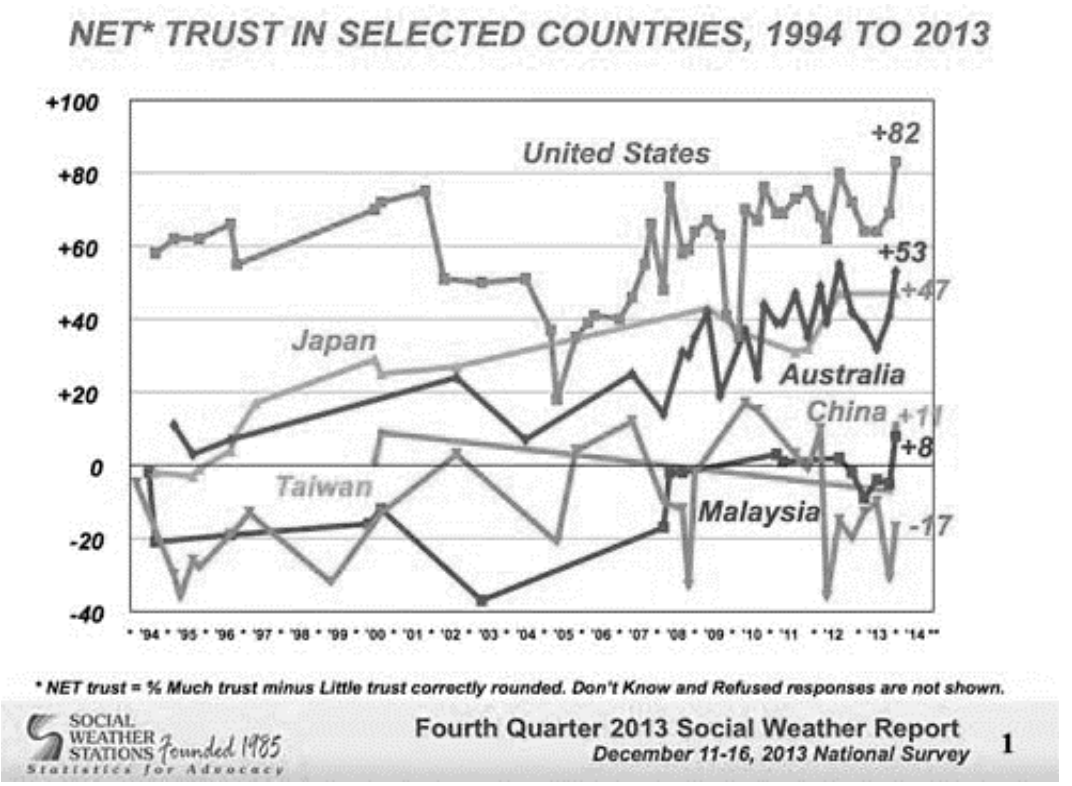
Source: Pew Research Global Attitudes Project (2013a, 2013b)

U.S. relief efforts reinforced America's commitment to Japan, reflecting the significance of the region in U.S. foreign policy and contributing to a general sense of goodwill (Konishi and Oros 2014). For example, 57% of Japanese believed that the United States provided a "great deal" of humanitarian assistance during and after the catastrophe in contrast to the less than 20% who believed the United Nations, European Union, and China provided a "great deal" of aid. Also, many Japanese believed that the United States is a nation that considers the interests of other countries. In 2010, 31% of the Japanese public believed that the United States takes into account the interests of other countries; in the wake of the nuclear disaster and the U.S.-led humanitarian mission, the percentage increases to 51% (Wike 2012). As table 3 demonstrates, the United States received high approval ratings in the Philippines before Typhoon Yolanda with 85% holding favorable views (Pew 2013). Also, many Filipinos consistently viewed the United States as a trusted ally of the Philippines before and after Typhoon Yolanda (see graph 1). In December 2013, one month after the typhoon struck, 82% believed that the United States was the most trusted country, an all-time high (Rood 2014).

The emergence of China as a military power has been viewed with consternation in the Philippines and Japan. Japan has the most negative views of China where only 5% expressed a positive view of China with 82% describing the island disputes and naval tensions as security concerns. While tensions with China are concerns in the Philippines with 84% expressing confidence in President Obama making the right decisions in global affairs. In addition, 67% of Japanese, 67% of Filipinos, and 61% of South Koreans believe that the United States, not China, is the leading economic power in the region (Pew 2013).

Network and social media coverage of the typhoon and its aftermath brought the suffering and plight of the victims to the global community and triggered donations and aid from around the world. CNN International provided 24/7 news coverage of the devastation to Tacloban in Leyete province and the surrounding areas as Philippine government television and private networks were criticized for not providing sufficient exposure of the impact of the typhoon (Reyes 2013). Although the storm was a significant climate event, there were only a few mentions of climate change by some of the global news networks in the coverage of the typhoon. According to Pew, MSNBC

Graph 1: Public Opinion in the Philippines of Select Countries



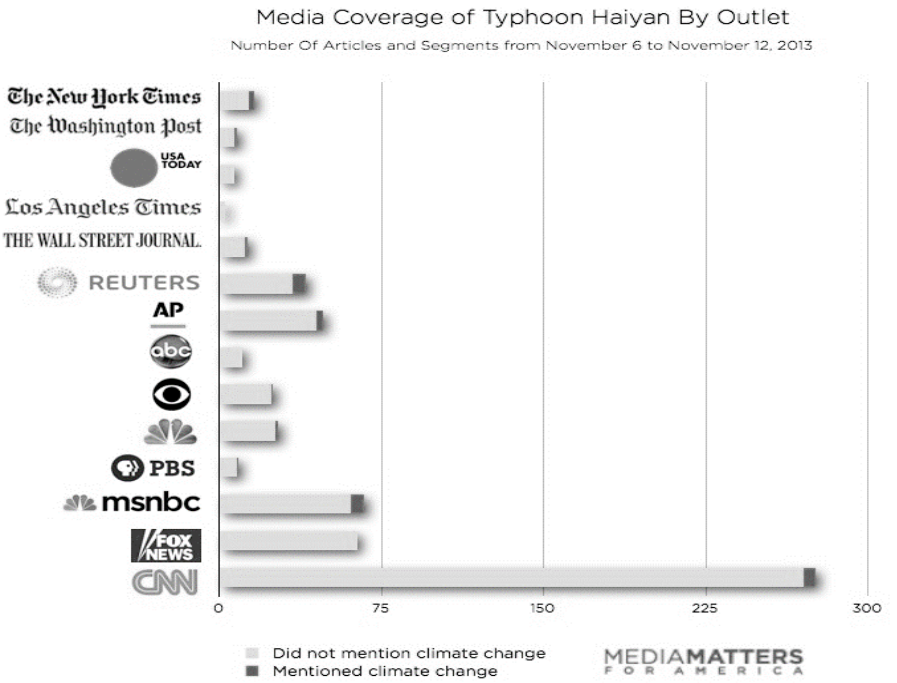
See: Rood (2014)

devoted four times as much coverage to healthcare (over 3 hours) than the typhoon (41 minutes) with Fox News giving 80 times more coverage to healthcare than the typhoon. However, CNN devoted more than 3.5 hours of news coverage to healthcare and roughly 5 hours to the typhoon (Jurkowitz, Vogt, and Anderson 2013) (see figure 4).

Coverage of the typhoon on social media was broader and more widespread than more established global media networks. Data collected by the social media monitoring group Radian6 reported more than 3.2 million general mentions of the typhoon on Facebook and Twitter between November 6 and 14. The highest percentage of mentions (74.9%) was on Twitter, followed by Facebook (19.2%) and mainstream news organizations (2.7%) with comments, blogs, videos, and forum replies filling in the remaining percentages. Those on Twitter were able to spread information and images about the natural disaster and kept content about damage and casualties up to date (Bandojo 2013).

Media coverage focused on Tacloban in Leyete province, which garnered 34.2% of the mentions as measured over the 6-day period between November 8 and 14 with other devastated areas overlooked by media. Many believed that the locus of the storm was in Leyete, even though it carved a destructive path in Cebu, Samar, Bohol, Iloilo, Capiz, Palawan, and Aklan. Perhaps even more important, vital information

Figure 4: Media Coverage of Typhoon Yolanda



Source: Media Matters for America: http://mediamatters.org/research/2013/11/19/typhoon-haiyan-study-finds-media-rarely-covered/196961

about making donations and participating in relief efforts were shared via tweets and mentions on Facebook. Roughly 290,729 posts mentioned "relief efforts," "donations," medical missions," and "financial aid" with regard to the global response to Yolanda. These social mentions peaked on November 12, which coincided with the bulk of the coverage on CNN International (Bandojo 2013).

However, the U.S. public was much less engaged with news coverage of the typhoon than previous natural disasters (see table 4). For example, 32% of Americans closely followed news coverage of the typhoon in comparison to the 55% who closely followed the tsunami and nuclear disaster in Fukushima, and the 58% that closely followed the 2004 Indian Ocean, and the 60% that closely followed the 2010 earthquake in Haiti. Between November 14 and 17 the typhoon was tied with economic news at 32% with healthcare at 37% as the top news story. The percentage of Americans closely following the typhoon mirrored levels of the 2008 earthquake in China (30%) and the 2010 earthquake in Chile (27%) (Pew 2013).

Table 4: Percentage of Americans Following Typhoon Aftermath "Very Closely"

Haiti earthquake	January 2010	60
Indian ocean tsunami	January 2005	58
Japan tsunami	March 2011	55
Philippines typhoon	November 2013	32
China earthquake	May 2008	30
Chile earthquake	March 2010	27
Burma cyclone	May 2008	23
Pakistan earthquake	October 2005	22

Source: Table adapted from Pew Research Center, November 14–17, 2013; Pew Research Center (November 19, 2013): http://www.people-press.org/2013/11/19/philippines-disaster-draws-limited-interest-donations/.

The percentage of Americans donating money and supplies to relief organizations dedicated to helping the Philippines lagged behind efforts to donate to previous natural disasters receiving more media attention. Although many planned to donate to Philippine relief efforts, just 14% made donations, which is less than donations made after Hurricane Katrina (56%), the earthquake in Haiti (52%), and the Indian Ocean (30%), and Fukushima Japan tsunamis (21%). 67% planned on not donating at all, which was the highest of all five natural disasters listed in the Pew survey. U.S. interest in the typhoon was lower across every age cohort. For example 45% of those over 65 closely following the story compared to the 67% who closely followed the 2011 tsunami in Japan and 20% among adults younger than 40 compared with 47% who closely followed the 2011 disaster in Japan (Pew 2013).

Americans contributed more than $300 million to earthquake relief in Haiti within 10 days of the natural disaster compared to more than $33 million to typhoon relief in the Philippines within 7 days of the storm (Hicken 2013; NPR 2010). While private sector donations are more informal and difficult to record, the UN Office for the Coordination of Humanitarian Affairs reported that private organizations and individuals around the world pledged $150 million of the total contributions to Philippines relief (Troilo 2014). Previous humanitarian crises prompted higher amounts of donations from private organizations and individuals. $3.9 billion was raised in response to the 2004 Indian Ocean Tsunami, $1.2 billion for the 2010 Haiti earthquake, and $450 million was given in response to the 2010 floods in Pakistan (Stoianova 2012). It could be that the implementation of America's new healthcare law dominated the headlines and drew attention away from typhoon relief efforts. While this may explain the smaller donations, it does not elucidate the lower contributions from private individuals and organizations across the globe.

Moving Forward

Our approach captures the interactive normative expectations and dynamic institutional and legal mechanisms that push and pull the United States into humanitarian operations. News coverage, public engagement and opinion, and historical milieu played significant roles in Operation Damayan. It is difficult to assess the complex array of factors shaping the U.S. relief effort in response to Typhoon Yolanda in isolation from previous cases. Normative factors, such as alleviating human suffering in the immediate wake of the storm by delivering aid and supplying developmental assistance, were consistent with those observed in the two earlier natural disasters. Strategic considerations were also present as the United States sought to improve its global image, build new and shore up existing alliances and partnerships, expand its economic interests, and increase its military presence in Asia and the Pacific.

Given that Operation Damayan involved real costs and benefits, the United States engaged in a strategic decision to uphold and build its image and reputation with allies while advancing its interests relative to China. U.S. participation was based on humanitarian and human rights grounds even though strategic interests and considerations were at stake. Self-interested motivations are integral to humanitarian action, meaning that strategic interests cannot be separated from efforts to alleviate human suffering (Farer 2005, 235).

References

ABC News/Washington Post. 2004. "Poll: Bush's Ratings Tepid, Expectations Mixed: Iraq Looms Large Over Second Term." http://abcnews.go.com/Politics/PollVault/story?id=419276

Acharya, Amitav, and Barry Buzan. 2010. *Non-Western International Relations Theory: Perspectives On and Beyond Asia*. London: Routledge.

Agence France-Presse. 2013. "Philippines Counts the Cost of Typhoon Haiyan." *Manilla Bulletin*, November 20. http://www.rawstory.com/rs/2013/11/philippines-counts-the-cost-of-typhoon-haiyan/

Ashley, Richard. 1983. "Three Modes of Economism." *International Studies Quarterly* 27 (4): 477–491.

Ashley, Richard. 1988. "Untying the Sovereign State: A Double Reading of the Anarchy Problematique." *Millennium: Journal of International Studies* (June): 227–262.

Bandojo, Jizelle. 2013. "The Anatomy of Social Media Use During #Yolanda." *All Famous Digital*, November 21. http://allfamous.com/trending/a-radian6-report-on-super-typhoon-yolanda/.

Bankoff, Gregg, Dorothea Hilhorst, and George Frerks. 2004. *Mapping Vulnerability: Disasters, Development, and People*. New York: Routledge.

Baum, Matthew. 2002. "The Constituent Foundations of the Rally-Round-the-Flag Phenomenon." *International Studies Quarterly* 46 (2): 263–298.

Bellamy, Alex. 2003. "Humanitarian Responsibilities and Interventionist Claims in International Society." *Review of International Studies* 29: 321–40.

Belloni, Roberto. 2005. "Is Humanitarianism Part of the Problem? Nine Theses." BCSIA Discussion Paper. Kennedy School of Government, Harvard University. April (3): http://belfercenter.ksg.harvard.edu/files/belloni.pdf.

Berinsky, Adam. 2009. *In Time of War: Understanding American Public Opinion from World War II to Iraq*. Chicago, IL: University of Chicago Press.

Biersteker, Thomas J. 1989. "Critical Reflections on Post-Positivism in International Relations." *International Studies Quarterly* 33 (3): 263–267.

Blank, Jonah. 2013. "How Philippines Typhoon Aid Helps USA: Rescue Efforts Boost America's Image in Asia." *USA Today*, November 14.

Bob, Clifford. 2005. *The Marketing of Rebellion: Insurgents, Media, and International Activism*. Cambridge: Cambridge University Press.

Burstein, Paul. 2003. "The Impact of Public Opinion on Public Policy: A Review and an Agenda." *Political Research Quarterly* 56 (1): 29–40.

Butler, Karina. 2001. *A Critical Humanitarian Intervention Approach*. New York: Palgrave.

Buzan, Barry. 2004. *From International to World Society?: English School Theory and the Social Structure of Globalization*. Cambridge: Cambridge University Press.

Caryl, Christian. 2005. "The Twists of Fate." *Newsweek*, January: 23.

Chayes, Abram, and Antonia Handler Chayes. 1996. *Preventing Conflict in the Post-Communist World: Mobilizing International and Regional Organizations*. Brookings Occasional Papers.

Chopra, Jaret, and Thomas G. Weiss. 1992. "Sovereignty Is No Longer Sacrosanct: Codifying Humanitarian Intervention." *Ethics and International Affairs* 6: 95–117.

Claude, Inis. 1966. "Collective Legitimization as a Political Function of the United Nations." *International Organization* 20(3) (Summer): 367–379.

Clinton, Hillary. 2011. "America's Pacific Century." *Foreign Policy*, October 11. http://www.foreignpolicy.com/articles/2011/10/11/americas_pacific_century (accessed March 2, 2014).

Coates, Anthony. 2003. "Humanitarian Intervention: A Conflict of Traditions." In *Humanitarian Intervention*, eds. Terry Nardin and Vanessa Williams. New York: New York University Press.

Cohen, Warren I. 2010. *America's Response to China: A History of Sino-American Relations*. New York: Columbia University Press.

Cox, Robert. 1999. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millennium: Journal of International Studies* 10 (2): 126–155.

Dean, Carolyn J. 2003. "Empathy, Pornography and Suffering." *difference: A Journal of Feminist Cultural Studies* 14: 88–124.

de Leon, Sunshine and Alexandra Zavis. 2013. "Philippines Typhoon Leaves Millions in Need of Food, Water, Shelter." *Los Angeles Times*, November 11.

Denmark, Abraham B., Rizal Sukma, and Christine Parthemore. 2010. *Crafting a Strategic Vision: A New Era of U.S.-Indonesia*. Center for a New American Security. June. http://www.cnas.org/files/documents/publications/CNAS_Crafting%20a%20Strategic%20Vision_Denmark.pdf.

Devetak, Richard A. 2007. "Between Kant and Pufendorf: Humanitarian Intervention, Statist Anti-Cosmopolitanism and Critical International Theory." *Review of International Studies* 33: 151–174.

Donnelly, Jack. 1993. "Human Rights, Humanitarian Crisis, and Humanitarian Intervention." *International Journal* 48 (4): 607–640.

Ehrlich, Sean and Cherie Maestas. 2010. "Risk, Risk Orientation, and Policy Opinions: The Case of Free Trade." *Political Psychology* 31 (5): 657–684.

Fackler, Martin. 2013. "China Is Seen Nearing U.S.'s Military Power in Region." *New York Times*, May 2: A4.

Farer, Tom. 2005. "Roundtable: Humanitarian Intervention After 9/11." *International Relations* 19 (2): 211–250.

Feaver, Peter D. 1998. "Public Opinion and Foreign Policy: Bridging the Gap." *TISS Report*. http://www.unc.edu/depts/diplomat/AD_Issues/amdipl_9?goodnight_disc2.html.

Feaver, Peter D. and Christopher Gelpi. 2004. *Choosing Your Battles: American Civil-Military Relations and the Use of Force.* Princeton, N.J.: Princeton University Press.

Finnemore, Martha. 1996. *National Interests in International Society*, New York: Cornell University Press, 2–3.

Fisher, Max. 2014. "47 Statistics That Explain Typhoon Haiyan." *Washington Post*, November 12. http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/12/47-statistics-thatexplain-typhoon-haiyan/.

Fixdal, Mona, and Dan Smith. 1998. "Humanitarian Intervention and Just War." *Mershon International Studies Review* 42 (2): 283–312.

Franck, Thomas, and Nigel Rodley. 1973. "After Bangladesh: The Law of Humanitarian Intervention by Force." *American Journal of International Law* 67: 275–305.

Frizis, Iakov. 2013. "The Impact of Media on Foreign Policy." *e-International Relations*, May 10. http://www.e-ir.info/2013/05/10/the-impact-of-media-on-foreign-policy/.

Gartner, Scott S. 2008. "The Multiple Effects of Casualties on Public Support for War: An Experimental Approach." *American Political Science Review* 102 (1): 95–106.

Gartner, Scott S. and Gary M. Segura. 1998. "War, Casualties, and Public Opinion." *Journal of Conflict Resolution* 42 (3): 278–300.

Gates, Robert. 2008. "Gates Pledges U.S. Support to Indonesian Military." February 25. http://archive.defense.gov/news/newsarticle.aspx?id=49061.

Gelpi, Christopher, Peter Feaver, and Jason Reifler. 2005/2006. "Success Matters: Casualty Sensitivity and the War in Iraq." *International Security* 30 (3): 7–46.

Gibbs, David. 2009. *First Do No Harm: Humanitarian Intervention and the Destruction of Yugoslavia*. Nashville, TN: Vanderbilt University Press.

Gil de Zúñiga, Homero, Nakwon Jung, and Sebastián Valenzuela. 2012. "Social Media Use for News and Individuals' Social Capital, Civic Engagement and Political Participation." *Journal of Computer Mediated Technology* 17 (3): 319–326.

Gladstone, Rick. 2013. "Top U.N. Relief Official Flies to Philippines to Help Coordinate Aid Efforts." *New York Times*, November 11: A12.

Global Humanitarian Assistance (GHA). 2012a. "Philippines: Key Figures 2012." http://www.globalhumanitarianassistance.org/countryprofile/philippines

Global Humanitarian Assistance (GHA). 2012b. "Indonesia: Key Figures 2012." http://www.globalhumanitarianassistance.org/countryprofile/indonesia.

Gowing, Nik. 1994. "Real Time Television Coverage of Armed Conflicts and Diplomatic Crises: Does it Pressure or Distort Foreign Policy Decisions." The Joan Shorenstein Center on the Press, Politics and Public Policy. http://www.ksg.harvard.edu/presspol/Research_Publications/Papers/Working_Papers/94_ 1.pdf.

Handwerk, Brian. 2005. "Tsunami Blogs Help Redefine News and Relief Effort." *National Geographic News*. http://news.nationalgeographic.com/news/2005/01/0126_050126_tv_tsunami_blogs.htm.

Haseman, John, and Eduardo Lachica. 2005. "Toward a Stronger U.S.-Indonesia Security Relationship." *USINDO*, August.

Henckaerts, Jean-Marie, and Louise Doswald-Beck. 2009 *Customary International Humanitarian Law*. Cambridge, UK: ICRC.

Hicken, Melanie. 2013. "Major Charities Raise Millions for Typhoon Haiyan Victims." *CNN Money*, November 15. http://money.cnn.com/2013/11/15/pf/typhoon-haiyan-donations/.

Hildebrandt, Timothy, Courtney Hillebrecht, Peter Holm, and Jon Pevehouse. 2013. "The Domestic Politics of Humanitarian Intervention: Public Opinion, Partisanship, and Ideology." *Foreign Policy Analysis* 9 (3): 1–24.

Howell, William, and Jon C. Pevehouse. 2005. "Presidents, Congress, and the Use of Force." *International Organization* 59 (1): 209–232.

Ignatieff, Michael. 1998. "The Stories We Tell: Television and Humanitarian Aid." In *Hard Choices: Moral Dilemmas in Humanitarian Intervention*, eds. Jonathan Moore. Lanham, MD: Rowman & Littlefield.

Inboden, Will. 2011. "What Obama's Done Right—And Wrong." *Foreign Policy*, December 28. http://foreignpolicy.com/2011/12/28/what-obamas-done-right-and-wrong/ (accessed March 3, 2014).

International Committee of the Red Cross (ICRC). 1977. "Article 18(2) of the 1977 Additional Protocol II." *Practice Relating to Rule 55. Access for Humanitarian Relief to Civilians in Need.* https://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule55_sectiond

International Monetary Fund (IMF). 2011. "Changing Patterns of Global Trade." June 15. http://www.imf.org/external/np/pp/eng/2011/061511.pdf (accessed March 12, 2014

Jacobs, Andrew. 2013. "Relief Supplies Pour into Philippines, but Remote Areas Still Suffer." *New York Times*, November 16: A10.

Jacobs, Lawrence R., and Benjamin Page. 2005. "Who Influences Foreign Policy?" *American Political Science Review* 99 (1): 107–123.

Janse, Ronald. 2006. "The Legitimacy of Humanitarian Interventions." *Leiden Journal of International Law* 19: 669–692.

Jentleson, Bruce. 1992. "The Pretty Prudent Public: Post Post-Vietnam American Opinion on the Use of Military Force." *International Studies Quarterly* 36 (2): 49–74.

Jurkowitz, Mark Paul Hitlin, Nancy Vogt, and Monica Anderson. 2013. "Obamacare v. Philippines Typhoon: How Cable Covered Two Big Stories." *Pew Research*, November 20. http://www.pewresearch.org/fact-tank/2013/11/20/obamacare-v-philippines-typhoon-how-cable-covered-two-big-stories/.

Kam, Cindy, and Donald R. Kinder. 2008. "Terror and Ethnocentrism: Foundations of American Support for the War on Terrorism." *Journal of Politics* 69 (2): 320–338.

Klarevas, Louis. 2002. "The 'Essential Domino' of Military Operations: American Public Opinion and the Use of Force." *International Studies Perspectives* 3 (4) (November).

Konishi, Weston S., and Andrew L. Oros. 2014 "Beyond Haiyan: Toward Greater U.S.-Japan Cooperation in HADR." *NBR Analysis Brief*, February 6. http://nbr.org/publications/analysis/pdf/brief/020614_Kinoshi-Oros_US-Japan_HADR.pdf.

Kuperman, Alan. 2008. "The Moral Hazard of Humanitarian Intervention: Lessons From the Balkans." *International Studies Quarterly* 52 (1): 49–80.

Linklater, Arthur. 1998. *The Transformation of Political Community: Ethical Foundations of the Post-Westphalian Era*. Cambridge: Polity Press.

Livingston, Stephen. 1997. "Clarifying the CNN Effect: An Examination of Media Effects According to Type of Intervention." Research Paper R-18, Joan Shorenstein Center, Press-Politics. http://shorensteincenter.org/wp-content/uploads/2012/03/r18_livingston.pdf.

Mack, Andrew. 2004. "A Signifier of Shared Values." *Security Dialogue* 35 (3): 366–367.
Macmillan, Robert. 2005a. "Editing Citizen Journalism." *Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2005/07/22/AR2005072200588.html.

Macmillan, Robert. 2005b. "Tsunami Prompts Online Outpouring." *Washington Post*, January 3. http://www.washingtonpost.com/wp-dyn/articles/A44262-2005Jan3.html.

Marszal, Andrew. 2013. "Philippines Rebel Deal Could end Decades-long Bloody Insurgency." *The Telegraph*, December 8. http://www.telegraph.co.uk/news/worldnews/asia/philippines/10504080/Philippines-rebel-deal-could-end-decades-long-bloody-insurgency.html (accessed February 16, 2014).

McGowen, Patrick J. 1974. "Adaptive Foreign Policy Behavior: An Empirical Approach." In *Comparing Foreign Policies: Theories, Findings, and Methods*, ed. James Rosenau. New York: Sage Publications.

McPhail, C., D. Schweingruber, and J. McCarthy. 1998. "The Policing of Protest in the United States, 1960–1995." In *Policing Protest: the Control of Mass Demonstrations in Western Democracies*, eds. Donatella della Porta and Herbert Reiter. Minneapolis, MN: University of Minnesota Press.

Minear, Larry, Colin Scott, and Thomas G. Weiss. 1996. *The News Media, Civil War, and Humanitarian Action*. Boulder, CO: Lynne Rienner Publishers.

Mizushima, Ashaho. 2012. "The Japan-US 'Military' Response to the Earthquake, and the Strengthening of the Military Alliance as a Result." *Fukushima on the Globe*, December 10. http://fukushimaontheglobe.com/the-earthquake-and-the-nuclear-accident/whats-happened/the-japan-us-military-response#sthash.HhU8vxxM.dpuf.

Mogato, Manuel, and Aubrey Belford. 2013. "Dramatic U.S. Humanitarian Effort in Philippines Aids Asia Pivot." *Reuters*, November 18. http://www.reuters.com/article/2013/11/18/philippines-typhoon-pivot-idUSL4N0J30OQ20131118.

Mueller, John C. 1994. *Policy and Opinion in the Gulf War*. Chicago, IL: University of Chicago Press.

Mueller, John C. 2005. "The Iraq Syndrome." *Foreign Affairs* 84 (6): 44–54.

Nathan, Andrew, and Andrew Scobell. 2012. *China's Search For Security*. New York: Columbia University Press.

National Public Radio (NPR). 2010. "Haiti Relief: Donating Via Text and Avoiding Scams." January 21. http://www.npr.org/templates/story/story.php?storyId=122818475.

O'Lery, Conor. 2005. "US Realises Late that Aid to Muslims Enhances its Image." *Irish Times*, January 5: 14.

Oliver, Pamela E., and Daniel J. Myers. 2002. "The Coevolution of Social Movements." *Mobilization: An International Quarterly* 8: 1–24.

Orford, Anne. 2003. *Reading Humanitarian Intervention: Human Rights and the Use of Force in International Law*. Cambridge: Cambridge University Press.

Organization of American States (OAS). 1967. "Charter of the Organization of American States, Article 18." United States Treaties 2394. Treaties and Other International Actor Series No. 2361: http://www.oas.org/dil/treaties_A-41_Charter_of_the_Organization_of_American_States.pdf.

Page, Benjamin, Robert Y. Shapiro, and Glenn Dempsey. 1987. "What Moves Public Opinion?" *American Political Science Review* 81: 23–44.

Palen, Leysia, and Sophia B. Liu. 2007. "Citizen Communications in Crisis: Anticipating a Future of ICT-Supported Participation." *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI 2007): 727–736.

Paris, Roland. 2001. "Human Security: Paradigm Shift or Hot Air?" *International Security* 26 (2): 87–102.

Pelling, Mark. 2003. *The Vulnerability of Cities: Natural Disasters and Social Resilience*. New York: Routledge.

Perlez, Jane. 2013. "China Increases Aid to Philippines," *New York Times* (November 14): http://www.nytimes.com/2013/11/15/world/asia/chinese-aid-to-philippines.html?_r=0

Pew Research Center (Pew). 2013. "Philippines Disaster Draws Limited Interest, Donations." November 19. http://www.people-press.org/2013/11/19/philippines-disaster-draws-limited-interest-donations/#news-interest.

Pew Research Global Attitudes Project. 2005. "U.S. Image Up Slightly, But Still Negative." June 23. http://www.pewglobal.org/2005/06/23/us-image-up-slightly-but-still-negative/.

Pew Research Global Attitudes Project. 2013a. "America's Global Image Remains More Positive Than China's." July 18. http://www.pewglobal.org/2013/07/18/americas-global-image-remains-more-positive-than-chinas/.

Pew Research Global Attitudes Project. 2013b. "Chapter 1: Attitudes Toward the United States." July 18. http://www.pewglobal.org/2013/07/18/chapter-1-attitudes-toward-the-united-states/.

Pham, J. Peter. 2004. "An Immense Charge: Realist Lessons About the Consequences of Intervention." *National Interest*, May 26.

Philips, Tom. 2013. "Typhoon Haiyan: Tacloban Deputy Mayor Calls on Rebels to Avoid Armed Violence." *The Telegraph*, November 14. http://www.telegraph.co.uk/news/worldnews/asia/philippines/10448673/Typhoon-Haiyan-Tacloban-deputy-mayor-calls-on-rebels-to-avoid-armed-violence.html.

Pottinger, Matt. 2005. "For German Survivor, Search for Loved One Prolongs Nightmare." *Wall Street Journal*, January 3. http://online.wsj.com/news/articles/SB110469358670614588.

Putnam, Robert. 1988. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42 (Summer): 427–460.

Quismundo, Tarra. 2013. "Storm Showed We Need US-Del Rosario." *Philippines Daily Inquirer*, November 26.

Regan, Tom. 2005. "Citizen Journalists Pass the Test in London." *Christian Science Monitor*, July 8. http://blogs.csmonitor.com/bandwidth/2005/07/citizen_journal.html.

Reus-Smit, Christian. 2001. "Human Rights and the Social Construction of Sovereignty." *Review of International Studies* 27: 519–538.

Reyes, Leo. 2013. "Filipinos Praise International Media for Typhoon Haiyan Report." *Digital Report*, November. http://digitaljournal.com/article/362151 (accessed March 4, 2014).

Rice, Condoleezza. 2006. "Remarks at the Indonesia World Affairs Council." March 15. http://2001-2009.state.gov/secretary/rm/2006/63160.htm.

Romualdez, Babe. 2013. "Babe's Eye View: Thank God for the United States!" *Philippines Star*, November 17. http://www.philstar.com/opinion/2013/11/17/1257688/thank-god- united-states.

Rood, Steven. 2014. "Philippines to the World: Thanks for the Haiyan Help." *In Asia: Weekly Insight and Analysis*, January 29. http://asiafoundation.org/in-asia/2014/01/29/philippines-to-the-world-thanks-for-haiyan-help/.

Rosenau, James. 1969. *Linkage Politics*. New York: Free Press.

Rosenau, James. 1970. "Foreign Policy as Adaptive Behavior: Some Preliminary Notes for a Theoretical Model." *Comparative Politics* 2: 367.

Rosenau, James. 1992. "Governance, Order, and Change in World Politics." In *Governance Without Government: Order and Change in World Politics*, eds. James Rosenau and Ernst-Otto. New York: Cambridge University Press.

Schwartz, James. 2005. "Myths Run Wild in Blog Tsunami Debate." *New York Times*, January 3. http://www.nytimes.com/2005/01/03/international/worldspecial4/03bloggers.html.

Shaw, Martin. 2000. *Theory of the Global State: Globality as an Unfinished Revolution*. Cambridge: Cambridge University Press.

Shirky, Clay. 2011. "The Political Power of Social Media: Technology, The Public Sphere, and Social Change." *Foreign Affairs*, January/February.

Sinclair, Timothy J. 1996. "Beyond International Relations Theory." In *Approaches to World Order*, eds. Robert W. Cox and Timothy J. Sinclair. Cambridge: Cambridge University Press.

Sobel, Richard. 2003. *The Impact of Public Opinion on U.S. Foreign Policy Since Vietnam: Constraining the Colossus*, New York: Oxford University Press.

Stoffels, Ruth Abril. 2004. "Legal Regulation of Humanitarian Assistance in Armed Conflict: Achievements and Gaps." *International Review of the Red Cross* 86 (855) (September): 519–520.

Stoianova, Velina. 2012. "Private Funding: An Emerging Trend in Humanitarian Donorship." April. http://www.globalhumanitarianassistance.org/wp- content/uploads/2012/04/Private-funding-an-emerging-trend.pdf

Strobel, Warren. 1997. *Late Breaking Foreign Policy*, Washington, DC: United States Institute of Peace.

Sullivan, Carl. 2004. "Tsunami and War." *Newsweek*, December 29.

Swaine, Michael D. 2011. *America's Challenge: Engaging a Rising China in the Twenty-First Century*. Washington, DC: Carnegie Endowment for International Peace.

Thakur, Ramesh. 2004. "A Political Worldview." *Security Dialogue* 35 (3): 347–348.

Thorson, Stuart J. 1974. "National Political Adaptation." In *Comparing Foreign Policies: Theories, Findings, and Methods*, ed. James Rosenau. New York: Sage Publications.

Troilo, Peter. 2014. "Private Sector Stepping Up in the Philippines." January 27. https://www.devex.com/en/news/private-sector-stepping-up-in-the-philippines/82729.

United Nations Office for the Coordination of Humanitarian Affairs. 2013. "Typhoon Haiyan Latest Reports." http://www.unocha.org/philippines and http://www.unocha.org/aggregator/sources/117.

United Nations Office for the Coordination of Humanitarian Affairs. 2013. "Philippines: Typhoon-Haiyan Situation Report No. 17." November 25. http://reliefweb.int/sites/reliefweb.int/files/resources/OCHAPhilippinesTyphoonHaiyanSitrepNo17.25November2013.pdf.

United States Agency for International Development (USAID). 2013. "USAID Facts on U.S. Aid for Typhoon Victims in Philippines, Fact Sheet #11, Fiscal Year (FY) 2014." *Philippines -Typhoon Yolanda/Haiyan*, November 22. http://iipdigital.usembassy.gov/st/english/texttrans/2013/11/20131113286673.html#axzz3LhHRysnV.

United States Agency for International Development (USAID). 2014. "Humanitarian Assistance." http://www.usaid.gov/philippines/humanitarian-assistance.

United States Trade Representative (USTR). 2011. "U.S. Trade Representative, the United States in the Trans-Pacific Partnership." November. http://www.ustr.gov/about-us/press-office/fact-sheets/2011/november/united-statestrans-pacific-partnership.

Wada, Shuichi. 2011. "Japan Chair Platform: Operation Tomodachi in Miyagi Prefecture: Success and Homework." *Center for Strategic and International Studies*, December 21. https://csis.org/publication/operation-tomodachi-miyagi-prefecture-success-and-homework.

Wendt, Alexander. 1995. "Constructing International Politics." *International Security* 20 (Summer) (1): 71–81.

Wheeler, Nick. 2000. *Saving Strangers: Humanitarian Intervention in International Society*. Oxford: Oxford University Press.

Wheeler, Nick. 2004. "Humanitarian Intervention after 9/11." In *Humanitarian Intervention*, ed. Anthony Lang. Georgetown: Georgetown University Press.

Wike, Richard. 2012. "Does Humanitarian Aid Improve America's Image?" *Pew Research Center: Global Attitudes and Trends*, March 6. http://www.pewglobal.org/2012/03/06/does-humanitarian-aid-improve-americas-image/.

Wilkenfeld, Jonathan. 1973. *Conflict Behavior and Linkage Politics*. New York: David McKay.

Williams, Anthony D. 2013. "Crowdsourcing Solutions to Global Problems." *Global Solution Networks*. http://gsnetworks.org/wp-content/uploads/2013/10/Williams-Crowdsourcing.pdf.

Wisner, Ben, Piers Blaikie, Terry Cannon, and Ian Davis. 2003. *At Risk: Natural Hazards, People's Vulnerability and Disasters*. New York: Routledge.

An Assessment of Lone Wolves Using Explosive-Laden Consumer Drones in the United States

Matthew Hughes[A] & James Hess[B]

The recent advent of the consumer drone offers terrorists new capabilities in sophisticated attacks, particularly lone wolves who can afford these drones and benefit from standoff and other features. Although terrorists have not yet employed explosive-laden drones in domestic attacks, drones available on the market can carry a payload sufficient to achieve lethal or destructive objectives sought by lone wolves motivated by diverse ideologies targeting long-term static, short-term static, or mobile targets. The Diffusion of Innovations Theory suggests that explosive-laden drones are not an immediate threat, but as pioneering terrorists experiment with consumer drones, this tactic may become more commonplace as existing defense mechanisms fail to protect targeted buildings, events and individuals. As consumer drones become more popular and more sophisticated, countermeasures and government policies must keep stride with this new and evolving threat.

Keywords: *analysis, lone wolf, terrorism, drones, national security*

Introduction

Lone wolf terrorism gains increasing media coverage as attack frequency and death tolls increase, but such attacks are also a testing ground for innovation. Advances in technology, competition in manufacturing and the diffusion of ideas through media arm the individual terrorist with a wider assortment of weapons and knowledge over time. On January 7, 2013, the Chinese drone manufacturer DJI released the Phantom drone for $679, marking the advent of the consumer drone and the availability of affordable drones to the public (Ripley 2015, 68). Though designed for drone enthusiasts and a variety of commercial and recreational uses, nefarious actors began experimenting with consumer drones. Outside the United States (US), there have been at least a dozen instances of terrorists attempting to use drones in an attack, either to carry an explosive to a target or to deliver a chemical agent (Quan 2014). While established terrorist organizations, mainly in the Middle East, experiment with larger captured drones or expensive models, consumer drones offer capabilities of bypassing traditional security measures to small organizations and sole individuals at affordable prices. In September 2013, a member of the German Pirate Party crashed a Parrot quadcopter near the feet of German chancellor Angela Merkel at a campaign rally in Dresden in order to protest government drone surveillance

[A] MA Candidate, School of Global and Security Studies, American Military University
[B] Associate Professor, School of Global and Security Studies, American Military University
doi: 10.18278/gsis.2.1.5

(Gallagher 2013). The motive was purely political, but the proximity of the drone to a head of state revealed a new challenge for security forces to tackle. Another high-profile incident occurred in January 2015, when a government employee accidently crashed his friend's DJI Phantom quadcopter into the White House lawn (Schmidt and Shear 2015). The innocent mistake exposed vulnerabilities of one of the most protected sites on U.S. soil and demonstrated how a sole actor can circumvent traditional security measures to gain access and proximity to a target. Just 3 months later, Japanese police arrested a man who landed a drone carrying a bottle of radioactive sand on the roof of the Japanese Prime Minister's Tokyo office (Abbott et al. 2016, 12, 14). Although many drone incidents are unintentional or carried out without harmful intent, these events highlight a relatively new capability available to the public, particularly lone wolf terrorists who may procure explosives, purchase a consumer drone and conduct an attack independently. The gravity of this drone risk increases each year, as the FAA estimates that "by 2020 there could be as many as 30,000 drones in the sky in the United States alone" (McKelvey, Diver, and Curran 2015, 44). Government policies lag far behind this evolving threat, presenting significant concerns for the near future.

What is the feasibility of a lone wolf using an explosive-laden consumer drone to conduct an attack in the United States? This question necessitates a thorough investigation of trends among lone wolf attacks and profile characteristics of a lone wolf in the United States, capabilities of drones currently on the market, modern and future defense measures, legislation relevant to drone flight and sales. Given current conditions, a reasonable hypothesis is that if the U.S. Government stalls in producing legislation relevant to consumer drones and corporations fail to take adequate steps in enhancing defense measures, then the feasibility of a lone wolf's use of an explosive-laden consumer drone increases, as does the probability of success in targeting infrastructure, the public or a high-profile individual. The purpose of this study is therefore three-fold: (1) to analyze the feasibility for a lone wolf to use an explosive-laden consumer drone in an attack within the United States; (2) to assess the vulnerabilities and security gaps based on current defense mechanisms and forecasted drone capabilities; and (3) provide recommendations for further analysis of relevant threats and risk mitigation strategies.

Analytical Framework

This study investigates the security concern that lone wolf terrorists may affix explosives to consumer drones for use in a domestic terrorist attack. The independent variable in this research is the feasibility of employing an explosive-laden consumer drone in a terrorist attack in the United States. Independent variables include consumer drone capabilities and limitations (present and future), relevant domestic lone wolf terrorism trends (i.e., target type, weapon of choice, ideologies), defense mechanisms and policies governing drone manufacture and use.

Analysis in this study relies on the assumption that lone wolf terrorism trends will generally remain consistent in the near future. Another assumption is that consumer drone technology will continue to improve and popularity will continue to

grow as forecasted by researchers. The Diffusion of Innovations Theory, introduced by French sociologist Gabriel Tarde in 1903 and further developed by E.M. Rogers in 1995, closely relates to this study of terrorists' use of consumer drones. This theory investigates "the conditions which increase or decrease the likelihood that a new idea," such as using an explosive-laden consumer drone in a terrorist attack, "will be adopted by members of a given culture," such as lone wolf terrorists in the United States ("Diffusion of Innovations Theory" 2016). Conditions contributing to the likelihood of lone wolves using drones include types of targets, advantages achieved through use of a drone, availability and cost, payload capacity, and the ability to use a drone as a lone operator with little training or practice. Rogers explained innovation "consists of four stages: invention, diffusion through the social system, time, and consequences" ("Diffusion of Innovations Theory" 2016). These stages represent factors influencing how ideas spread through a society and the rate at which members of that society adopt these ideas. Rogers elaborated on diffusion, stating that there are five categories of adopters, all following a standard deviation curve, with innovators espousing the new idea in the earliest stages (2.5%), early adopters following suit shortly thereafter (13.5%), the early majority (34%), the late majority (34%), and the laggards (16%) ("Diffusion of Innovations Theory" 2016). In regard to the consumer drone dilemma, terrorists, in general, remain in the invention phase as innovators experiment with the concept of delivering explosives in an attack via air. As terrorists continue to experiment with drones, the probability of such an attack increases as consumer drones become more widely available and the government lags behind in legislation and restrictions.

Analysis and Findings

It is necessary to thoroughly review trends among past lone wolf attacks in the United States in order to assess implications of new consumer drone technology available to terrorists. Trends reveal commonalities in target selection and aid in predictive analysis. Comparing drone models currently on the market reveals potential new capabilities for lone wolves, helping to discern how such terrorists might employ drones against select targets. A study of strengths and weaknesses of various defense mechanisms further sheds light on weaknesses in homeland security. A careful study of these factors exposes faults and gaps that must change, aiding in determining the most practical recommendations to shore up these vulnerabilities.

Lone Wolf Terrorism within the United States

Established terrorist groups have attempted to use drones in attacks, but most incidents have occurred in the Middle East. With large sums of money and resources, these groups have had the means to purchase or capture a drone and equip it with explosives. Even so, large groups such as Al-Qaeda or the Islamic State have not conducted a drone attack in the United States, preferring to use bombs or firearms in attacks. Payoffs involved in utilizing consumer drones generally do not support these larger terrorist groups' objectives. The limited payload of consumer drones does not

support the large bombs and high death tolls characteristic of Al-Qaeda or Islamic State attacks. Similarly, martyrdom is a chief objective sought after by Islamic State operatives, who either conduct a suicide attack equipped with a bomb on their person or plan a complex attack, shooting a crowd until killed. Such groups generally use bombs and firearms in attacks and seek shock and awe through publicity, but utilizing a drone detracts from this objective given the limited carnage. These factors may explain why larger terrorist groups, which have the resources and means to purchase or capture a drone and equip the drone with explosives, have not attempted such an attack in the United States.

The closest semblance of a specialized attack with a drone occurred when the FBI foiled a plot in September 2011 involving large model aircraft. The FBI arrested Rezwan Ferdaus, a Massachusetts-based Al-Qaeda supporter, who planned to target the Pentagon and East Potomac Park with model aircraft packed with explosives supplied by FBI undercover employees he believed to be Al-Qaeda operatives ("Man Sentenced" 2012). Although the scenario did not meet criteria for a lone wolf incident, Ferdaus' independent purchase of model aircraft, personal surveillance of targets, and innovative plot to fly explosive-laden model planes into targets demonstrates the feasibility of a sole actor acquiring the materials necessary for a similar attack. Large terrorist groups have had the means to conduct an attack with drones, Consumer drones seem particularly attractive to lone wolves, as opposed to members of established terrorist groups, due to affordable prices, risk-averse utility, and payoffs closely aligned with objectives of lone wolf terrorists, as evidenced by trends of domestic lone wolf terrorism.

In the past, the expensive nature of aerial platforms likely deterred lone wolves from experimenting with such a tool in an attack. Individuals plotting without outside resourcing or support were generally restricted to either stealing an industrial drone used for crop dusting or commercial purposes or purchasing an expensive model through hobbyist channels. High costs and restrictive supply channels made such a prospect highly unlikely to domestic lone wolves, who were generally "unemployed, single white males with a criminal record" (Hamm and Spaaj 2015, 6). Trends since 2012 indicate domestic terrorists are younger and often without a criminal record due to their youth, largely due to Islamic State recruiting efforts on social media platforms. Consumer drones, with popular models priced below $2,000 and likely to become more affordable in coming years, are now within purchasing ability of the typical lone wolf in the United States. Purchasing these models does not require a background check, nor is specialized training required to operate these drones, enabling an individual to acquire and gain proficiency on a drone with minimal personal interactions.

Consumer drones offer advantages to risk-averse lone wolves. Lone wolves in the United States generally "mix personal vendettas with established ideologies," seeking political change or retaliation for some perceived wrong while maintaining a degree of self-preservation (Eby 2012, 34). The most common ideologies fueling attacks include Islamist, anti-government, anti-abortion, racism, and personal motivations. Between September 11, 2011 and June 30, 2016, approximately 40.3% of domestic lone wolf incidents were motivated by Islamist ideologies, in many cases inspired by

Islamic State propaganda on social media platforms (Hughes 2016, 66). While Islamist terrorists can certainly employ consumer drones in attacks, lone wolves responsible for attacks motivated by anti-government, anti-abortion, and other ideologies might be more prone to using drones for the safety benefits. Such terrorists generally have a stronger sense of self-preservation than religiously motivated terrorists seeking glory and martyrdom, such as followers of Al-Qaeda and the Islamic State. Physical standoff afforded by consumer drones, with up to a 2,000-m reliable range, grant lone wolves greater chances for evasion following an attack (Abbott et al. 2016, 5). This distance and the ability to fly an explosive-laden drone into a target remotely avoids risks associated with security video footage and access control points scanning or checking identification.

Trends in domestic lone wolf terrorism indicate the utilization of consumer drones would yield strong benefits for lone wolves. Bombs were the weapon of choice in 54% of domestic lone wolf attacks between 2001 and 2012 (Eby 2012, 37). Consumer drones provide a means to deliver a bomb in a way that bypasses traditional security measures hindering placement by hand. Aerial delivery also reduces the risk of discovery of the bomb prior to detonation, as the terrorist can fly the bomb to the target and detonate the bomb once within an acceptable blast radius. Between 2001 and 2012, lone wolf targets included buildings (43% of cases), the public (37%), a person or place of interest (14%), and infrastructure (4%), with the remaining 2% of targets unknown to law enforcement (Eby 2012, 33). Consumer drones provide lone wolves the means to bypass security features around buildings, such as perimeter fences and access control points. Drones can also increase the carnage in an attack targeting the public by detonating a bomb at a slightly higher altitude and increasing the blast radius, or achieve greater proximity to a person of interest by guiding the drone remotely past personal security escorts and guards.

The advent of consumer drones, now affordable and widely accessible to the public, may influence future attacks due to new capabilities, such as overcoming physical standoff and bypassing layered physical security through flight, anonymity through remote control operation, and other risks to the terrorist. Terrorist applications of consumer drones remain a foggy area, due to the lack of historical attacks involving drones, but innovators will likely experiment and hone methods in the coming years. As Hamm and Spaaj conclude, "although lone wolf terrorism may not be increasing in the United States, it is undergoing dramatic changes in terms of modus operandi," which may include consumer drones in the near future (Hamm and Spaaj 2015, 5). As consumer drones drop in cost and include more features, lone wolves will likely experiment with drones for terrorist plots.

Although drones are now affordable to the common profile among lone wolves in the United States, it is unlikely attacks in the near future will incorporate this new technology, at least, in the form of carrying explosives toward a target. According to the Diffusion of Innovations Theory, 2.5% of a given population is innovators, experimenting with new methods and tactics, which others in the population adopt at later stages ("Diffusion of Innovations Theory" 2016). Due to the lack of events involving consumer drones among lone wolf attacks, lone wolves likely fall into this

invention and innovation phase. Explosive-laden consumer drones are an unlikely terrorist tool in near-term attacks, but variables such as types of targets and standoff, drone payload capacities and drone defense mechanisms can influence the likelihood of lone wolves employing such methods of attack.

Feasibility of the use of Explosive-laden Consumer Drones

To date, there has not been a terrorist attack in the United States involving a consumer drone carrying explosives, though similar plots exist as far back as 2011, as revealed in the FBI investigation of Rezwan Ferdaus (Finn 2011). As consumer drones become more accessible, affordable and sophisticated, security concerns continue to grow. Consumer drones vary in dimensions, capabilities and cost. Table 1 includes six popular drone models currently on the market, listing characteristics of capabilities relevant in a terrorist attack involving an explosive-laden drone. All six are equipped with a camera and can only operate in dry conditions.

Table 1: Select List of Commercially Available Drones and Relevant Factors

Model	Weight (kg)	Payload (kg)	Flight Time (min)	Range (m)	Max Speed (mph)	Price
Blade 350 QX2	1	0.2	10	1,000	32	$285–435
3DR IRIS+	0.9	0.2	16	800–1,000	40	$720–865
DJI Phantom 2 Vision +	1.2	0.2	25	600	33	$1,150–1,730
DJI Phantom 3 Professional	1.2	0.3	28	1,900	35	$1,440–1,730
Walkera Scout X4	1.7	0.5–1.0	25	1,200	40–50	$1,010–1,300
Yuneec Q500 Typhoon	1.1	0.5	25	600	54	$1,300–1,590

Source: Abbott et al., *Hostile Drones*, 5.

Depending on the type of target and desired end state, these factors differ in relative importance. Terrorist targets fall into three distinct categories: long-term static targets, temporary static targets, and mobile targets (Abbott et al. 2016, 15). Lone wolves in the United States have plotted against or attacked each type of target. Several variables influence suitability of different drone models and likelihood of success. As these characteristics continue to evolve for optimal drone configuration and utility and capabilities continue to improve, these factors will alter how terrorists may employ a consumer drone in an attack.

Long-term Static Targets

Based on characteristics and trends of past lone wolf attacks within the United States, likely long-term static targets include prominent government facilities, sports stadiums, chemical plants and facilities, natural gas pipelines, and similar infrastructure. Depending on the desired effect, drones provide terrorists few advantages in targeting some structures, such as bridges, sports stadiums and some government facilities, due to the close proximity they can attain through vehicles and other means of transporting a significantly larger explosive payload. Areas with layered security and standoff, however, may be more vulnerable to drones, which can achieve greater proximity to protected sites by approaching targets via flight (Jackson et al. 2008, 28). Hence, a lone wolf terrorist could feasibly use an explosive-laden drone to cause much more damage to a chemical plant than by attempting to use another payload delivery method.

Long-term static targets are easier for a terrorist to target, due to their permanence and a terrorist's ability to conduct reconnaissance through virtual or physical means and attack on his/her own timeline. On the other hand, this permanence allows for a more robust defense, including physical standoff and obstacles, radar, and passive sensors. In targeting long-term static structures, payload is generally the most important feature, as the explosive blast may need to rupture pipes or other metallic walls to detonate protected chemicals or inflict damage on targets within a structure. Range is also vital to success, as the drone may need to traverse considerable physical standoff posed by perimeter fences, restricted areas and a lack of dead space offering concealment. The importance of flight time varies among targets, as this factor is directly proportional to physical standoff. Speed is less vital to mission success, as the likelihood of interdiction remains low, even if guards or other defense measures detect the drone.

Temporary Static Targets

Short-term, or temporary, static targets are more dynamic than long-term static targets and, though often scheduled far in advance, locations may change due to weather or other unforeseen factors. Such targets include summits, speeches by politicians and sporting events or large gatherings, often containing some degree of local security (Abbott et al. 2016, 15). Lone wolves might attack particular events for ideological reasons, but may also seek to capitalize on live media coverage and a high concentration of people. In many such instances, security is such that a terrorist might infiltrate a crowd with a larger explosive device, such as the pressure cookers in the Boston Marathon bombing of 2013. A drone, despite payload limitations, does not require prepositioning and the terrorist can guide the bomb remotely to the largest concentration of people in real-time. This method bypasses typical forms of security and detection, increasing the odds of success.

Payload is the most significant factor in an attack deliberately targeting a crowd of people, as the terrorist aims to inflict the greatest number of casualties. Small metallic objects packed around the explosives can enhance this objective, producing shrapnel

that expands the kill radius. Range also contributes to success, providing adequate standoff to avoid detection and improve chances of escaping the scene. Whereas long-term static targets may have permanent fences and surveillance cameras monitoring vulnerable areas and high-traffic pathways, physical security measures protecting temporary static targets often include road barriers, access control points or inspection sites and law enforcement patrols. Drone flight ranges generally exceed the distance between such security features and protected events or venues, weakening the effects of security against lone wolves employing an explosive-laden drone. Drones with a greater maximum speed may mitigate the chance of interdiction and minimize early warning and reaction time of the crowd.

Mobile Targets

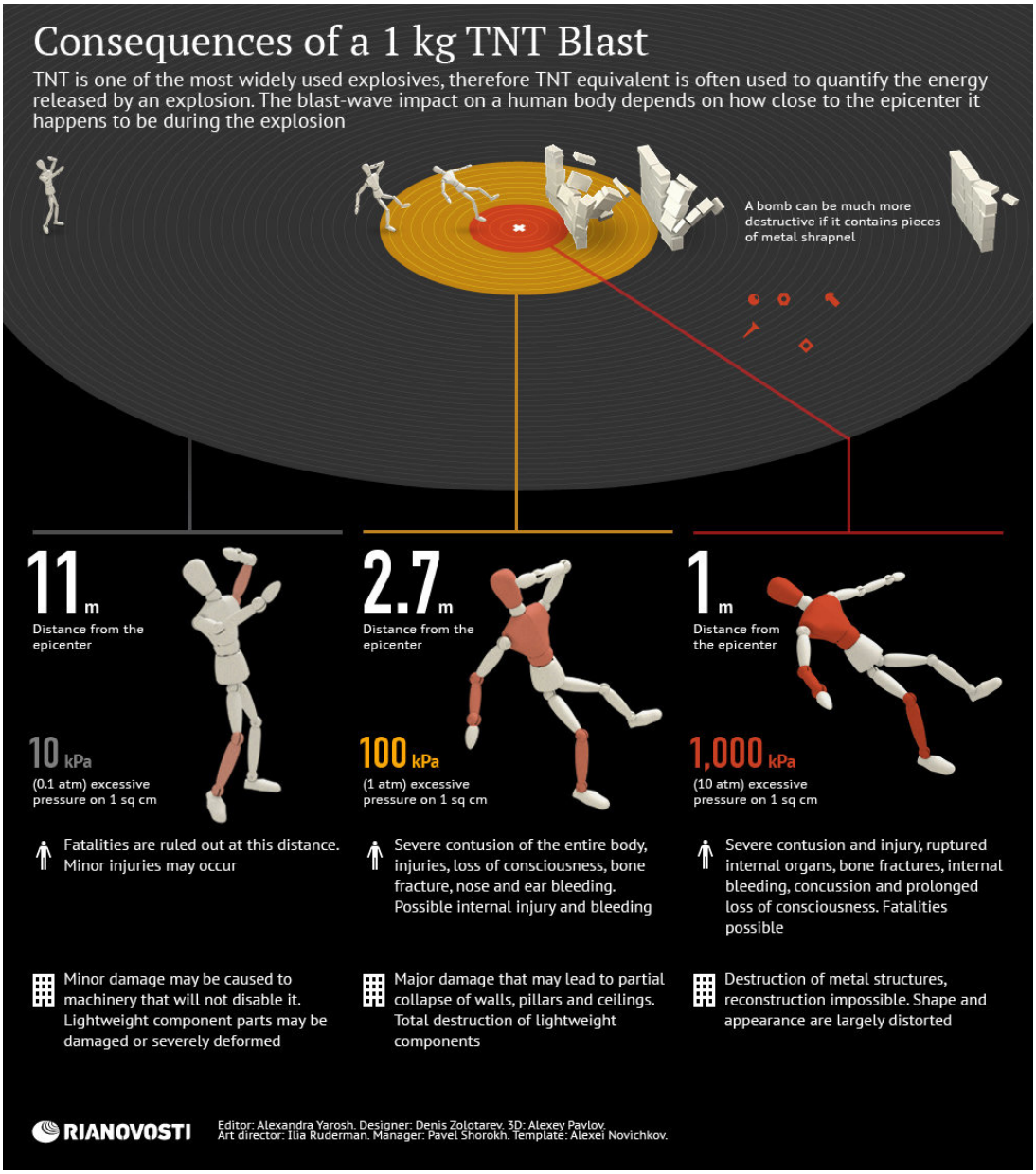
Mobile targets are usually more difficult for a lone wolf to attack, as security measures include announcing events or appearances with little time in advance and restricting knowledge of movements and routes to a small group of individuals. Mobile targets are moving targets, lacking a fixed position and constantly subject to change, such as a military convoy or the President of the United States (Abbott et al. 2016, 15). Based on trends in ideology, these targeted individuals are often prominent government authorities, heads of corporations or leaders of religious groups. Between September 11, 2001 and January 1, 2012, lone wolves targeted a person or place of interest in 8 of the 56 domestic lone wolf terrorism cases, with assassination targets ranging from abortion doctors to the President of the United States (Eby 2012, 33). Terrorists may choose to target such figures at their homes or near their workplaces, as such locations may be easier to locate than events or appearances announced with little advance notice. A lone wolf would likely employ a drone with explosives against a figure with a guard detail or similar security measures, which might interdict more common terrorist tactics such as a car bomb.

A drone's maximum speed plays a much more crucial role against a mobile target, such as in the assassination of a political leader. An increase in a target's reaction time increases his/her ability to find cover and the ability of guards to interdict the attack by shooting the drone down. Payload plays a slightly smaller role, especially if the explosive charge is equipped with small objects to produce shrapnel. Increased range can enable a terrorist to bypass physical security features protecting the mobile target and avoid surveillance cameras and media coverage sorted through in forensic investigations following an attack. Greater range also increases the probability that the terrorist can escape quickly and undetected, avoiding initial cordons or roadblocks in the wake of an attack.

Optimal Consumer Drones and Potential Effects

A drone's payload capacity is the most important feature in a terrorist attack involving an explosive-laden consumer drone. Range and maximum speed are important considerations, their relative importance depending on the type of target, while flight

Figure 1: Damage Inflicted by 1.0-kg of TNT (R.E. Factor of 1)



Source: "Potential Damage from a 1 kg TNT Explosion" 2013.

time and price are less important factors. In regards to the explosives transported by a drone, terrorists may use a variety of methods to achieve their objective, such as affixing a cluster of grenades, including small metal objects to produce shrapnel or using a homogenous substance. The relative effectiveness (RE) Factor of a material, measuring that substance's explosive properties compared to TNT (RE Factor of 1.0), is a useful factor to determine the potential effects of an explosive-laden consumer drone. Some models currently on the market can carry up to a 1.0 kg payload, which can inflict the damage described in Figure 1 if the substance's RE Factor is equal to or greater than 1.0.

Current payload limitations severely restrict the amount of potential damage resulting from an explosive-laden consumer drone flying into a building, specialized facility or crowd, but payload capacities will likely increase in the future. Existing drone models can feasibly carry the sufficient amount of explosives to assassinate an individual, injure dozens in a dense crowd, trigger a larger explosion at a chemical facility or cause minor damage to buildings, depending on the proximity of the blast. The government has not established constraints for payload weight, so that capacity will likely increase over time as companies manufacture larger and more robust drones. The prospect of heavier payloads seems more realistic as companies like Amazon experiment with drones to deliver packages.

Evaluation of Defense Mechanisms

Similar to the defense-in-depth concept for physical security practiced by government agencies and corporations, a series of defense mechanisms improves the odds of detection and interdiction. Many technical assets can defend long-term static targets, but it is unfeasible to implement such costly defense mechanisms for temporary static targets or mobile targets. Unfortunately, "drones can easily bypass many of the security measures implemented since 9/11," including many sophisticated defense assets, yet some can potentially mitigate the likelihood or severity of a drone attack (Maddox and Stuckenberg 2015). The most viable detection methods include acoustic sensing, radar and the human eye, while the most efficient interdiction methods are geofencing and kinetic defense. Additional interdiction methods include command link jamming and global navigation satellite system (GNSS) jamming, but these are less feasible options as "jamming the radio signal of a drone (or cellphone or anything else) is illegal in the United States under long-standing federal law," because it may interfere with emergency services (Ripley 2015, 70). These countermeasures must continue to evolve as consumer drone features improve and become more effective in overcoming and bypassing existing security measures.

Acoustic Sensing

Consumer drone models produce distinct noises difficult to replicate. Acoustic sensors can detect nearby drones by these unique sound signatures generated by drone motors (Sathyamoorthy 2015, 88). One such sensor, called a DroneShield, can quickly detect a drone by model and send out a text-message alert to nearby guards for monitoring and interdiction (Ripley 2015, 67). Although the tool is passive and only serves to detect when a drone flies nearby, the automated text mechanism increases the chances of interdiction by alerting guards who can shoot down the drone. The DroneShield is equipped with a database of "common UAV acoustic signatures," reducing the chance for false alarms and increasing precision detection rates (Sathyamoorthy 2015, 88). This detection mechanism is more affordable than most and is easily installed and transportable. While the DroneShield may be most effective in defending long-term static targets and less so defending some temporary static targets,

due to increased ambient noise, it was implemented at the 2015 Boston Marathon and it can protect mobile targets, as the tool is available for vehicles, such as a VIP convoy (Abbott et al. 2016, 17; Sathyamoorthy 2015, 88). Unlike some visible defense mechanisms, it is unlikely a lone wolf would detect or become aware of acoustic sensors near a target prior to the attack. One significant challenge with this technology is the internal sound database, which will require updates as companies manufacture new drone models. Nonetheless, the DroneShield's ability to identify specific drone models may cue security forces to recurring instances of a unique drone flying nearby, possibly probing the perimeter and testing security responses or conducting reconnaissance for a future attack.

Radar

Radar is one of the most effective methods to detect and track aerial threats, but this defense mechanism encounters unique challenges when applied to consumer drones. Air surveillance radar in the United States is ineffective against consumer drones, as these systems detect and track, but do not interdict, planes moving at high speeds, as opposed to smaller drones moving at relatively slow speeds (Sathyamoorthy 2015, 88). Installation and maintenance of radar systems can be very costly, explaining their limited presence in the United States. Some sophisticated radar systems "can see something as small as a bird flying," presenting false positives or distinguishing small drones from birds using precision radar and analytics (Elias 2016, 20; Maddox and Stuckenberg 2015). Such systems can provide early warning to long-term static targets, especially with physical standoff in the form of clearings between a facility and its perimeter fence, but a cost–benefit analysis yields poor results in defending temporary static or mobile targets. Furthermore, drone operators may fly at low altitudes, below 100 ft, to capitalize on inter-visibility lines created by surrounding terrain to block line-of-sight required for radar detection (Elias 2016, 20). Radar systems are not the most feasible or easily implemented methods to defend against lone wolves operating an explosive-laden drone, providing a false sense of security for sites protected by a dense array of radar systems.

The Human Eye

The naked eye remains the most reliable and practical defense against an explosive-laden drone. Ironically, no technical asset detected or brought down the consumer drone that landed on the White House lawn; instead, "a Secret Service officer standing guard" spotted the drone (Leonnig and Whitlock 2015). A combination of human senses provide a redundant means to identify and locate drones, such as seeing a drone's shadow on the ground or hearing a drone overhead. In Iraq, where radars "intentionally eliminate slow-flying targets on or near the ground" to prevent overtaxing tracking systems, human eyes are also "the most effective means of detecting such slow-flying threats," such as consumer drones (Gormley 2003, 8–9). Proving to

be especially effective in warzones, the human eye also has a history of identifying drones in recreational settings. After experimenting with various technical defense assets tailored to drone detection, Major League Baseball security officials concluded, "One of the best ways to detect drones is simply to deputize the crowd [because] when it comes to spotting small drones, 80,000 eyeballs are better than radar" (Ripley 2015, 72). Although this may not be the best defense for long-term static targets, where a small guard force would likely patrol access points and areas with few physical barriers, the human eye is the optimal defense for a temporary static target, such as a large crowd at an event. Complacency may detract from effectiveness, as drones become more common in the skies and operators disregard flight restrictions. While observant crowds may provide early warning, they offer little in the form of interdiction.

Geofencing

Geofencing is one of the most cost-effective and viable methods to mitigate the chance of a terrorist using a consumer drone in an attack. Invented by DJI and first implemented in April 2014, GPS geofencing is a technique where a manufacturer designates no-fly zones in coded form, imbedded in firmware, to prevent drones from entering certain areas (Poulsen 2015). Within the United States, DJI currently has no-fly zones around airports and the White House, but DJI and other drone manufacturers should include additional no-fly zones in future firmware or as updates to protect vital infrastructure and other potential terrorist targets.

Individuals with technical and sophisticated knowledge of firmware could potentially bypass or disable such security measures, but such knowledge and skills are not a common trait among lone wolves in the United States. Geofencing could, therefore, convince a potential lone wolf to abandon a target or select a different target unprotected by this security feature. Alternatively, it might force a lone wolf to seek expertise or technical assistance through the internet, Dark Web or other means, delaying an attack and increasing the likelihood of interdiction by the Intelligence Community. If the terrorist is unaware of geofencing features, the defense mechanism might interdict the drone during the actual attack. These no-fly zones would be most effective in defending long-term static targets, but manufacturers can implement and push updates to include temporary static targets.

Kinetic Defense

Shooting down a drone with small arms fire is the most likely and feasible form of drone intercept in an area not geofenced or if a drone bypasses geofencing restrictions. In urban areas, where most of lone wolf temporary static and mobile targets exist, retired Air Force Major General Frederick F. Roggero stated, "it would be tough to detect and tough to defeat kinetically without shooting it down and causing collateral damage" (Leonnig and Whitlock 2015). Faster drone speeds and smaller dimensions certainly contribute to potential collateral damage caused during interdiction attempts. Additionally, "shooting down drones is usually illegal," and

may carry costly fines, so citizens and members of law enforcement are unlikely to do so (Ripley 2015, 70). Law enforcement and defense agencies in other countries have experimented with other kinetic defense mechanisms to mitigate collateral damage and increase likelihood of interdiction. Such mechanisms include a net gun, similar to a net shot to catch feral animals, and net-equipped drones that can fly over a nefarious drone and snag it in a net, but these methods are not very reliable (Ripley 2015, 67; Sathyamoorthy 2015, 93). New kinetic defense methods will likely evolve as consumer drones become more versatile over time.

Recommendations

Federal Restriction of 5-pound Payload Capacity for Consumer and Commercial Drones

Due to the relatively recent dawn of consumer drones, regulatory measures and policies in the United States remain underdeveloped and behind the curve. Currently, the FAA requires users to register drones weighing more than 0.55 lbs, which includes the drone models in Table 1 and most drones with payload capacities ("Frequently Asked Questions" 2015). Empirical evidence and qualitative data reflects that payload is the most significant factor influencing drone suitability for terrorist attacks involving explosive-laden drones, yet existing laws do not regulate payload capacities. The FAA delegates the majority of drone regulation to state and local authorities, but the FAA and Congress should establish guidelines and restrictions limiting payloads for future models, enforceable in all states. Senator Booker (D-NJ) introduced the Commercial UAS Modernization Act (S. 1314) in the Senate on May 13, 2015, which would establish "barriers to allowing payload carriage" on drones, but the bill has yet to move beyond the Senate ("S.1314—Commercial UAS Modernization Act" 2016, 24). Such proposed legislation works in stark contrast of developments in drone delivery systems. Amazon's Prime Air program, for instance, involves a drone capable of transporting a 5-pound payload (Weatherby 2016). Policies governing drone utilization lag behind Amazon's progress in drone research and development. For now, circumstances of utility drive drone design and payload in industry and commercial sectors to remain below a 5-pound weight capacity, as most of Amazon's products weigh less than 5 pounds, but this weight capacity may increase in the future (Weatherby 2016). The FAA and Congress should establish a maximum payload at or near five pounds to mitigate effects in the instance of a terrorist attack employing such drones, restricting the use of drones capable of transporting heavier payloads to the military and specialized industries. Hackers have already demonstrated that delivery drone prototypes are vulnerable to hijacking through sophisticated means (Wagstaff 2013). Although most lone wolves lack the knowledge to hijack one of these drones, the capability exists and the payoff of employing a drone with five pounds of explosives instead of two pounds yields significantly more damage.

Legislation and Increased Collaboration for Geofencing Firmware

To date, no United States laws require drone manufacturers to incorporate geofencing into their firmware. Following the quadcopter incident on the White House lawn in 2015, DJI emphasized geofencing and pushed a "mandatory firmware update" but even then, its geofenced areas only include airports and the White House (Poulsen 2015). This cost-effective method to restrict drone flight can greatly contribute to protection of long-term static targets, but may also protect short-term static and mobile targets through proper coordination. Senator Chuck Shumer (D-NY) introduced an amendment to the FAA Reauthorization bill last year stating, "If geo-fencing technology were mandated in every drone sold in America," it would "effectively fence off drones from sensitive areas like airports, the Pentagon and major sporting events like the United States Open and more" (Laing 2015). The bill failed, but politicians should continue to investigate the benefits of geofencing and push for requirements in newly manufactured drone models, such as firmware and mandatory periodic updates to incorporate new geofences, as this passive feature can slow down or prevent attacks conducted by unsophisticated lone wolves unable to bypass or circumvent firmware.

Drone manufacturers are responsible for most of the recent progress in geofencing efforts. DJI recognizes the utility of this feature and plans to implement as many as 10,000 no-fly zones for airports and some national borders in the future, but the United States Government should collaborate with DJI for additional no-fly zones over other sensitive locations (Poulsen 2015). Geofencing can mainly benefit long-term static targets, but government agencies have failed to feed information to drone manufacturers developing firmware and constructing geofences. The Department of Homeland Security's Protective Security Coordination Division, which conducts vulnerability assessments for sites of 16 different critical infrastructure sectors, should collaborate with DJI and other drone manufacturers to implement new no-fly zones over these sensitive sites ("Critical Infrastructure" 2016). Such collaboration can significantly enhance the security of long-term static targets across the United States in a relatively short amount of time.

Increased Focus in Academia

There is certainly potential for further research and analysis on this looming threat. Between September 2013 and the January 2015 quadcopter incident at the White House, the National Counterterrorism Center's working group on drones grew from four members to 65, reflecting its concern for terrorists' use of drones (Schmidt and Shear 2015). Similarly, some academic institutions developed specific groups to investigate and analyze drones, such as the Center for the Study of the Drone at Bard College, but there is room for continued growth in this new field of study. Lt. Col. (Ret.) Mitchell [last name withheld], former Chief of MQ-1 Training for a USAF Special Operations Squadron, suggested, "a study should be considered where they hire someone and say—"Go buy one [a drone] and see what you can do." This kind of

practical study will fill in gray areas very quickly" (Maddox and Stuckenberg 2015). DHS and other governmental agencies should collaborate with universities to promote and endorse such research. Students are ideal candidates to conduct such experiments. They can go through the unfamiliar process of targeting by conducting reconnaissance by visiting the site or through open source intelligence collection. They can then research and purchase a drone through the same unclassified mediums a lone wolf would use, learn how to fly and program the drone and attempt an attack with mock explosives in a controlled setting under approved conditions. Such experimentation can transform theoretical studies into practical application, aiding refinement of defense mechanisms and exploring the possible terrorist applications of consumer drones.

Conclusions and Recommendations for Additional Research

For less than $1,600, anyone can acquire a ready to fly, GPS-enabled and camera-equipped consumer drone that can carry a small amount of weight. This offers terrorists new capabilities in executing attacks, particularly the ability to bypass traditional security measures and gain unprecedented access to a vulnerable target. Lone wolves in the United States break the mold of global terrorism, motivated by anti-governmental ideologies more than religious or other principles. Innovators among these lone wolves may use consumer drones to target a number of long-term static, temporary static or mobile targets in the coming years.

Consumer drones currently on the market offer a diversity of capabilities, of which payload, maximum range and maximum speed are most important. None of these can carry more than 1.0 kg of a substance, significantly limiting the destructive capacity of an explosive-laden drone; even so, a precision attack can render devastating effects against a vulnerable target. It is very likely that lone wolves will continue to use firearms and bombs in attacks rather than explosive-laden consumer drones due to a much higher probability of inflicting more casualties and causing more damage.

A variety of sophisticated defense mechanisms exist which can detect small drones at low altitudes, but there are few mechanisms capable of interdicting a drone in flight toward a target. Collaboration between government agencies and drone manufacturers may improve security conditions by implementing no-fly zones over sensitive sites through firmware, potentially delaying or deterring many attacks. Such defenses can help secure long-term static targets, but temporary static targets and mobile targets remain vulnerable, generally reliant on the human eye for detection with no reliable interdiction mechanisms.

Legislation limiting payload capacity of consumer drones can curtail future challenges associated with this type of terrorist attack. Additionally, legislation requiring geofencing firmware in drones offers a viable defense mechanism that drone manufacturers can quickly implement. Much of this new field remains unexplored, especially terrorist applications of drones, as most research is theoretical, without practical experiments or trials. Academia can hedge the risks of nefarious innovators by exploring the bounds of consumer drones before lone wolves, enhancing defense efforts by exposing vulnerabilities.

This field remains the subject of many fictional plotlines and alarmist articles, but there is a general lack of academic research detailing the feasibility of consumer drones in attacks. Researchers can further explore general terrorist applications of consumer drones, such as reconnaissance of otherwise inaccessible targets or drones as delivery agents for chemical or biological agents. Studies can also investigate other types of payloads, such as fragmentary grenades and various explosive substances. Researchers should actually run trial runs for drones carrying such payloads to demonstrate feasibility and probable damage. A study of international responses may yield useful approaches for the United States to follow in defending against drone threats. Some defense studies detail strategies and defense practices in the United Kingdom, Ireland, Japan, and Malaysia, but researchers can continue to investigate conditions in other countries to gauge effectiveness of different defense methods and assess vulnerabilities on a global scale. Such studies may also reveal how the United States Congress compares with other nations in passing relevant legislation and restrictions and how this might weaken security. Researchers may look into the research and development behind new drone models and features to assess possible terrorist applications and prepare defense measures.

References

Abbott, Chris, Matthew Clarke, Steve Hathorn, and Scott Hickle. 2016. *Hostile Drones: The Hostile Use of Drones by Non-state Actors Against British Targets*. London: Remote Control Project.

"Critical Infrastructure Vulnerability Assessments." 2016. *Department of Homeland Security*. https://www.dhs.gov/critical-infrastructure-vulnerability-assessments (accessed May 28, 2016).

"Diffusion of Innovations Theory." 2016. University of Twente. https://www.utwente.nl/cw/ theorieenoverzicht/Theory%20clusters/Communication%20and%20Information% 20Technology/Diffusion_of_Innovations_Theory/ (accessed May 28, 2016).

Eby, Charles A. 2012. *The Nation that Cried Lone Wolf: A Data-driven Analysis of Individual Terrorists in the United States Since 9/11*. Master's Thesis, Naval Postgraduate School.

Elias, Bart. 2016. *Unmanned Aircraft Operations in Domestic Airspace: U.S. Policy and the Regulatory Landscape* (CRS Report No. R44352). Washington, DC: Congressional Research Service. https://www.fas.org/sgp/crs/misc/R44352.pdf.

Finn, Peter. 2011. "Mass. Man Accused of Plotting to Hit Pentagon and Capitol with Drone Aircraft." *The Washington Post*, September 28. https://www.washingtonpost.com/national/national-security/mass-man-accused-of-plotting-to-hit-pentagon-and-capitol-with-drone-aircraft/2011/09/28/gIQAWdpk5K_story.html (accessed May 16, 2016).

"Frequently Asked Questions." 2015. Know Before You Fly. http://knowbeforeyoufly.org/ frequently-asked-questions/ (accessed October 20, 2016).

Gallagher, Sean. "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs." *Ars Technica*, September 18. http://arstechnica.com/informationtechnology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/ (accessed October 16, 2016).

Gormley, Dennis M. 2003. *UAVs and Cruise Missiles as Possible Terrorist Weapons* (Occasional Paper No. 12). Monterrey, CA: James Martin Center for Nonproliferation Studies.

Hamm, Mark, and Ramon Spaaj. 2015. *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*. Terre Haute, IN: Indiana State University.

Hughes, Matthew A. 2016. *The Islamic State's Influence on Lone Wolf Terrorism in the United States*. Master's Thesis, American Military University.

Jackson, Brian A., David R. Frelinger, Michael J. Lostumbo, and Robert W. Button. 2008. *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*. Santa Monica, CA: RAND Corporation.

Laing, Keith. 2015. "Schumer Moves to Require Geo-fencing on Drones." *The Hill*, September 14. http://thehill.com/policy/transportation/253565-schumer-moves-to-require-geo-fencing- on-drones (accessed May 6, 2016).

Leonnig, Carol D., and Craig Whitlock. 2015. "Drone Incident at White House Highlights Long- Studied, Still-Unsolved Security Gap." *The Washington Post*, January 26. https://www.washingtonpost.com/politics/drone-incident-at-white-house-highlights-long-studied-still-unsolved-security-gap/2015/01/26/ed2e7f9e-a594-11e4-a7c2- 03d37af98440_story.html (accessed May 3, 2016).

Maddox, Stephen, and David Stuckenberg. 2015. "Drones in the U.S. National Airspace System: A Safety and Security Assessment." *Harvard National Security Journal*, February 24. http://harvardnsj.org/2015/02/drones-in-the-u-s-national-airspace-system-a-safety-and- security-assessment/ (accessed April 28, 2016).

"Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists." 2012. *Federal Bureau of Investigation*. https://archives.fbi.gov/archives/boston/press-releases/2012/man-sentenced-in-boston-for-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-detonation- devices-to-terrorists (accessed October 12, 2016).

McKelvey, Nigel, Cathal Diver, and Kevin Curran. 2015. "Drones and Privacy." *International Journal of Handheld Computing Research* 6 (1): 44–57. (accessed April 23, 2016). doi: 10.4018/IJHCR.2015010104.

"Potential Damage From a 1kg TNT Explosion." 2013. *Sputnik*, August 13. http://sputniknews.com/infographics/20130813/182605201/Potential-Damage-From-a-1kg- TNT-Explosion.html (accessed May 7, 2016).

Poulsen, Kevin. 2015. "Why the US Government is Terrified of Hobbyist Drones." *Wired*, February 5. http://www.wired.com/2015/02/white-house-drone (accessed April 22, 2016).

Quan, Douglas. 2014. "Terrorists' Use of Drones on RCMP's Radar; Intelligence Assessment." *The Province*, December 30. (accessed April 21, 2016). Proquest (1640950854).

Ripley, Amanda. 2015. "To Catch a Drone." *The Atlantic Monthly* 316 (4): 66–68, 70, 72–74. Proquest (1726692327).

"S.1314 – Commercial UAS Modernization Act." 2015. *Library of Congress*. https://www.congress.gov/bill/114th-congress/senate-bill/1314/actions (accessed May 14, 2016).

Sathyamoorthy, Dinesh. 2015. "A Review of Security Threats of Unmanned Aerial Vehicles and Mitigation Steps." *The Journal of Defence and Security* 6 (1): 81–97. Proquest (1768942810).

Schmidt, Michael S., and Michael D. Shear. 2015. "Drones Spotted, but Not Halted, Raise Concerns." *The New York Times*, January 29. http://www.nytimes.com/2015/01/30/us/for-super-bowl-and-big-games-drone-flyovers-are-rising-concern.html?_r=0 (accessed May 28, 2016).

Wagstaff, Keith. 2013. "Could Prime Air Drones be Hacked? Probably, but Amazon Might not Care." *NBC News*, December 4. http://www.nbcnews.com/technology/could-prime-air-drones-be-hacked-probably-amazon-might-not-2d11691755 (accessed December 19, 2016).

Weatherby, Lea. 2016. "Amazon Drone Delivery: 30 Minutes and 5-Pound Limits for 'Prime Air.'" *Inverse*. https://www.inverse.com/article/10330-amazon-drone-delivery-30- minutes-and-5-pound-limits-for-prime-air (accessed October 23, 2016).

Is China Playing a Contradictory Role in Africa? Security Implications of its Arms Sales and Peacekeeping

Earl Conteh-Morgan[A] & Patti Weeks[B]

This article offers a critical analysis of the conflict and regional security implications of one of the strategies (arms sales) utilized by China to expand and consolidate its presence in Africa. This worrying trend is juxtaposed against its equally increasing peacekeeping and peacebuilding activities in post-conflict states within the continent. The analysis, accordingly, argues that the simultaneous growth in the scope of arms transfers and increase in contributions to peacekeeping and peacebuilding activities is tantamount to a contradictory policy toward Africa. Arms sales to African states encourage some incumbent regimes to maintain their despotic and oppressive rule thereby increasing the probability of violent conflicts between regimes and opposition groups. Small arms also prolong civil wars because of the easy access to them. While Chinese arms have been implicated in many conflicts in Africa, China at the same time is also enhancing African Union peacekeeping activities through generous financial donations as well as participation in humanitarian assistance, national police training, and resettlement of ex-combatants, among other activities. The question is, why does China pursue these seemingly antithetical policies within Africa? Or, why does China play this contradictory role contrary to its narrative of noninterference in the internal affairs of other states?

Keywords: *China, Africa, Arms Sales, Peacekeeping, Peacebuilding.*

Introduction

China's growing presence in Africa has spawned many explanations of its political, economic cultural and other activities in the continent. A good deal of its interactions with African states involves arms sales and support for peacekeeping and peacebuilding activities. In its dealings with African states it deliberately tries to set itself apart from the West's record of colonial rule and exploitation of the continent. China constantly reiterates and underscores its foreign policy of non-interference in the affairs of African states. Nonetheless, it has not been able to escape the lure of the benefits that are associated with arms sales to Africa, plus its negative consequences, as well as the geopolitical ties that it enhances between China and Africa. Accordingly, the objective of this article is to analyze China's seemingly contradictory

[A] Professor, School of Interdisciplinary Global Studies, University of South Florida
[B] Adjunct Professor, Department of History and Political Science, University of South Florida
doi: 10.18278/gsis.2.1.6

arms transfers/military relationships with African countries and simultaneous active engagement in peacebuilding activities in African countries where its weapons have been implicated in bloodletting and war crimes in general. In other words, what are the geopolitical and geo-economic rationales for increasing Chinese arms transfers and military relationships with African nations in contrast to its contributions to UN peacebuilding efforts and support for African peacekeeping activities? How do arms transfers to African nations and involvement in peacebuilding activities portray China as playing contradictory roles in Africa? What are the conflict and peace implications for African countries of these seemingly contradictory activities by China?

For a long time, arms transfers to Africa have been dominated by the US, Britain, France, and Russia (Grant 2012; Pierre, 1982. However, recent trends in Chinese industrialization and China's growing scope of political, economic, and diplomatic activities may suggest that a fundamental shift in arms transfers to Africa may be occurring that, over time, could have important consequences for increased internal wars or peacekeeping operations in the continent.

The literature on arms transfers has long suggested that arms transfers to developing countries tend to widen the scope of violence and even intensify or increase the duration of wars thereby making the maintenance of peace more difficult (Klare 2014; Sanders 1990; Schelling 2008). At times bilateral arms transfer relationships take the added form of arms production, whereby the supplier sets up arms production facilities in the recipient country.

Reasons for Antithetical Policies

The primary reason why China pursues these seemingly antithetical policies in Africa is found in its overall geo-strategy in the continent. This geo-strategy is a combination of geopolitical and geo-economic policies. The latter refers to the economic objective of ensuring access to Africa's strategic resources, while the former refers to consolidating political ties with all African states, especially with the politically important ones. First, China sees African states such as Kenya, South Africa, Ethiopia, the Democratic Republic of Congo, Nigeria, and Zimbabwe, among others, as countries with which to engage in lucrative trade (hence arms sales) as part of its geo-economic rivalry with the West. At the same time there are countries in Africa that need peacebuilding and peacekeeping assistance because of ongoing civil wars or postwar reconstruction. Accordingly, China participates in both peacekeeping and peacebuilding activities which help to strengthen its geopolitical ties with these African states. These humanitarian activities present opportunities for China to put into practice its frequent pronouncements that it is a friend of Africa.

China's policy of non-interference in human rights within the recipient country makes it an attractive and willing source of weapons for African countries. Since many African countries attempt to break free of Western rules and regulations about arms procurement, they turn to China which does not burden them with external impositions associated with arms transfers and production, such as human rights, or democratic ideals. Besides, where an arms production facility/factory is set up within

a developing country, it tends to bolster morale and a sense of independence and autonomy in military hardware. In other words, a domestic arms production facility reduces a country's dependence on more developed countries. More arms production autonomy inevitably means less dependence on major suppliers, at least, for small arms or light weapons. Moreover, apart from the determination by African countries to lessen dependence on Western suppliers, they also want to ensure reliability and consistency of supply. The major arms suppliers often impose embargos on arms sales to countries whose policies they find objectionable. For instance, the US often makes human rights issues a key criterion in determining US military aid and sales. China, on the other hand, does not use human rights and democracy as criteria for transferring arms to African countries. Many resolutions are passed in the UN Security Council, or by Western governments barring the sale of weapons to governments engaged in wars against rebel groups or neighboring states. Furthermore, China's Africa policy is also one that provides benefits and employment opportunities for skilled Chinese citizens (Baah and Jauch 2009; Lynch 2012). This is an example of China's geo-economic objective in Africa. By establishing arms factories, and training Africans to use the more sophisticated weapons they supply, skilled Chinese such as scientists, engineers, and industrial managers are offered more opportunities for applying their skills and knowledge. The interaction between African and Chinese skilled workers, it is hoped, would produce better understanding between the two in competition with the West. In addition, China's arms industry, just as the arms industries of other nations, is designed to be both a military and economic asset. For an arms industry to be sustainable it has to be profitable, thus the need for arms exports to other nations. The revenue generated from arms exports feeds into research and development for new and better weapons systems. This is especially the case with China where the government with its State Owned Enterprises (SOEs) is the key, if not the sole, exporter of weapons to developing countries (SIPRI 2011). Arms exports are therefore an economic imperative, and a sine qua non for maintaining an arms industry. Besides, Chinese arms find a ready market in some African countries that consider themselves, or would like to be perceived as regional influentials. Countries such as Nigeria in West Africa, Kenya in East Africa, or the Democratic Republic of Congo (DRC), and South Africa, among others, fall into this category. Still others import Chinese arms in order to feed the conflicts in the DRC, Sudan, Central African Republic, among others. While arms transfers during the Cold War were predicated largely on the need to supply warring factions in civil wars, or proxy wars, or post-independence struggles for power, today regime survival or incumbent regime efforts fuel arms transfers. The coercive military balance between regime and dissidents is determined largely by the access to a steady supply of weapons.

The Chinese arms transfer rationales have undergone change in response to changes in power political and economic competition in the international system (Caldwell 2015). In particular, during the era of political ideological rivalry between communism and capitalism, China supplied weapons to both state and non-state revolutionary actors with the aim of bolstering Maoism and China's national interests. The focus was largely ideological and not motivated by profit. Currently, in this era

of economic globalization and commercial competition, Chinese arms serve more of a profit motive (Mullen 2016). In its arms relationship with African nations, arms sales have more commercial and political bases and thereby promote both the geo-economic and geopolitical goals of Africa.

China's Multidimensional Approach in Africa

This analysis focuses on China's contradictory policies of arms sales/military cooperation and peacebuilding/peacekeeping activities in African nations. This in no way asserts that China alone is responsible for the sale of weapons to sub-Saharan African nations. However, while arms sales and peacebuilding activities may seem contradictory policies, they are an integral aspect of China's multidimensional approach to Africa which includes activities such as agriculture and health training, educational cooperation, mineral investments, infrastructure development, telecommunications services, and military cooperation, among many others. This approach has inevitably led to the seeming contradictions between the simultaneous expansion of arms sales and peacekeeping activities. In fact for a long time, the foremost arms suppliers to Africa have been the US, France, Britain, and Russia. In terms of largest world arms suppliers, China was for a long time not among the five top global suppliers. It was only in 2010 that it ranked among the top five suppliers occupying the position of third largest weapons supplier (SIPRI 2011). China has realized that in order to achieve its geo-strategic and economic ambitions it needs to be more competitive with the leading arms suppliers, the US, Britain, Germany, France, and Russia. Its increasing competitiveness may in large part be due to its arms sales to sub-Saharan African states. Its ongoing geo-political and economic objectives in African countries have, at the same time, widened and even strengthened its arms trade with African states.

China's growing penchant for increasing its arms sales to Africa is driven by both domestic factors as well as external imperatives of economic globalization—in this latter case is the need to compete with the foremost global arms suppliers, the US, France, Russia, Britain, and Germany in particular. The domestic factors that may be largely responsible for China's arms transfer to Africa are: (1) the Chinese state's inability to regulate or monitor all arms exports from China; (2) China's arms sales to African nations of geopolitical and geo-economic importance to China in Africa, such as Sudan and Zimbabwe; and (3) the freedom of trade that comes with economic liberalization in China which has spawned many private enterprises, some of which are engaged in arms transfer purely for the profit motive. These internal–external factors responsible for China's arms transfer to Africa are driven by what could be referred to as the globalization imperative. This last reason is directly related to the fact that many Chinese enterprises with close ties to the People's Liberation Army (PLA) no longer benefit from that symbiotic relationship. The (PLA) formally divested itself from commercial operations after Jiang Zemin called for the dissolution of China's military-business complex (Hyer 1992; Taylor and Wu 2012). Military acquiescence to divestiture was contingent on generous compensation from Beijing as well as allowing

the PLA to pursue profits via arms sales. Accordingly, it currently exercises strong influence over defense-related enterprises and searches for its own arms export markets. The exposure of defense companies to more independent commercial management is driven by the need for China to compete with the major arms suppliers. Most of the profits earned remain with these companies while a portion goes to the Ministry of Finance. The result is that the PLA no longer receives profits from civilian enterprises and now relies to a large extent on arms sales. The need to increase profits from arms sales result in selling weapons that escape the scrutiny of the state. Consequently, the vigorous search for markets in Africa is the result of necessity by the PLA to regain its lost domestic commercial profits via external commercial arms relationships.

The dissolution of China's military business complex, it could be argued was a deliberate policy to ensure that the country becomes more competitive in arms sales relative to other major powers. What the policy did, is to privatize its arms industry and open it to domestic competition among Chinese firms. Many of China's privately owned firms entered the African market and thereby acted as competitors to firms from other major countries. However, because of China's non-conditional policy of arms sales, it was not long before Chinese weapons were implicated in atrocities in Sudan, especially Darfur, the Democratic Republic of Congo, in Liberia, and Zimbabwe, among others. In order to quell the growing negative image of itself in Africa because of its support of despotic regimes through arms sales, it expanded its peacekeeping and peacebuilding activities in the continent. Its involvement in increased peacekeeping was also a reaction to calls on it to be a more responsible partner in the international system. In other words, while China is searching for commercial opportunities in Africa, at the same time, it wants to preserve a good image in the world. It does not want to be seen as the enhancer of genocides, authoritarian regimes, or supporter of despots in the African continent. China attempts therefore to skillfully balance weapons sales with an expanding peacebuilding agenda in order to silence some of the criticism directed at it by the West.

African nations can be categorized into two broad categories, those that are of geopolitical importance such as Nigeria, South Africa, Kenya, and Ethiopia. These are sometimes referred to as anchor states. They could also be referred to as sub-regional hegemons. In Africa, these four states exercise considerable influence within their regions. They are characterized by a substantial power base relative to others within the same region. They often have a stronger and larger military, a larger population, and larger geographic size, critical raw materials, and a strategic location, relative to the many small African nations. They sometimes aspire to regional hegemony and could become directly involved in the foreign policy and economic goals of major powers. In sub-Saharan Africa, Nigeria, South Africa, Kenya, in particular generally possess many or all of the geo-strategic and geo-economic characteristics of sub-regional influentials. For instance, has the geo-economic and geo-strategic importance of Nigeria correlated strongly with Chinese arms transfers to that country? Nigeria as a sub-regional hegemon or anchor state in West Africa receives regular military assistance and arms transfer from China. The military ties between Nigeria and China are regularly cemented by reciprocal visits at the level of Defense Ministers. In June

2004, Nigeria's defense minister paid a state visit to China. China reciprocated by, among other things, agreeing to supply new combat jets to Nigeria, signing a contract with Nigeria's defense ministry worth over $250 million to transfer 15 Chengdu F/FT-7NI aircrafts in 2005 (Chau 2007). Transfers of sophisticated Chinese arms are usually followed by training of African military personnel on how to use them. Accordingly, in 2006 several Nigerian pilots traveled to China to undergo training on the use of the new aircrafts. In addition to the transfer of aircrafts, China also transferred air-to-air missiles, rockets, and anti-tank bombs, among others, worth $32 million. Between 2004 and 2006 other arms transfer or military assistance agreements between China and Nigeria were worth over $70 million involving supplies of patrol boats, trainer and fighter aircraft, and military transports. There are several other examples of China cementing its relationship with African countries through military assistance. Among the many examples is China's donation of $43 million worth of military equipment to Nigeria in October 2005. The equipment ranged from uniforms, communication technology, bullet proof helmets and vests, to computers, among other things (Enuka 2011). China did not just transfer this equipment to Nigeria, but the transfer was later followed by several Chinese military experts whose mission was to train Nigerian military personnel on how to use the donated equipment.

Within the past decade, the 10 African countries with the highest level of military cooperation with China are Algeria, Angola, Egypt, Ghana, Nigeria, South Africa, Sudan, Uganda, Zambia, and Zimbabwe (Alessi and Xu 2015). Although the value of arms transfers from China to Africa could be described as modest compared to trade in oil and other commodities, military interactions are carried out through high level political delegations, while arms transfers and high level bilateral ties are used as instruments to help secure more economic access to critical raw materials. Since the end of the 1990s high level military delegations have been a regular occurrence between Beijing and several African countries. Of the 10 countries engaged in high levels of military cooperation with China, six of them are either suppliers of oil, gas, and other critical resources, or they have substantial Chinese commercial investments. This places China–Africa weapons transfers and military cooperation into two distinct dimensions: (1) countries with strategic minerals like Sudan and Nigeria, and South Africa, and the Democratic Republic of Congo; and (2) anchor states/regional influentials/sub-regional hegemons like South Africa, Nigeria, Kenya, and Ethiopia, among others. In some cases there is an overlap between the two where geo-economic countries like Sudan, Nigeria, and South Africa are also regional hegemons.

China's Arms Sales Strategy to Africa

During the 1990s, Chinese weapons were considered to be substandard in firepower and offensive capability vis à vis the most simplistic, low-tech military armaments available, and limited to a defensive capacity, having only "nuisance value" (Bitzinger 1991). Consequently, Chinese weapons exports were limited to less than 10%. However, Chinese arms sales, especially in Africa, have increased. China has aggressively marketed its weapons to poorer and less technologically advanced

African states because of its inability to compete for sales in the more technologically advanced arms markets dominated by the US, Britain, France, and Russia.

China's aggressive arms sales in African markets have placed it among the top five arms suppliers in the world. It currently has arms transfers deals or military relationships with several large African states such Egypt, Nigeria, Ethiopia, Zimbabwe, and South Africa, as well as smaller states like the Republic of Congo, Equatorial Guinea, Eritrea, Burundi, and Sierra Leone, among others. One of the strategies utilized by China to make its arms sales attractive is the use of favorable financing. Many African countries cannot afford expensive, sophisticated weapons that fetch premium prices in the international marketplace. So China caters to this market, making its weapons affordable to cash poor countries through loans with very low interest rates or mineral rich countries willing to grant access to natural resources in a quid pro quo arrangement for supplying weapons. Consequently, the cost of Chinese made weapons remains below market, giving China the competitive edge through affordability, defined as inexpensive, rather than affordability defined as sophistication (Baker 2015). This translates into poor African countries having easy access to small, inexpensive, easy-to-use arms from China that have the potential to fuel eruptions of instability, increase political repression, and stifle economic development in recipient countries. This strategy by China has the dual effect of strengthening its ties with authoritarian leaders who need weapons to perpetuate their rule, and benefiting from sales to these authoritarian regimes thereby achieving its geo-economic objectives. China, stated differently, is using a "catch all" strategy in its dealings with African states. Moreover, China uses frequent and aggressive marketing tactics to capture market share in Africa, constantly promoting its military hardware at annual arms exhibits held in various states spanning the continent. The list of cooperating Chinese manufacturing firms is lengthy and includes companies such as China National Electronics Import-Export Corporation (CEIEC), China Electronics Technology Corporation (CETC) International, and China Aviation Industrial Base Corporation (CAIBC), as well as hundreds of smaller manufacturers. Apart from a strategy of affordability through attractive financing and payment options, China also ensures a wide array of arms and military hardware in its export inventory. Consequently, the scope of its offerings include small arms, armored vehicles, tactical and air defense weapons, naval ships, short range tactical ballistic missiles fighter jets, and communications surveillance and reconnaissance equipment. The list of available equipment also includes uniforms, boots and packs, as well as police items such as protective clothing and riot gear. Variation in wealth and military strength among African countries allows China to sell both small inexpensive, low-tech weapons as well more expensive and sophisticated military weapons. Consequently, transfers include battle tanks, guided missiles, air defense systems, and armored personnel carriers. Furthermore, China's success in African markets is also enhanced by its long standing policy of non-interference. This policy has allowed China, on occasion, to sell weapons to opposing warring entities as was the case in the Ethiopia-Eritrean conflict. Similarly, Chinese weapons were used in the Darfurian genocide in the Sudan where Janjaweed militia systematically murdered, raped, and tortured civilians (Enuka 2011).

Once established, the arms transfer relationship between China and its African trading partner becomes reinforced by the recipient who will be in constant search of spare parts, ammunition supply, maintenance upgraded technology, and weapons training which may take place in Africa or China. Although Chinese arms sales in Africa is small relative to transfers with the more traditional suppliers and former colonial powers of Britain and France, as well as the leading arms suppliers of Russia and the US, Chinese arms sales in Africa attract particular attention and criticisms because: (1) its arms transfers to states of international concern such as Sudan and Zimbabwe; (2) its willingness to supply arms to any country in Africa with an ability to pay for them; and (3) the contradiction between its long-standing policy of non-interference and its practice of supplying arms to warring factions within a sovereign nation. Arming sectarian combatants within a sovereign nation is inherently interventionist in nature and unequivocally interference in a country's internal affairs, especially when that country is in the throes of civil war, and where civilians have experienced gross human rights violations.

Chinese Arms: Negative Impact on African Conflicts

Although the value of arms transfers from China to Africa could be described as modest compared to trade in oil and other commodities, high-level military interaction and high-level political delegations have succeeded in enhancing China's access to critical raw materials in Africa (Hyler 1992). Since the end of the 1990s, military delegations have been a regular form of interaction between China and African countries. Arms transfers and military cooperation between China and African nations fall into two categories: (1) countries with strategic minerals like Sudan and Nigeria. These are geo-economically important countries to China in particular; and (2) key states like Nigeria, Kenya, South Africa, Ethiopia, the DRC, Ghana, and Zimbabwe, among others. Generally, many African states find China an attractive arms trading partner because of its "no strings attached" approach to transfer. China does not make its weapons sales conditional on either human rights or democratic reforms.

China is currently a key supplier of conventional weapons in Africa where arms transfers there inevitably contribute to civil strife and carnage in more than a few local conflicts. It is generally alleged that the light weapons used in the massacres in eastern DRC were Chinese. There, children as young as 11 years old were given weapons by warlord Thomas Lubanga, and forced to take part in brutal ethnic fighting between 2002 and 2003 (SAFERWORLD 2011). Moreover, according to Amnesty International reports, in February 2012, both Russian and Chinese supplied weapons fueled conflict in Sudan. In particular, arms transfers such as helicopter gunships, attack aircraft, air-to-air ground rockets and armored vehicles, including ammunition, are responsible for serious human rights violations in Darfur, Sudan. Small arms of Chinese manufacture were used by the Sudan Armed Forces (SAF) and government supported militia, including Sudan's Popular Defense Force (PDF) to carry out atrocities in Darfur. While all of the carnage cannot be directly attributed to Chinese supplied arms as other countries were active in supplying weapons as well, it is important to note that

an estimated 70,000 people were displaced from eastern Darfur in 2011 due to ethnic attacks directed toward the Zarghawa community by the SAF and government-backed militias. Nevertheless, Amnesty International confirmed that Chinese-made weapons are found all over Sudan including Southern Kordofan (Deen 2012).

In December 2011, a SIPRI report found that by 2010 China was the foremost exporter of arms to Africa, a continent well known for gross human rights violations. Between 2006 and 2010 China had captured a full 25% of the market compared to only 9% in the preceding 5 year period between 2001 and 2005 (SIPRI 2011). The reason for China's leading role in arms transfers over traditional leaders like the US, Russia, France, Germany, and the UK, is the fact that it is willing to transfer military aid or make more attractive deals in exchange for critical resources rather than cash. Moreover, China is also prone to ignore UN sanctions against arms trade with countries like Sudan or Zimbabwe where severe human rights violations occur. However, some critics believe that China's arms transfer role in Africa is exaggerated by Western countries noting that while China transfers largely small or light weapons, exporters like the US focus on quality transferring more sophisticated weapons, while Russia concentrates on quantity, making it the largest arms supplier to Africa. China takes much of the blame because it supplies small, low-tech, arms which are relatively inexpensive and easy to use and as a result, cause more destruction because of their scope and frequency of use compared to more sophisticated heavy weapons. Small or light arms are also responsible for civil unrest, atrocities, civilian deaths and involvement of child soldiers in rebellions. It is much easier to use a Chinese Type 56 rifle (China's version of the Russian Avtomat Kalashnikov (AK) assault rifle) than a Chinese aircraft which would require specialized training before it could be operated. China is viewed as playing a contradictory role where arms transfers and peace-keeping are concerned. For example, in the case of Sudan, China finally submitted to pressure to support UN Peacekeeping, but at the same time failed to suspend its arms sales which negatively impacted the regions of Darfur, South Kordofan, and the Blue Nile. China is, in other words, not interested in joining an arms embargo, or unilaterally ending arms sales in zones of conflict in Africa. China, one could argue, is a captive of its own foreign policy doctrine of non-interference in the affairs of another country (McPartland 2012).

Chinese exports to Sudan comprise of attack aircraft, munitions, and armored vehicles which are used against civilians. According to Amnesty International, following a raid at the Zam Zam camp for displaced civilians in Sudan in December 2011, ammunition was discovered bearing Chinese "41" and "71" manufacture codes, and (20) 06 and (20) 08 manufacture dates indicating that it was transferred to Darfur after the imposition of a UN arms embargo (Amnesty International 2012). China's violation of the UN arms embargo on Sudan is evident throughout the country with Chinese made ammunition bearing its own manufacture codes discovered in Darfur and the South Kordofan regions in 2011. Using either Chinese or Russian-made weapons, the SAF has focused its attacks on both military targets and civilian populations. In 2009, Chinese-trained Guinean Commando units were responsible for the killing of about 150 people during a protest against authoritarian rule in Conakry. In eastern DRC, Chinese trained Congolese troops were implicated in the killing of many innocent

civilians demonstrating that an increase in Chinese arms transfers to Africa is likely associated with more strife and bloodletting.

While China is largely known for its sale of small weapons and the human carnage left in their wake in places like Sudan and the DRC, the Chinese are also active in supplying sophisticated weapons to oil-rich African states including armored vehicles, artillery, jet fighters, and training and transport aircraft. China's sophisticated weapons transfers to Sudan include F-6 and F-7 fighter aircraft, light tanks, and anti-aircraft systems. Zimbabwe was the recipient of nine J-7 fighter aircraft and six K-8 trainer aircraft as well as 10 T-69 tanks and 30 T-59 tanks. Nigeria has expanded its assets with its US$251 million purchase of 15 F-7 fighter aircraft (Young 2016). And Angola ordered eight Su-27 fighter aircraft. Transfer of This sale corresponded very strongly with the fact that in 2005 Angola exported 17.5 million tons of crude oil to China becoming China's largest oil supplier by 2006. Chinese arms transfers are strongly associated with oil and trade agreements with geo-economically important countries such as Angola, Nigeria, Gabon, Equatorial Guinea, and the DRC, among others. Angola is surpassed only by Sudan as China's most geo-economic trading partner in Africa. Sudan has been the recipient of more Chinese made weapons and military equipment such as cargo trucks, battle tanks, and transport aircraft. These are in addition to mortars, rocket launchers, and air defense systems (Chang 2007). The level of sophistication of Chinese arms transferred to Sudan is strongly associated with Sudan's geo-economic importance to China. China is the recipient of more than, or approximately, 90% of Sudan's oil exports. China's military presence in Sudan is quite substantial, with over 4000 Chinese military personnel in the country to protect its extensive and multi-billion dollar oil infrastructure investments (Human Rights First 2008).

Zimbabwe is not oil rich, but endowed with a variety of critical minerals that China needs in its industrialization efforts. Accordingly, Zimbabwe has been the recipient of small arms and ammunition and sophisticated weaponry such as different types of armored fighting vehicles, and jet aircrafts. Moreover, China supplied the Mugabe regime instruments of opposition control such as radio-jamming equipment to disrupt opposition party broadcasts, and riot control equipment to suppress protests and demonstrations. In particular, oil-rich or strategic mineral endowed countries are the recipients of millions of dollars in Chinese investments, including military assistance or arms sales. The Republic of Congo is also rich in oil and supplies China with approximately 5% of its oil requirements. Congolese military forces are armed with major Chinese weapons such as the Type 59 tanks, Type 63 107-mm rocket launchers, Type 60 122-mm howitzers, and Type 59 130-mm cannons. This is in addition to various types of Chinese light weapons. Critics argue that China ignores the UN international arms embargo on Congo and continues to sell weapons to the country.

Other geo-economic African countries such as Egypt, Algeria, Nigeria, the DRC, and the like have received weapons systems such as the K-8 trainer aircraft, the J-7 fighter aircraft, training ship, missile fast craft with C802 ship-to-ship missiles. States that are not so geo-economic such as Mauritania, Zambia, Namibia, Eritrea,

Burundi, and Tanzania, all receive weapons systems from China. The transfer of weapons is inevitably accompanied by the dispatch of technical advisors by China, or the training of African military personnel in China. China in addition, maintains military attaches in some African nations such as Algeria, the DRC, Egypt, Ethiopia, Liberia, Libya, Morocco, Mozambique, Nigeria, Namibia, Sudan, Tunisia, Zambia, and Zimbabwe (Puska 2007). China supplies significant amounts of weapons to states with critical resources that maintain strong trading ties with China However, there are states such as Ghana or Uganda which are not significant in terms exporting critical resources to China, but have strong ties with China. This means that China is also using arms transfers as a means of enhancing its commercial profits.

Regardless of whether arms transfers have a negative or positive effect, they are nonetheless one of Beijing's instruments of economic policy and cementing political ties with African nations. In Nigeria in particular, China willingly provides weapons to the Nigerian state in its battle against insurgents in the oil-rich Niger Delta. Naval patrol boats and arms have been readily supplied by China to help protect oil infrastructure in the Delta against rebel attacks. In 2006, China's state-controlled oil firm, CNOOC negotiated an investment of over $2 billion for 45% of stake in a Nigerian offshore oil field. In addition, 3 months later China invested an additional $4 billion in oil infrastructure projects (Mahtani and White 2006). China continues to expand its oil investments in Nigeria, as well as forging closer military ties (arms transfers, military training, high level military cooperation, etc.) with the Nigerian military. In a similar fashion, Zimbabwe's economic importance correlates strongly with its procurement of both small arms and more sophisticated weapons from China. Zimbabwe is endowed with critical minerals holding the second largest deposits of platinum as well as numerous other minerals including gold, copper, uranium, and ferrochrome. As a result of its attractiveness to China, it is able to get both small arms and more sophisticated military jets. The Mugabe regime is aware of the leverage it has over China because of its focus on cementing ties with countries of geo-economic importance. The Zimbabwean state takes advantage of this and is therefore able to procure all sorts of arms and other technology from China. The Zimbabwean air force is armed with K- jet aircrafts used in training jet fighter pilots and for use in low intensity warfare. The Zimbabwean military is also in possession of 12 FC-1 fighter planes and several military vehicles worth over $200 million. In sum, Chinese weapons have been widely dispersed in Africa. A few examples are Chinese weapons in the hands of Chadean rebels fighting to overthrow the regime, or the use of Chinese weapons in wars in Liberia, and Sierra Leone, as well as in many parts of eastern and central Africa.

Peacekeeping Efforts by China

China does not only transfer military equipment on a bilateral basis, but it has given monetary assistance to the OAU/AU Peace Fund in order to enhance the organization's ability to resolve African conflicts. Accordingly, in 1999 it donated $100,000 to the OAU Peace Fund and again in 2000 an additional $200,000

was donated to the OAU Peace Fund (Rothberg 2015). China's rationale was to show its full support for peacekeeping efforts by Africans themselves, as well as to express its admiration for the organization's continued maintenance of peace and stability in the continent. China's support of the OAU has been regular and generous, as well as varied in terms of funds and equipment. In 2003 and 2005, respectively, China donated $300,000 and $400,000 to the AU as an expression of its commitment to African peacekeeping efforts (Agubamah 2014). There is a marked increase in China's donations to African peacekeeping efforts when one takes into account its 1999 and 2000 donations of $100,000 and $200,000 respectively (Chau 2007). It has since 1990 participated in UN Peacekeeping Operations (UNPKO) several of them in African countries. It is currently, or has been, involved in the following UN Peacekeeping Operations:

1. Democratic Republic of Congo (MONUC, established in 1999) with China supplying 218 troops, and 12 military observers;

2. Ivory coast (UNOCL, established in 2003) with China supplying seven military observers;

3. Liberia (UNMIL, established in 2003) with China supplying 565 soldiers, 18 police, and three military observers;

4. Ethiopia and Eritrea (UNMEE, established in 2000) with China supplying seven military observers; and

5. Western Sahara (MINURSO established in 1991) with China supplying 13 military observers.

In China's overall peacekeeping role in Africa, Chinese troops, or military observers are accordingly involved in humanitarian assistance, protection of human rights, national security reform, national police training, formation and restructuring of militaries, as well as functions of disarmament, demobilization, repatriation, resettlement, and reintegration (DDRRR). These functions are quite the opposite of the negative effects some of its arms transfers are having or have had on civil strife within these same countries where Chinese troops, police, or observers are operating.

Chinese contributions to peacekeeping in Africa are steady, consistent, and expanding. For example in the DRC it contributed 218 out of about 1,600 troops, in Liberia 565 out of about 14,000 troops, and in Ethiopia and Eritrea seven out of the 202 military observers. Most of China's peacekeeping personnel are military troops with expertise in various tasks and functions. While many play a defensive role of UN installations, personnel, and civilians, others have expertise in engineering, logistics, and health care. Those with engineering skills are often engaged in the construction of roads, bridges, camps, and digging of wells for water. Most of the troops that China contributes to peacekeeping are engineers, transportation experts, and medical staff. In the DRC, 175 of the 200 Chinese peace-keepers were engineers, in addition to 40

medical personnel (SAFERWORLD 2011). In other words, China's view of peace-keeping has a heavy focus on building infrastructure, providing medical care, and overall humanitarian assistance, as a way to promote its national interest, cement its economic relationship with African states, project an image of non-interference and a responsible major power in the international system (Fung 2016). This expanding role of China beyond the geo-economic objective of pursuing resources and profits is becoming a normal aspect of its foreign policy in the continent.

While on the one hand China's arms transfers are linked to civil strife and bloodletting, they are on the other hand used in peacekeeping operations. It could be argued that Chinese arms supplies to African peacekeeping troops involved in AU or UN peace-keeping operations play a positive role of improving peace and security. For example, Chinese supplied arms have been used in peace-keeping by Zambian troops in Sudan. China has consistently given its support to AU peacekeeping efforts and has made it part of its policy orientation towards Africa. In China's 2003 FOCAC Addis Ababa Action Plan it was stated this way:

> "We are resolved to step up cooperation and work together to support an even greater role of the United Nations, the African Union and other sub-regional organizations in Africa [It promised to] provide, within the limits of its capabilities, financial and material assistance as well as relevant training to the Peace and Security Council of the African Union. In order to strengthen capacity of African states to undertake peacekeeping operations, we look forward to the strengthening of China's cooperation with African states and sub-regional organizations in the areas of Logistics" (Forum on China-Africa Cooperation, Addis Ababa Action Plan, 2004–2006, 222).

Again, in the 2009 FOCAC Meeting, China reiterated its willingness to continue support for AU Peace-keeping and conflict resolution. In January 2010, as part of China's initiative, the UN Security Council deliberated on how best to maximize peacekeeping by the UN and sub-regional organizations. The Chinese Ambassador to the UN, Zhang Yesui, specifically underscored the need for the international community to aid African efforts at peace-keeping. He stated that:

> "The African Union and sub-regional organizations in Africa have been committed to resolving hotspot issues in Africa through good offices and peacekeeping operations, but their efforts are constrained due to deficiencies in funding and capacity building. We support the establishment and deepening of the strategic partnership between the United Nations and the African Union in maintaining peace and security in Africa" (HE Ambassador, Zhang Yesui, UNSC 2010).

China's previous rigid opposition to UN Peace-Keeping has softened since the late 1990s. It realized that Chapter VII UN Peace-keeping had become outdated

when examined in the light of situations in war ravaged countries of the DRC and Liberia in 2003. The brutality, carnage, and atrocities associated with the wars of the mid-1990s to early 2000s, made it necessary not just to limit peace-keeping to self-defense but rather to occasionally engage in peace-enforcement expressed in rapid and effective intervention to save civilian lives and even prevent further escalation of conflict. However, China's geo-economic interests at times stand in the way of allowing UN interventions in all countries. For instance, in 2006 China did not give its support for UN peace-keeping expansion in Sudan under UNMIS. It was only after a great deal of pressure from the international community, and its likely negative effect on the Olympic Games hosted by China in 2008, that it acquiesced to the wishes of the United Nations. At the same time, its contribution to peace-keeping in terms of numbers of troops and financial contribution surpassed that of the other great powers. In 2010 China's UN peace-keeping contribution reached $300 million (SAFERWORLD 2011). By 2010 the majority of Chinese peace-keepers were deployed in African countries such as Mozambique, Sierra Leone, Liberia, the DRC, Cote d'Ivoire, and others.

Influenced by its non-interference policy, China's peacekeeping troops largely play a "supportive role" of building infrastructure, providing medical, logistical, and transport support. China plays a very intensive and extensive peace-keeping role in the DRC, but at the same time it is a purveyor of small arms that are responsible for a great deal of the ethnic carnage, especially in eastern DRC. For instance, within MONUC China takes the lead role in military observer functions. China is so serious about peace-keeping that it has a Civilian Peace-Keeping Police Training Center to train Chinese police officers to be deployed to UN missions. It also established a Peace-Keeping Affairs Office in December 2001. In 2009, it further set up a new peace-keeping center for the training of Chinese military peace-keepers.

China has been heavily involved in peacekeeping activities even in a non-geo-economic country like Liberia. The UN Mission in Liberia established in 2003 focused on disarmament, demobilization, rehabilitation, and reintegration (DDRR) with the specific objectives of security sector reform, national police training, and a restructured Liberian army. The Chinese peace-keepers are mainly involved in infrastructure development and medical care. In July 2010 China deployed peace-keepers in Liberia numbered 585 strong, the fifth highest behind Pakistan, Nigeria, Bangladesh, and Ghana. The Chinese provide the main source of transportation for the peace-keepers. They transport not just peacekeepers, but fuel, water, and other essential items around Liberia. In the area of infrastructure rehabilitation, Chinese engineers have been busy upgrading roads and bridges, and with the maintenance of runways at airports around the country. By 2010, Chinese engineers along with other peace-keeping forces had rehabilitated hundreds of miles of road networks and bridges. In medical work, Chinese medical staff have provided basic health care to several town and villages, and also assisted in building local medical capacity (UNMIL 2010). Chinese police have also worked very hard on beefing up community security through the training of local Liberian police to effectively combat armed robbery, riots, and violent protests. The Chinese contingent has been especially commended for its efficiency and effectiveness in Liberia.

China is actively involved in peace-keeping in Africa for a number of reasons. Since peace-keeping is a multilateral effort, it is a way for China to show that it supports cooperative solutions to global security problems, especially ones that are relevant to Africa (Richardson 2011). Involvement at the UN level helps China boost its influence not just within this world body, but also among African nations. In other words, peace-keeping helps boost China's image as a responsible country that is actively engaged in promoting a peaceful and harmonious world. Its focus on Africa creates a positive image of itself among African nations at the UN and beyond (Fung 2015). With peace-keeping it enhances its multilateral and bilateral diplomacy in the international system. It has become the only Security Council member that does not hesitate to send its peacekeeping troops to troubled spots like the DRC, Sudan, or Liberia, among others (Yao 2016). Its willingness to deploy troops in African states counters the negative image created by its arms sales to despotic regimes and zones of conflict. Additionally, its active involvement in aid, trade, investment, and peacekeeping in Africa increases its geo-economic presence all over the continent. According to a report by SAFERWORLD in January 2011:

> "In some more general ways, peace-keepers do serve China's economic interests: they promote peace in countries where Chinese banks and commercial actors have made significant investments and have an interest in restoring stability. They also improve bilateral relations with the governments that have given their consent to peacekeeping missions" (76).

China is even using peacekeeping to interact with other militaries around the world within African nations. In Liberia it interacted with Indian, Pakistani, Nigerian, and other military troops. Liberian President Ellen Johnson-Sirleaf commended Chinese peace-keepers for not only enhancing the peace and security of Liberia, but for also contributing to its postwar reconstruction in the form of infrastructure development and helping to build medical capacity in the country.

China's involvement in peacekeeping in developing countries helps provide a sense of global legitimacy to peace-keeping operations since it is the only great power that is not viewed as being under the influence of the US and other Western powers. The Western powers are often viewed by many developing countries as simply out to enhance and even impose their agenda on smaller or weaker nations. It is perhaps only in Sudan that China is not viewed as legitimate or neutral because of its close geo-economic ties and extensive vested interests with the Khartoum regime. Another weakness in China's peacekeeping role is the fact that it is rigidly state-centric in its peacekeeping approach. Beijing's belief that only the state or incumbent regime can be legitimate alienates rebel factions or opposition groups within countries at war. It is not surprising that Chinese workers have been the victims of kidnapping and even massacres by rebel groups in conflict areas. China tends to deviate from guidelines set by the rest of the world regarding aid, trade, and investment. It is the same with its approach to peacekeeping. For instance, China is rigidly opposed to any form

of imposition on countries undergoing post-conflict reconstruction, especially an externally imposed and predetermined model of political and economic governance. According to Chinese scholars what is most important is not just the promotion of democratic governance, but the reduction of poverty and ending unemployment. The rationale is that poverty is associated with instability therefore the long-term objective of peace-building must be to ensure human security by focusing on alleviating both poverty and unemployment.

Summary and Conclusions

China's engagement with Africa is multipronged and predicated on a geo-strategy of geopolitical objectives with the primary focus on strengthening political ties with all states in Africa, and geo-economic objectives with the principal focus on access to Africa's resources. Both objectives are partly achieved by the seemingly contradictory policies of arms sales which generate profits for China, produce dependence by African states, and thereby enhance stronger political ties, and peacekeeping/peacebuilding activities by China which equally strengthen political ties with African states, but also give China a good image in the world. It is rather obvious that one of the anomalies of China's foreign policy toward Africa is the contradiction between its arms transfers to Africa on the one hand, and its peacekeeping activities on the other. There is a direct clash between monetary support for the AU, deployment of troops to achieve peace in areas of civil strife and interfering in Africa's conflicts through arms transfers. Chinese small arms are used in many of Africa's wars. During the Darfur "genocide" weapons used to commit atrocities against the people of Darfur were supplied by China. The irony is that the United Nations Mission in Sudan (UNMIS) included as many as 446 of the 900 soldiers, 9 of the roughly 660 police, and 14 of the 599 military observers. Similarly, during the war between Ethiopia and Eritrea China was known to have supplied both sides with weapons. However, the United Nations Mission in Ethiopia and Eritrea (UNMEE) established in July 2000, included a Chinese contribution of 7 out of the 202 military observers. Moreover, China is accused of supplying weapons to the Democratic Republic of Congo, while at same time contributing troops to the UN Mission in DRC (MONUC) in its support of disarmament, demobilization, repatriation, resettlement, and reintegration (DDRRR). China contributed 218 of the 16,594 soldiers and 12 of the 713 military observers in that conflict.

While China is not the only country to support both conflict resolution and weapons transfers in war-torn societies, its small arms have nonetheless contributed to protracted wars and bloodletting. In fact, China has been implicated in the Ivorian, Liberian, and Sierra Leonean conflicts because of the role played by Chinese firms smuggling small arms to rebels and mercenaries thereby prolonging and even exacerbating those conflicts. Arms transfers to developing countries never contribute to peace. Therefore one can conclude that China's non-interference policy is calculated to: (1) distance itself from the colonial legacy of the Western countries in Africa; (2) camouflage the aggressive pursuit of African resources and deflect attention from such

aggressive behavior while presenting an image of China being different from the West; and (3) shroud the fact that Chinese military personnel are ready to do battle and have even done so in Sudan, the Niger Delta of Nigeria, and the DRC. These points make China's longstanding policy of non-interference in Africa tenuous. In particular, China's arms transfer and peacekeeping policy in Africa is schizophrenic because it supports the AU peacekeeping efforts with funds, while at the same time supplying weapons to oppressive authoritarian regimes, effectively contributing to small arms proliferation through its modestly priced weapons, militarizing the African continent.

The danger in China–Africa relations is the fact that China could end up being a role model for the continent furthering human rights violations that could escalate into civil strife. Perhaps the most important concerns related to China's peacekeeping activities in Africa is reconciling its historical record with two fundamental concepts found in the definition peacekeeping; protection and promotion of basic human rights for individuals, the core values and primary goals of UN peacekeeping operations.

China has not fared well on the international scene, earning criticism for its suppression of human rights defenders, control, intimidation, and harassment of lawyers that take politically sensitive cases or seek redress of abuses of power at the hands of government officials, ethnic discrimination, and severe religious repression of Muslim Uyghurs in Xinjiang, mass rehousing and relocation policies in Tibet, and suppression of Hong Kong's "Occupy Central Movement," just to name a few.

In Africa, China is already playing out its human rights violations in places like Sierra Leone, where a mass and forced relocation of employees was carried out by the nation's largest mining employers. The families of the workers were forced to settle in an arid area that does not support productive agriculture. The reports of forced labor in mining sectors, poor safety conditions, long work schedules of up to 18 hour shifts, and anti-union activities enforced by Chinese companies in countries like Eritrea, Zambia, and Sudan, among others. The UN often points out that while China repeatedly calls for political solutions to conflict situations in African states, as an influential member of the UN Human Rights Council, it regularly votes to prevent scrutiny of serious human rights abuses in the continent and around the world. The persistence of human rights abuses in a country eventually results in political instability and human insecurity in all its various forms.

China's domestic policy emphasizing a "harmonious society" has been incorporated into its foreign policy toward Africa. What began as a policy to reduce inequalities and social injustice has now taken on a new meaning. "Stability at all costs" has become the overarching objective. Observers claim the government uses the ideology to justify suppression of dissent and tightening controls on information inside China. Extending and superimposing that ideology in Africa, China is assisting some African regimes like the one in Ethiopia in controlling and monitoring the use of the internet by its people. China has also helped the Zimbabwean regime of Mugabe in jamming the radio broadcasts of its opposition party.

While China seems to have made impressive strides in African security and peacekeeping activities through its financial and military assistance to the African Union and UN peacekeeping activities, its priority in Africa is still geo-economic

interests or economic ties with African states. Because bilateral economic activities are the greatest focus of China in Africa, peacekeeping and security issues have not yet been discussed with sub-regional organizations like the Economic Community of West African States (ECOWAS) in West Africa. Outright or significant commitment by China for a more effective African Union or an African security force may be slow in coming. However, some Chinese scholars have proposed the idea of an African Peace Fund as a key condition for more effective African peacekeeping efforts. China would most likely prefer to work with the UN in its efforts to contribute to African peace and security. While African sub-regional organizations and the AU can collectively put pressure on China to do more in the area of security and peace in Africa, it appears that China will continue to improve its record on peacekeeping via the UN and its peacekeeping missions in Africa as a way of counteracting the accusations that it is flooding Africa with small arms that are used in many of the ongoing conflicts.

The current levels of China's peacekeeping activities in Africa have had a positive impact because of the level of infrastructure development and medical work performed by Chinese peacekeepers. However, some of the potential obstacles to an expanded Chinese peacekeeping effort would be: (1) the issue of what constitutes legitimate intervention; and (2) China's role in arms transfers that help fuel conflicts in contrast to its peacekeeping activities. Positive developments are that China is becoming more flexible with regard to the legitimacy of UN peacekeeping interventions, and it is at times even advocating within the UN Security Council use of peace-enforcement in situations of gross violations of human rights and humanitarian crisis.

While China supplies a significant number of weapons to states with critical resources with which it maintains strong trading ties, there are also states such as Ghana or Uganda which are not significant in terms of exporting critical resources to China, but maintain strong military ties with China. This means that China is also using arms transfers as a means of enhancing its commercial profits. Arms transfers whether they generate positive or negative effects are simply part of the multipronged diplomatic strategy of China toward Africa. Other dimensions of China's multiple diplomacy are in the areas of aid, trade, investment, health education, and culture. The arms transfer sector is increasing in scope but still lags far behind the aid, trade, and investment strategy. Arms transfers therefore, play the dual role of consolidating relationships/ties with African states, and to some extent, acting as a commercial end in itself.

Finally, the argument can be made that because African armies are poorly equipped and underfunded, Chinese military aid is beneficial to them because it helps uphold the internal integrity, if not territorial integrity of African states. However, on a more critical level, the virtual lack of interstate wars among African states results in regimes using weapons for self-preservation purposes. Such was the case in Guinea. Overall, China is likely to expand and intensify its military relationships with Africa via arms transfers, military attaches, high level military exchanges and meetings, and even joint military exercises.

On a more critical reflection, the African security implications of China's seemingly contradictory role in Africa is manifested in a rhetoric of non-interference

and peace-building, contradicted by the proliferation of light and inexpensive weapons implicated in some of the most serious cases of bloodletting on the continent. It could be argued that as China widens its engagement with African states it will continue to consolidate military agreements, and engage in more arms transfers on a continent that already has a strong potential for the eruption of more conflicts related a combination of gross inequalities, ethnic rivalry and diversity, and the absence of the rule of law, as well as a strong culture of coups, civil wars, and other forms of civil strife. While it is true that China is not the only great power supplying weapons to African states, the affordability of Chinese weapons enables protracted African wars, and their continued proliferation within the continent. This is more likely to be the case in both the near and distant future because China often does not adhere to UN arms embargoes, sanctions against African states, or their diplomatic isolation. Its preoccupation to consolidate its diplomatic ties, and strengthen its partnerships with African states means it often takes an approach different from those of Western states.

References

Agubamah, Edgar. 2014. "China and Peacekeeping in Africa." *International Journal of Humanitarian and Social Science* 14 (11 pp.193-197.).

Alessi, Christopher, and Beina Xu. 2015. "China in Africa." *CFR Backgrounds*. www.cfr.org/china/china-africa/p9557 (accessed August 15, 2016).

Amnesty International on Darfur. 2012. "Sudan: No End to Violence in Darfur." http://www.amnestyusa.org/research/reports/sudan-no-end-to-violence-in-darfur (accessed August 15, 2016).

Baah, Anthony Y., and Herbert Jauch, eds. 2009. "Chinese Investments in Africa: A Labour Perspective." *African Labour Research Network*, May 2009. www.cebri.org/midia/documents/315.pdf

Baker, Benjamin D. 2015. "Chinese Arms Companies are Picking up the Pace in Africa and the Middle East." *The Diplomat*. www.thediplomat.com/2015/Chinese-arms-companies-are-picking-up-the pace-in-africa-and-the-middle-east (accessed August 15, 2016).

Bitzinger, Richard A. 1991. *Chinese Arms Production and Sales to the Third World*. Santa Monica, CA: Rand.

Caldwell, Mark. 2015. SIPRI: "China's Arms Trade with Africa at Times Questionable." www.dw.com/en/sipri-chinas-arms-trade-with-africa-at-times-questionable/a-18319346 (accessed August 15, 2016).

Chang, Andrei. 2007. "Chinese Arms and African Oil." *SpaceDaily*. http://www.spacedaily.com/reports/Analysis_Chinese_arms_and_African_oil_999.html (accessed August 15, 2016).

Chau, Donovan C. 2007. "Political Warfare in Sub-Saharan Africa: U.S. Capabilities and Chinese Operations in Ethiopia, Kenya, Nigeria and South Africa." http://www.strategicstudiesinstitute.army.mil/pdffiles/pub766.pdf (accessed August 15, 2016).

Deen, Thalif. 2005. "Politics: NGOs Blast Security Council for Inaction in Sudan." www.ipsnews.net/2005/03/politics-ngos-blast-security-council-for-inaction-in-sudan/ (accessed August 15, 2016).

Enuka, C. 2011. "China's Military Presence in Africa: Implications for Africa's Wobbling Peace." *Journal of Political Studies* 18 (1): 15–30.

Forum on China-Africa Cooperation, Addis Ababa Action Plan, 2004–2006. http://www.focac.org/eng/ltda/dejbzjhy/DOC22009/t606801.htm (accessed August 15).

Fung, Courtney J. 2015. "What Explains China's Deployment to UN Peacekeeping Operations?." *International Relations of the Asia-Pacific* doi:10.1093/irap/lcv020

Fung, Courtney J. 2016. "China's Troop Contributions to U.N. Peacekeeping." www.usip.org/publications/2016/07/26/china-s-troop-contributions-un-peacekeeping

Grant, Jonathan. 2012. "Merchants of Death: The International Traffic in Arms." *Origins, Current Events in Historical Perspective* 16 (3).

Human Rights First. 2008. "China's Arms Sales to Zimbabwe." *Fact Sheet*. https://www.humanrightsfirst.org/wp-content/uploads/pdf/080428-CAH-china-zimbab-arms-fs.pdf (accessed August 15, 2016).

Hyer, Eric. 1992 "China's Arms Merchants: Profits in Command." *China Quarterly* 132: 1101–1118.

Klare, Michael. 2014. *American Arms Supermarket*. Austin: University of Texas Press.

Lynch, Colum. 2012. "China's arms exports flooding sub-Saharan Africa." The Washington Post (WP Com (US) https:www://washingtonpost.com/world/national-security/chinas-arms-exports-flooding-sub-saharan-africa/2

Mahtani, Dino, and David White. 2006. "China in Move to Gain Foothold in Nigerian Oilfields." *Financial Times*, April 27. http://www.ft.com/cms/s/0/bc85fc3e-d58a-11da-93bc-0000779e2340.html#axzz4HRGK7UVO (accessed August 15, 2016).

McPartland, Ben. 2012. "China's Presence Grows in Murky World of Arms Trading." http://www.france24.com/en/20120307-china-arms-trade-africa-sudan-usa-uk-business-military (accessed August 15, 2016).

Mullen, Jethro. 2016. "China's Weapons Sales to Other Countries are Soaring." *CNN Money*, February 22. money.cnn.com/2016/02/22/news/china-arms-exports-rising/

Pierre, Andrew J. 1982. *The Politics of Global Arms Sales*. Princeton, NJ: Princeton University Press.

Puska, Susan. 2007. "Military Backs China's Africa Adventure." *Asia Times*. Http://www.atimes.com/atimes/china/if08ad02.html (accessed August 15, 2016).

Richardson, Courtney J. 2011. "A Responsible Power? China and the UN Peacekeeping Regime." *International Peacekeeping* 18 (3): 286–297.

Rothberg, Robert I. 2015. "China Joins African Peacekeeping." www.chinausfocus.com/peace-security/china-joins-african-peacekeeping

SAFERWORLD REPORT 2011: Chinese Growing Role in African Peace and Security. http://www.saferworld.org.uk/resources/view-resource/500-chinas-growing-role-in-african-peace-and-security (accessed August 15, 2016).

Sanders, Ralph. 1990. *Arms Industries: New Suppliers and Regional Security*. Washington, DC: National Defense University.

Schelling, Thomas C. 2008. *Arms and Influence*. New Haven, Conn. Yale University Press.

SIPRI Yearbook. 2011. Oxford University Press on behalf of Stockholm International Peace Research Institute. http://www.sipriyearbook.org/view/9780199695522/sipri-9780199695522.xml (accessed August 15, 2016).

Taylor, Ian, and Zhengyu Wu. 2012. "China's Arms Transfers to Africa and Political Violence." *Terrorism and Political Violence* 25 (3): 457–475.

United Nations Security Council. 2010. http://www.un.org/en/sml (accessed August 15, 2016).

Wengraf, Lee. "The New Scramble for Africa." *International Socialist Review*, Issues #60 Features. isreview.org/issue/60/new-scramble-africa

Yao, Jianing. 2016. "U.S. Military Observers Visit Chinese Peacekeeping Infantry Battalion in South Sudan." *China Military Online*, March 22. http://eng.mod.gov.cn/DefenseNews/2016-03/22/content_4647228.htm

Young, Tom. 2016. *Readings in the International Relations of Africa*. Bloomington: Indiana University Press.

Review of *On Intelligence: The History of Espionage and the Secret World*

John Hughes-Wilson (2016). *On Intelligence: The History of Espionage and the Secret World*, First Edition. London: Constable. ISBN: 978-1-472-11353-5. 528 pages. £25.00

The field of intelligence studies is a relatively new academic discipline that has developed an identifiable intellectual community. It has served as a conduit through which the history of war, the development and decline of empire as well as the calibration of foreign policy have been subjected to fresh formats of inquiry and analysis. The study of the relationship between the practice of intelligence and its impact on state policy in so far as military action is concerned is one, given the repercussions, respectively, of the attack on 9/11 and the decision to go to war against Saddam Hussein's Iraq, that is of particular interest to scholars, policymakers and practitioners of the craft. It is also a subject area of inestimable fascination to a general reading public with a ready appetite for stories on espionage and accustomed to a market in which there has been a surge in the popular history genre. This has meant that studies on the history of military intelligence, as is the case with other genres of history, have been divided into those that fit alternately into the academic and popular writing categories.

John Hughes-Wilson, a retired British Army Intelligence Corps colonel whose career spanned active service in the Falkland Islands and Northern Ireland as well as administrative postings in Whitehall and NATO, is an author whose offerings on military intelligence history fit into the popular writing category. His brief but robust introduction offers no apologies for avoiding "getting completely lost in the thickets of philosophy and Hegelian dialectic" as an academic text might tend to do. Instead, his work adopts a case study approach to explain and analyze the operation of the intelligence apparatus within the context of espionage and the conduct of war.

Before this, he takes the reader through preliminaries: a chapter on a condensed history of the development of what he refers to as the "Second Oldest Profession" from biblical times to the modern era, followed by a brief consolidating chapter stressing the importance of intelligence in national self-defense by references to statements written by Machiavelli and Sun Tzu while at the same time offering words of rebuke for the shortcomings of Clausewitz's 1832 masterwork, *On War*. He provides a lucid overview of the fundamentals of the intelligence cycle, providing admittedly simplified diagrammatic representations of the process, a collection plan as well as an indicator and warning display. These are tools he deploys to function as key reference points for analysis when he explores the different themes which he proceeds to set out. His consideration of HUMINT and the factors typically enabling intelligence agencies to penetrate their competitors is predicated on the traditional MICE acronym: Money, Ideology, Compromise/Coercion and Ego. These factors provide the backdrop to his retellings of major espionage failings and successes of American and British intelligence agencies including that of the Walker family's betrayal of U.S. Navy secrets and Oleg Penkovsky's role in the Cuban Missile Crisis.

doi: 10.18278/gsis.2.1.7

Hughes-Wilson is particularly adept at fleshing out the historical development of SIGNIT and IMINT from the most rudimentary technology to the highly advanced equipment of today. His case study on how signals intelligence was crucial in ensuring the victory of the U.S. Navy over the Imperial Japanese Navy at Midway is particularly gripping. It is also enlightening about the organizational pathologies perpetually at play in contemporary intelligence structures, one aspect of which relates to the vexed question of the ownership of SIGNET: does it reside with the communicators and signalers on the one hand or with the intelligence people?

Hughes-Wilson is an engaging writer who brings the reader inside the mind of the prudent intelligence operative: consistently asking questions and performing an officious bystander test as he sifts through large amounts of information. He is very good at guiding the reader through the practical application of the theories undergirding the intelligence process. This is particularly illuminating in regard to his summation of the severe deficiencies in the American intelligence apparatus in 1941 on the eve of a war that all knew was coming. For it is the case that the problems leading up to Pearl Harbor, including those of over compartmentalization and inter-organizational rivalries, are ones of enduring relevance and bring into focus the need for all-source integration and assessment; an ideal which is difficult to achieve within any national security establishment.

The choice of case studies tailored to fit a particular theme of the intelligence process, whether related to failures or successes, provides the basis for a series of illuminating deconstructions. For instance, the failure of the political leaders of the Soviet Union and Israel to predict the oncoming onslaughts, respectively, of Operation Barbarossa in 1941 and Operation Badr in 1973 was due, Hughes-Wilson argues, not with nonpossession of the correct information predicting enemy intentions but instead centered on the translation of information into intelligence. In the former case, it hinged on a developed organizational culture of only reporting information which the dictator found palatable while the latter was caused by the monopolization of all-source intelligence by Israeli Military Intelligence. On the issue of protecting state secrets, he uses the recent high-profile cases of Bradley Manning, Julian Assange, and Edward Snowden as exemplars explaining the impact of an inadequate security checking mechanism, the increasing difficulty of securing masses of electronically collected data in the high-technology age and the eternal dilemma of balancing national security concerns with that of protecting whistleblowers acting in the public interest. For deception, the Allied planning of the highly risky, but ultimately successful, D-Day landings is used while the area dealing with intelligence fiascos considers the U.S. Special Forces operations in Son Tay, Vietnam and Iran at the time of the hostage crisis. The author also provides an excoriating analysis of the role played by the leaders of the British intelligence community in enabling the administration of Tony Blair to produce a "dodgy dossier" which led the country into a war of dubious legality against Saddam Hussein's Iraq in 2003.

The issue of intelligence and the challenges posed to national security by terrorism and by cyber warfare are also given consideration by the author. He provides a thoughtful summary on the grievances and "catalysts for conflict" that often form the

backdrop to terror campaigns before focusing on the contemporary security concerns associated with the "War on Terror". He is adept at summarizing the interrelatedness of cyber war, cyber terrorism, and cybercrime. Here, the threats posed by China, the Russian Federation, and North Korea are pointedly noted as he stresses the complexities associated with tracing the source of attacks and the severe consequences that could impinge on civil and military capacities in the event of an all-out war.

Hughes-Wilson provides a lengthy but highly readable consideration of military intelligence that succeeds in giving the reader a fairly comprehensive overview of the practice of intelligence and security. While it falls short of the rigor expected of an academic text in terms of theoretical detail and the provision of a comprehensive bibliography and citations, it cannot be faulted for being unchallenging or lacking in analytical content. The revolutionizing effect of technological advancement on the gathering, dissemination, and evaluation of intelligence is cogently explained as indeed is the underpinning rationale of his assessment that Julian Assange's "Wikileaks" project has succeeded in redefining security.

But it does have its shortcomings. For instance, there is no discernible standard regarding the selection or non-inclusion of case studies. Also, given the contemporary prevalence of asymmetric warfare, an examination of the role of intelligence in conflicts between state and nonstate militaries would have been apt. The conflict in 2006 between Israel and the Lebanese militia Hezbollah would have presented an ideal case study. It is clear to military analysts that a series of skillfully planned deceptions and security strategies on the part of Hezbollah provided the means for the militia to withstand the might of the Israeli Defence Force. A thorough consideration of intelligence ought arguably to have included an appraisal of the darker aspects of the use of intelligence gathering in counterinsurgency strategies. U.S. military intelligence covertly orchestrated death squads using a recurring modus operandi to tackle insurgencies in Vietnam, Central America, and Iraq while British army officer Frank Kitson's concept of "gangs and counter-gangs" was ruthlessly employed in Kenya and Northern Ireland. In a similar vein, the use of anti-Warsaw Pact "stay behind" cells under the command of NATO during the Cold War-era communist containment strategy is not mentioned. Still, as a work which covers a great deal of ground and one that attempts to synthesize a narrative and analysis of the broad aspects of process and organizational efficacy within the political contexts of the day, it is likely to be of interest not only to the connoisseurs of popular history, but also to scholars and practitioners in the field of intelligence.

Adeyinka Makinde
University of Westminster

Review of *Confronting Al Qaeda: The Sunni Awakening and American Strategy in Al Anbar*

Martha L. Cottam and Joe W. Huseby, with Bruno Baltodano (2016). *Confronting Al Qaeda: The Sunni Awakening and American Strategy in al Anbar.* Rowman & Littlefield Publishers. ISBN: 978-4422-6485-4 (Hbk), 978-1-4422-6486-1 (Ebk). 150 pages.

Confronting Al Qaeda: The Sunni Awakening and American Strategy in Al Anbar by Martha Cottam, Joe Huseby, with Bruno Baltodano is an excellent analysis on the Sunni Awakening during Operation Iraqi Freedom. The book is well-researched and presented with sound critical analysis. Perhaps the greatest strength of the book is the incorporation of image theory. Image theory is used in International Relations to evaluate perceptions, and in this case, it is primarily used to explain the tribal perceptions of Al Qaeda in Iraq (AQI, later ISIS) and the American military in Al Anbar.

Cottam, Huseby, and Baltodano discuss the evolution of the Sunni tribes in Al Anbar province from the beginning of the Iraq War in 2003 through the period of the Awakening to the resurgence of ISIS. The authors clearly demonstrate that while the tribes had affiliation with Saddam Hussein prior to the war, it was not a case of supporting the former regime. The initial policies implemented by the transitional government hurt the image of efforts of the United States in Iraq through sweeping policies implemented by those who had little understanding of the geo-political situation within Iraq. These policies alienated the Sunni tribes and allowed AQI to exploit the situation, which, along with a growing insurgency (also fueled by misguided policies), led to violence and chaos in the post-Hussein Iraq.

The authors further explained that once the Sunni tribal leaders realized that the goal of AQI was to destroy the tribal identity in order to advance their own ideology, the tribal sheiks began to look toward the Americans. Almost simultaneously, the U.S. military realized that it needed to change its strategy, in regards to dealing with the tribes, and began to employ and negotiate with the sheiks in order to develop an anti-AQI alliance in Al Anbar. As strategies were developed that removed AQI presence in towns across Al Anbar province, the joint United States and Sunni tribal alliance built police stations, networks of informants, economic opportunities, and enhanced infrastructure to consolidate their gains. The authors do an admirable job relating how these efforts met with resistance from the Shi'a-led Iraqi central government in Baghdad. Despite these challenges from Baghdad, the Sunni Awakening was tremendously successful in liberating their province from the control of AQI.

Throughout *Confronting Al Qaeda*, the authors routinely point out the changes in the tribes' perception of AQI and the United States. The authors' use of image theory is valuable tool to explain how and why these changes occurred. Introduced on page 13, Table 1.1 provides the type of images as well as the associated characteristics of these images. For example, the table discusses the imperialist, barbarian, rogue, ally, and enemy images in image theory that relate to the post-Saddam Iraq in Al Anbar. The

doi: 10.18278/gsis.2.1.8

authors do discuss the image theory from multiple perspectives, but the key discussion in how the tribes' perceptions evolved from 2003 to 2007. This evolution is based on interviews from key leaders, to include sheiks, from both the tribes and U.S. military. The authors discuss each shift in perspective at the end of each chapter to reinforce the events that occurred during that time period and the relationship to image theory.

I highly recommend *Confronting Al Qaeda, The Sunni Awakening and American Strategy in Al Anbar* to any student interested in understanding the events that occurred in Al Anbar province from 2003 to 2007 during Operation Iraqi Freedom. It is primarily an analytical effort, using strong empirical data, to explain the successes that the United States found during the Iraq insurgency. Above all, it is an important reminder that success in counterinsurgency operations is found through a mature understanding of the complex operational environment that militaries are likely to encounter after regime change.

James Hess, Ph.D. Faculty Director and Associate Professor
American Public University System

Review of *The Spy's Son: The True Story of the Highest Ranking CIA Officer Ever Convicted of Espionage and the Son he Trained to Spy for Russia*

Bryan Denson (2015). *The Spy's Son: The True Story of the Highest Ranking CIA Officer Ever Convicted of Espionage and the Son He Trained to Spy for Russia*. London: Scribe Publications. ISBN: 9781925106657 (pbk). 368 pages

The same motivations that compel an individual to spy for their country can be the very things that motivate them to betray the same. Recruitment and running of intelligence agents versus counterintelligence and the discovery of spies in our midst have fascinated, and repulsed, those both within and without the business for centuries. They present extremes—often the ultimate acts of bravery or treachery depending, once again, from whichever viewpoint one sits.

In mid-1994, only 2 months after CIA counterintelligence officer Aldrich Ames was sentenced to life in prison for betraying many of the most closely guarded secrets of U.S. intelligence operations against the Soviet Union, another CIA operations officer, Harold James "Jim" Nicholson was offering his services to the recently emerged Russian Foreign Intelligence Service (SVR); the newly renamed First Chief Directorate of the KGB.

A very good case officer Nicholson had had a number of overseas posting and deployments during his career with the CIA. Much of his case work, as explained in the book, was focused on transnational threat issues, including counterterrorism and organized crime, but one of his more recent postings at home was as a senior instructor at the CIA's training facility in Virginia—colloquially known as "The Farm." It was here that Nicholson would be responsible for training the next generation of CIA case officers; he would know those who would be posted overseas in diplomatic roles, and he would know those being considered for "nonofficial cover" (or NOC) roles. Nicholson would have, of course, known the Ames story and surmised that the Russians might "be in the market for another highly placed mole inside the CIA." He might not have direct access to the "crown jewels" in espionage parlance—how the Americans might have penetrated Russian intelligence—in the way that Ames and FBI mole Robert Hanssen would, but he would have the next best thing; the names of the next crop of American spies lining up to participate in "the Great Game."

Fifteen years after Ames' conviction, the author Bryan Denson, an investigative reporter with The Oregonian, first came across Nicholson as he was about to be charged with espionage crimes for the second time. Nicholson's youngest child, Nathan, was also in the courthouse that day. Thanks largely to the 20-year-olds evidence, Nicholson senior would become not just the highest-ranking CIA officer ever convicted of espionage, but also the only U.S. intelligence officer caught betraying his country on two separate occasions, and the only American discovered and convicted of engaging in espionage activities with a foreign government from within the confines of an American federal prison.

doi: 10.18278/gsis.2.1.9

The result of that chance encounter saw Denson spend the next 5 years investigating the circumstances that lead to this extraordinary situation, and *A Spy's Son* tells what he discovered. Denson would initially discover that Nicholson had first been sentenced to nearly 24 years for spying for the SVR in 1997. As with nearly all espionage or intelligence cases like this one, much of the story in the public record, but a lot was not. It is believed that former KGB/SVR Counterintelligence Officer—and CIA source—Alexander Zaporozhsky—was responsible for pointing the Americans in the direction of Nicholson. The Soviet spy was to the CIA what Nicholson was to the KGB/SVR and, as Denson suggests, "Jim and Zaporozhsky weren't all that different. They climbed to the higher rungs of their nations' respective spy services, and picked their nation's pockets to sell secrets to their competitors."

The author pieces the more familiar background together with a selection of first-hand accounts from sources close to both cases. Members of the family, including Nathan—who spent some 200 hours being interviewed—provide further depth of background and context which enables Denson to examine the intertwined layers of betrayal and treachery. Denson describes how Nicholson was able to manipulate his son, and exploit Nathan's desperate and unconditional love and loyalty, in order to re-establish contact with the SVR again. Nathan was soon his father's enthusiastic agent, but in less than 2 years, he had been arrested by the FBI. How he was discovered, why he confessed, and what happened to both after they were convicted are described by Denson in a dispassionate, but genuinely sympathetic, narrative that places a more human face on what many will still regard—particularly after reading this book—as a most sordid profession.

The story of Jim Nicholson's treachery is not a particularly well-known one compared to other Cold War and post-Cold War traitors; Ames, Hanssen, and the most famous "Harold" of them all—Harold Adrian "Kim" Philby. But what makes Nicholson's act of betrayal all the more significant, and something that Denson draws out particularly well, is that his psychopathy seemingly knew no bounds. We ultimately see that Nicholson senior was of sufficient moral reprehensibility that he convinced his youngest son Nathan, who absolutely adored his father, to do exactly the same. The quality of tradecraft demonstrated by Nicholson senior, although impressive as it is, must stand to one side as the author weaves a sorry tail of destroyed ego, egomania, betrayal and self-aggrandisement of epic proportions; an individual described in the book as a "cunning, self-centred, self-righteous, and evil…master manipulator."
A worthwhile addition to any intelligence studies enthusiast's library.

Rhys Ball
Military Historian and Intelligence Studies Lecturer
Massey University's Centre for Defence and Security Studies (CDSS)
Auckland, New Zealand

Review of *The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal*

David E. Hoffman (2015). *The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal.* New York: Doubleday . 0385537603. Photographs. Notes. Index. Pp Xii, 336

The Billion Dollar Spy is easily one of the catchiest titles to come out of the nonfiction Cold-War war-in-the-shadows era. In fact, the dust jacket art makes it appear to be misplaced on bookstores shelves, as it looks like one of those seemingly churned out "thrillers." Instead, David E. Hoffman has given us a real-life thriller that rivals its fictional counterparts, except there are no exotic locations, handsome James Bond, or Jason Bourne type men or exotic and dangerous femme fatales.

Adolf Tolkachev is the hero of the book and, unlike our cinema stars, was a hero in the greatest sense of the word. Tolkachev is perhaps as great of a hero as the earlier Soviet spy Oleg Penkovsky, code named HERO who informed the clueless West among other things of the presence of Soviet nuclear missiles in Cuba. In the West, those who sold secrets to the Soviets generally did so for financial gain. Robert Hansen stands to mind for sheer greed but so do the Walkers, a family that was a spy ring whose disclosures to the Soviets left the West vulnerable to a first strike by Soviet nuclear ICBM submarines as they disclosed how NATO tracked Soviet submarines through the critical UK–Greenland–Iceland gap. Then you have those who were attracted for ideological purposes, generally those of a leftist bent to start with such as the Cambridge Five and the Rosenbergs, and other Soviet agents that were attracted by the New Deal. Tolkachev is vastly different from these types because it is harder to get a grasp on his motivations. Penkovsky is easier to understand as his family, despite his rise to some prominence, had suffered from the Bolshevik Revolution. However, Tolkachev is harder to profile in any of the normal psychological aspects.

Yet Tolkachev seems to be a mere historical footnote until this work. How important was he? In the late 1970s, it seemed that the Soviets had moved ahead of the West in fighters and radars. Tolkachev from 1978 to 1985 gave his handler officers thousands of pages of top-secret documents. The book goes into great detail how Tolkachev had to be ingenious and innovative in gaining access to the materials as well as the necessary spy craft. The parts on his use of cameras, dead drops and such, all standard spy genre fare, become far more interesting when you realize a single slip means the death of not a fictional character but a man with a family. The key revelations that Tolkachev gave to the West dealt with their ground radars that defended against attacks, and radars on their warplanes that provided an unknown new capacity, that would gain a tactical advantage in aerial combat by achieving faster lock-on for their missile systems.

Hoffman savages the Central Intelligence Agency by taking them to task for their failure to respond to the Soviet threat by developing sources. Hoffman lays out in brutal fashion that James J. Angleton, head of counterintelligence from 1954 to

doi: 10.18278/gsis.2.1.10

1974, did as much damage as any Soviet agent. Angleton was obsessed with moles and feared that EVERY Soviet "walk-ins" were provocateurs. Admiral Stansfield Turner later ordered a freeze on any Moscow ops for fear of a penetration, turning away ALL valuable sources. It is with good cause why the American people have right to question the leadership of the Intelligence Community as they seem, time and time again, like Sisyphus, doomed to roll the rock of wrong decisions up the hill.

Like Macintyre's work on Kim Philby, the British intellectual who betrayed the West, this book is a must read. It is interesting to note that what seemed dangerous to us from that era seems now almost polite compared to ISIS beheadings and mass suicide attacks in marketplaces. What the book drives home in an understated fashion is that the American and Western Intelligence Community, despite 60 years of effort, never really got a foothold in the Soviet system, despite the expenditure of billions of dollars. The lesson for today is relevant for when we hear the Intelligence Community talking about all the resources devoted to the fight against terrorism. Use this as a lesson—and note we have had no real defections from inside the Islamo-fascist movements. The lesson here is simply that individual heroism will sometimes win out over bureaucratic ineptness. Thankfully, the Soviets were as hidebound in some of their methods as the West; else, the bravery of individuals like Tolkachev would have been for naught, whose documents one must consider led to the final victory of both sides who did not find cause to unleash a nuclear Armageddon.

Robert Smith