ASPJ
Africa and Francophonie

3rd Quarter 2016　　　　　　　　**Volume 7, No. 3**

AU PRESS

AIR UNIVERSITY
INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE

AIR FORCE RESEARCH INSTITUTE

AIM HIGH . . . FLY-FIGHT-WIN

AIR & SPACE POWER JOURNAL

http://www.af.mil

http://www.aetc.randolph.af.mil

http://www.au.af.mil

Editorial

Articles

Cyber Power, Deterrence, European Union Peace Building, International Courts and Tribunals, and Climate Change and Conflict Prevention

Military practitioners face a daunting task, posits Col Richard J. Bailey Jr. in "Dilating Pupils: The Pedagogy of Cyber Power and the Encouragement of Strategic Thought." They must incorporate cyberspace and cyber power into an already complex suite of military applications. However, our nascent experience with the technology shows that we have yet to understand fully the domain's intricacies. Students of cyber strategy must acknowledge and respect the challenges inherent in this conundrum. Thinking strategically about cyber power is a complex endeavor. This article proposes that strategy is ultimately dependent on understanding one's environment and adapting to uncertainty; thus, we still have much work to do in the cyber domain. Biases and frameworks, many of which result from etymological foundations, often hamper our understanding of the cyberspace environment. In addition, contextual confusion often leads to polarization in the early literature and a tendency to use anachronistic analogies to aid in comprehension—both of which present problems to strategic thinking. Uncertainty in cyberspace is a product of the dialectical nature of strategy and the limits to useful information—both organic and synthetic—inherent in cyberspace and in our application of cyber power, therefore making adaptation critical to the cyber strategist. To make the most of their intellectual journey, students of cyber strategy must attempt to address these challenges or, at the very least, respect them.

In "Uncertainty and Deterrence," Prof. Yakov Ben-Haim postulates that the decision to initiate or refrain from war is accompanied by multifarious uncertainty. Uncertainty deters, but deterrence is uncertain. What looks like the better option may be more uncertain than the alternative, so the decision maker may choose the putatively less attractive option. The author develops an analytical framework for studying this reversal of preference. The analysis uses two concepts: the innovation dilemma and robust satisficing (satisfying a critical or essential outcome requirement). Decision makers face an innovation dilemma when they

choose between a new, innovative, but poorly understood option and a standard option that is more thoroughly understood. The decision makers want the best possible outcome, but all outcomes are highly uncertain. The robustly satisficing choice is the one that meets critical requirements despite large error or surprise. Professor Ben-Haim discusses a historical example—the Six-Day War—and applies his analysis to a theoretical question: does uncertainty increase the propensity for war?

Prof. Witold Mucha's article "Enable and Enhance—That's It? European Union Peace Building and the Enable and Enhance Initiative" postulates that in the summer of 2014, Germany's decision to supply arms to Kurdish Peshmerga in their fight against the Islamic State of Iraq and Syria (ISIS) revealed the importance of the Enable and Enhance Initiative (E2I) as discussed by the European Union's (EU) member states. In addition to Berlin, policy makers in London and Paris, among others, also followed the rationale of taking responsibility in foreign affairs without being directly involved in military combat. However, as recent initiatives have shown, the E2I approach comes with limitations. Based on EU peace-building initiatives in South Sudan and Mali, the article analyzes the challenges confronted by any "getting fit initiative." The analysis comes to a twofold conclusion: (1) recent EU peace-building missions have failed in terms of design, scope, and unintended effects, and (2) academics have similarly failed to recommend feasible policy solutions.

International courts and tribunals have experienced strong growth over the last two decades, but no such institution has been established for international environmental governance. In "The Role of International Courts and Tribunals in Global Environmental Governance," Prof. Steinar Andresen notes that many existing international courts are relevant to this issue area but that they have had very little significance in terms of the effectiveness of global environmental governance. Because of the alleged ineffectiveness of this system, nonstate actors have argued for the establishment of an international environmental court (IEC). No state support this idea since they prefer the existing system. This article argues that a new IEC would probably not make much difference in the effectiveness of this governance system and that the chances that one will be established in the foreseeable future are extremely low.

The article "The Implications of Climate Change for the Military and for Conflict Prevention, Including through Peace Missions" by Prof. Shirley Scott and Mr. Shahedul Khan discusses five implications of climate change for the military: (1) installations and equipment will be affected by the consequences of climate change, including rising sea levels, (2) the military will have an increased responsibility to reduce its own environmental footprint, (3) military strategists will need to factor the consequences of climate change into their planning, (4) the military is likely to play a greater role in responding to natural disasters, and (5) the military will contribute to enhanced emphasis on conflict prevention. The

article explores in further detail the potential for peace operations to contribute to climate change adaptation as one dimension of conflict prevention.

Rémy M. Mauduit, Editor
Air and Space Power Journal–Africa and Francophonie
Maxwell AFB, Alabama

Dilating Pupils

The Pedagogy of Cyber Power and the Encouragement of Strategic Thought

C OL R ICHARD J. B AILEY J R ., P H D*

> *Actions taken and actions to be taken are weighty factors in the strategist's thinking, of course, but they are elements to be shaped and manipulated, not strict lessons leading to instructions that must be followed.*
>
> —Everett Carl Dolman
> *Pure Strategy* (2005)

T he pedagogy of cyber power presents an interesting conundrum. Although cyberspace and its related technologies have been around for decades, our *thinking* about them has yet to mature. Given the prominence of cyber power in recent international struggles, however, the urgency of integrating the technology into military strategy introduces a particular challenge. How do we *use* cyber power when we have yet to *understand* it? On a related note, how do we *teach* cyber power, particularly to practitioners who are expected to incorporate it into strategic decision making, given this lack of understanding? An exploration of this puzzle requires that we first examine the challenges of teaching strategy, independent of the particularities of cyber power. Next, a study of the environment of cyberspace will expose its etymological frameworks and biases, perhaps informing how modern

*The author is an associate professor of strategy and security studies at the School of Advanced Air and Space Studies, Maxwell AFB, Alabama. He earned his BS in engineering sciences at the United States Air Force Academy in 1992, an MA in international affairs from Washington University in St. Louis in 1997, and a PhD in government from Georgetown University in 2006. His research interests include military strategy, civil-military relations, American sociopolitical behavior, and cyber power. His latest works include *Strategy: Context and Adaptation from Archidamus to Airpower* (Annapolis, MD: Naval Institute Press, 2016) (coeditor and contributing author); *The Baltic Security Puzzle* (Lanham, MD: Rowman and Littlefield, 2015) (chapter contributor); "Fighting More Fires with Less Water: Phase Zero and Modified Operational Design," *Joint Force Quarterly* 77 (2nd quarter 2015): 101–8 (coauthor); and "You Can't Take the Human Factor Out of Warfare," Opinion-Editorial, *US News and World Report*, 17 October 2014. Colonel Bailey plans to retire later this year and will serve as the next president of Northern New Mexico College.

This article was presented as a paper at the American Political Science Association Teaching and Learning Conference, Washington, DC, January 2015, and at the International Studies Association National Conference, New Orleans, February 2015. It will appear as a chapter in a forthcoming book on cyber strategy tentatively scheduled for publication by the University of Copenhagen Press.

society approaches new technologies. Finally, an analysis of the uncertainties inherent in cyberspace and cyber power will shed light on the major problems associated with designing and articulating strategy in this virtual domain.

The Challenges of Defining—and Teaching—Strategy

The School of Advanced Air and Space Studies is often touted as the premier school of strategy in the United States Department of Defense. The rigorous yearlong graduate program prepares its students for the dizzying array of complex problems they will face as senior military officers. Ironically, if you ask the 14 members of its all-PhD faculty for their definitions of *strategy*, you will most likely hear 14 slightly (and not so slightly) different answers. That is, the school thrives on its reputation for encouraging a broadening of mind-sets, of "creating habits of mind and patterns of inquiry" that serve graduates well in their follow-on assignments.[1] In other words, as Professor Dolman's quotation at the beginning of the article reminds us, no precise answers exist where strategy is concerned. Therefore, a multitude of varying definitions actually enhances the educational experience; that is why we encourage our students to determine their own perceptions of strategy's meaning as a critical part of their educational journey. As for the faculty of the School of Advanced Air and Space Studies, each of us (as you may have guessed) brags about our personal definition as being more useful than our colleagues' offerings. The friendly rivalry, however, is important not only for keeping each other on our toes intellectually but also for enriching the educational experience of our high-powered students. The definition I propose for strategy in this article is useful for the encouragement of strategic thought regarding cyber power, particularly since we must approach such an enterprise with humility, an open mind, and a vigorous intellectual curiosity. Let us define *strategy*, therefore, as *a continual artistic endeavor to optimize competitive advantage through an understanding of one's environment and an adaptation to uncertainty*. Several words in this definition require clarifying explanation.

Continual—Strategy is not a temporally framed endeavor. If we follow Lawrence Freedman's prescription for "thinking about strategy as a story told in the future tense," then the application necessarily continues ad infinitum.[2] In a military planning effort, terms like *end point* or *termination point* allude to some sort of finality to an operational enterprise. These terms are important and helpful to frame a finite effort and to direct the use of limited resources accordingly. However, strategy is a different animal, in that it is an intellectually iterative exercise. That is, although goals and objectives are important to an operational initiative, strategy looks forward to determine how efforts shape the larger picture. For example, a strategist should ask, How does the completion of a particular task, if successful, change the behavior of the other actors in the scenario? Might it change an opponent's decision calculus? Are

there constraints that this effort strengthens or weakens? Does the accomplishment of an objective open new avenues for tangentially related efforts? And so on. Strategy must be respected as a continual process so that as the environment changes, intellectual rigor adjusts to meet new demands.

Artistic—Prussian strategist Carl von Clausewitz famously wrote that "everything in strategy is very simple, but that does not mean that everything is very easy."[3] The complexities inherent in one's environment and the issues involved in adapting to uncertainty call for much more than the application of scientific principles. B. H. Liddell Hart opined, "However far our knowledge of the science of war be extended, it will depend on art for its application."[4] Simply put, for the strategist, neither perfect information nor perfect understanding exists. Therefore, students—and practitioners—of strategy require an innovative mind and a creative approach to problem solving to make the most of an endeavor.

Optimize Competitive Advantage—Strategy usually involves some type of an opponent. In the military, the opponent may be a declared enemy or enemies. In business, it can be one or more competitors for market share or perhaps market forces themselves. In any case, strategy aids in some sort of struggle. In the preface to his seminal book *Strategy: The Logic of War and Peace*, Edward Luttwak states that "as a vision of strategy emerged out of the shadows of words read, problems investigated, and warlike events actually experienced, I found that its content was not the prosaic stuff of platitudes, but instead paradox, irony, and contradiction."[5]

Luttwak uses the term *paradox* because of the presence of an intelligent opponent in strategic ventures. If strategy focuses inward at one's own resources, goals, and constraints, it completely misses the effects of a strategically minded opponent. Such a foe not only affects the dynamics of the environment but also adds to the uncertainty enveloping the engagement.[6]

Environment and Uncertainty—Ultimately, then, the primary aims of the strategist are to think deeply about his or her environment and to prepare for the probability—or eventuality—that things will not go exactly as expected. The environment is complex because of its dynamic nature and because of our imperfect perception of it. Our misunderstandings are a product of incomplete knowledge and of our own biases or improper frameworks. In addition, strategists constantly face the tendency to assume that greater access to information keeps the forces of uncertainty at bay. In fact, the reverse is often true. In the cyber domain in particular, often the challenge lies not in obtaining *enough* information but in determining *which* information to use from a seemingly endless trove. These two areas, environment and uncertainty, will guide the rest of the article to provide a potential framework for teaching cyber strategy.

Teaching strategy ultimately involves encouraging a broadening of perspectives and an understanding of one's own intellectual habits. Herein we find another para-

dox of learning strategy: if students gain a respect for what they *do not* know and, just as important, for what they *cannot* know, only then can they make the most of their strategic journey. Imagination, creativity, intellectual flexibility, and high-minded responsiveness are the tools that guide them as they prepare for both the study of strategy and its future applications.

In the cyber realm, deconstructing the environment and adapting to uncertainty are seemingly impossible tasks. However, if practitioners are expected to integrate cyber power into a larger strategic worldview, then they must explore these two avenues of thought. It is toward these two areas that we now turn.

Understanding the Environment of Cyberspace

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding. . . .

—William Gibson

In the 1984 science fiction book *Neuromancer*, William Gibson popularized the term *cyberspace*, which he had introduced in the short story "Burning Chrome" two years earlier. He probably did not recognize at the time that the term he attached to the virtual environment would become the standard moniker for everything we associate with today's digital world.[7] Thirty years later, the ubiquity of computer networks and their impact on the human experience present a conundrum. Without question, the technology affects almost every aspect of our lives, but its application vis-à-vis power dynamics and grand strategy has yet to be understood. No power dynamic is ever *fully* understood, but our nascent exploration of the cyber field still leaves us analogous to Laika on the rocket after liftoff. In other words, we have gained an immediate awareness that our environment has changed but probably do not understand the extent of those changes, how or why we got there, or where we are headed. To gain an appreciation for the context of cyber power, we must look at the etymology of cyberspace to reveal the biases and frameworks inherent in the terminology we use and explore the difficulties in defining the cyber domain.

The Etymology of Cyberspace

The main argument presented in this section is that the terminology used to describe the elements of cyberspace affects the way we *think* about it. This proposition has had a profound effect on the development (or lack thereof) of a coherent strategy for its use and has made the teaching of cyber strategy incredibly difficult. To develop this line of argumentation, we look at cyber terminology to reveal how its particular se-

mantics shape biases. If those biases create frameworks of understanding, then they may limit the way we think about the technology.

As blogger Mark Forsyth aptly noted, "New things need new words, but they usually end up with old ones."[8] Let us start with the term *cyberspace* itself. Even before Gibson's first popular use of the word, scholars and practitioners published a wide variety of related definitions, each with its own accompanying justifications. In the 1940s, Norbert Wiener, a professor of mathematics at the Massachusetts Institute of Technology, called for increased use of statistical analysis to explain societal phenomena. He interpreted the interaction of systems (biological, mechanical, and societal) as forms of *communication* with feedback mechanisms and, more importantly, predictive qualities. Wiener and his colleagues became the foundational pioneers of a transdisciplinary field of study he termed *cybernetics*. The root *cyber* comes from the Greek *kybernan*, a term meaning *to steer* or *direct*.[9] For Professor Wiener, cybernetics' etymology connoted a direction of order from disorder: "Guided by feedback, organic, mechanical, or social bodies create pockets of order, strong signals in an entropic sea of noise."[10] For many military strategists in the middle of the twentieth century, cybernetics offered hope that through feedback analysis, one might be able to learn enough about war to mitigate uncertainty in conflict. For decades, these strategists challenged Clausewitz's famous dictum that "war is the realm of chance."[11] Thus was born a revolution in military affairs (RMA), suggesting that information, if properly processed, could fundamentally change the essence of warfare. RMA literature embraced the 2,500-year-old philosophy of Chinese thinker Sun Tzu, who wrote, "One who knows the enemy and knows himself will not be endangered in a hundred engagements."[12] Critics of RMA literature claimed that cyberneticists' overconfidence in information as a panacea ignored the omnipresence of uncertainty in combat, leading for example to the "spectacular inefficiency and failure" of strategy in the Vietnam War.[13] Daily statistics on body counts and sorties did nothing to capture either the will of the North Vietnamese people or the eroding support from the American public.

How do semantics, then, ultimately affect our conceptualization of cyber strategy? Put simply, use of the root *cyber* in *cyberspace* and *cyber power* has always implied a mechanism for creating at least some order out of chaos. As experience shows, however, uncertainty is always present in warfare; thus, even though we use these terms, we must be aware of their limitations and remain mindful to keep them in the proper perspective. Cyber power, at its core, is fueled by information. However, even robust access to information will fall well short of clearing Clausewitz's fog of war. Students of strategy must respect this eventuality and prepare themselves for the intellectual challenges that it entails.

Let us consider the connotations of the second half of the term *cyberspace*. The word alludes to, or at least conjures up, an image of a physical *space*. Thus, the term

itself is nothing more than a metaphor. However, if strategists think of cyberspace solely in physical terms, they run the risk of closing their minds to the potential of the technology and to missing its unique nonphysical characteristics. The mention of cyberspace in conjunction with the physical domains adds to this tendency. The United States Air Force, for example, clarified its mission statement in 2005, rallying its Airmen "to fly, fight, and win . . . in air, space, and cyberspace."[14] When cyberspace joins air and space as domains of military operations, it is natural for the mind to apply the analogy to an imagined geospatial entity and put it on equal footing with the physical domains.[15]

Even if we try to imagine cyberspace as analogous to a three-dimensional space, its boundaries would be impossible to identify. In reality, the only physical space involved in cyberspace is the architecture providing the infrastructure for its employment. Rather, cyberspace is a metaphor helping us to visualize a domain in which information "travels" via networked computer systems. One of the most complete definitions of cyberspace comes from Daniel Kuehl, who described it as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange information via networked information systems and physical infrastructures."[16] Martin Libicki was one of the first to identify three distinct layers of cyberspace: the physical (routers, wires, switches, etc.), the syntactic (the information systems themselves, along with the protocols for formatting and distributing information), and the semantic (the nexus between the transferred information and the human reception and understanding of that information).[17] Almost every early work on cyberspace emphasized that it is the only man-made military domain. The basic concept entails that, as opposed to other domains of military power (land, sea, air, and space), human-made objects must be present in order for cyberspace to exist. Although humankind creates objects to traverse and optimize the use of the physical domains, only in cyberspace is our intervention required to *create* the domain. However, even if we recognize this unique feature, what are its associated strategic implications? Ultimately, they are either nonexistent or irrelevant. The only possible connection exists either in a scenario in which someone or something destroys the global Internet architecture or through a cataclysmic event like a global electromagnetic pulse.

Because cyberspace has no physical boundaries, no simple rules exist for partitioning either responsibilities or control. Thus, military strategists have had to look beyond traditional assumptions about the application of military force in a physical setting. Consider, for example, the factor of distance. In a physical confrontation, the distance to an enemy target is critically important to a land or sea engagement and relatively important to an air attack but almost negligible in cyberspace. A skilled hacker with advance knowledge of an enemy's computer vulnerabilities can affect both his networks and perhaps his physical assets. No matter where the target is lo-

cated, the hacker can engage it from practically anywhere on the planet in literally fractions of a second. Even extraterrestrial targets like satellites may be vulnerable.

The meaning of words can evolve and even transform over time. Consider the meaning of *computer*. The term has been used in the English language since the 1600s, but it has completely transformed to mean something fundamentally different. Before the twentieth century, the word denoted a human being who processed numbers by hand. However, with the advent of the microprocessor and the growing popularity of home computing in the 1970s and 1980s, society began to use *computer* to describe the mechanism more than the person who performed the function: "By that time, computers—like science-fiction cyborgs—had completed their transformation from human to machine."[18]

Why is terminology important to the student of strategy? Let us consider the dual meaning of words and phrases. According to linguistics professor Kate Kearns, a sentence "is composed of *lexical meaning*, which is the meaning of the individual words, and *structural meaning*, which is the meaning of the way the words are combined" (emphasis in original).[19] Even the lexical meaning can frame the way we approach a topic both intellectually and emotionally. Political lobbyists are highly skilled in this arena and use language to shape national discussion. Consider the abortion debate in the United States. Lobbyists (and politicians) opposed to *late term* abortions—those that take place in the second or third trimester of a pregnancy—were able to rename them *partial birth* abortions in the public sphere. The latter term is much more evocative and has the tendency to call up images of terminating a *living* human being. The language itself can frame how we might *think* or *feel* about a subject, just based on the lexical meaning of the words used to describe it.

It is helpful to extrapolate this understanding to the terms we use in cyberspace. Because the lexical meanings of the words we use to describe elements in cyberspace are rooted in understandings and perceptions of physical objects and concepts, their structural meaning becomes bound in archaic frameworks:

> A long-standing and influential view about language is that the meaningfulness of language amounts to its "aboutness." Words and expressions symbolize and describe—and are thus about—things and phenomena in the world around us, and this is why we can use language to convey information about reality. Accordingly, the meaningfulness of language consists of connections between words and expressions and parts of reality.[20]

How can budding strategists cope with this dilemma? Moreover, how can we teach cyber strategy in a way that counters this tendency? Ideally, we would come up with new terms for cyberspace and its elements that evoked a more expanded intellectual framework. Unfortunately, this effort would be futile. The words describing cyberspace have been around for decades, so the likelihood of changing the language at this point is remote. The only recourse is to understand the limitation of the terms and to fight to overcome the biases they subconsciously create. In any case, the education of

cyber strategy must start with an understanding of the cyber environment—and a large part of that environment is founded in the language we use to describe it.

How Do We Experience New Technology? Polarization and Analogies

An appreciation for the biases and frameworks provided by the language of cyberspace unlocks part of our understanding of its intellectual environment but does not offer a comprehensive picture. A complementary approach involves applying a sociological lens. In other words, we may gain a more thorough understanding of the cyber environment by exploring how society adapts to it over time. Two main patterns emerge when we apply this analysis: a polarization in the literature and a tendency to use analogies to past technological advances.

To explore the phenomenon of polarization in the literature, we must first ask why society tends to think about extreme positions when it experiences new concepts. A modified scenario from Alexander Wendt serves us well here.[21] Imagine turning on your television to live, late-breaking news that an alien spacecraft has landed in the middle of Central Park in New York City. Without any other information, what would your first thoughts be? What does the image of the spacecraft convey to you? To put it in popular movie terms, you may see this in one of two extreme camps. Perhaps you imagine the friendly, benevolent, kind-hearted visitors from *E. T. the Extra-Terrestrial* or the closing scene of *Close Encounters of the Third Kind*. Or maybe you picture the dark, ominous, resource-starved aggressors from *War of the Worlds* or *Independence Day*. Few people actually think of something in between. Put simply, most of us tend to explore the new or unknown with either feelings of trepidation or the hopeful promise of a panacea. James Gleick put it best: "Every new medium transforms the nature of human thought. In the long run, history is the story of information becoming aware of itself."[22] As human thought about cyberspace and cyber power evolves, the salvationists and alarmists are falling into their respective camps. A review of popular literature on cyber power reveals this phenomenon.

When Tim Berners-Lee created the World Wide Web, he was conscious of the social power it could enable. His design eschewed a proprietary approach. Instead, the Web "invited—*required*—its inhabitants to help build it. It was a World Wide effort" (emphasis in original).[23] Designers like Berners-Lee, however, just as the inventors of the Advanced Research Projects Agency Network before him, were far more conscious of the revolutionary potential of a borderless information source than any propensity for malfeasance: "The development of social machines requires the development of mechanisms that allow users of social machines to more freely share data without having to worry about it being used in inappropriate ways."[24] Thus, the floodgates opened, and access to both the benevolent and the nefarious became instantly possible.

To many people, cyberspace inspires hope—of information as a panacea to cure our social ills. In terms of warfare, cyber power might encourage an overall decrease in destructive violent action, a "computer-enabled assault on violence itself."[25] It also might spur organically (and peacefully) generated social and political change. Evgeny Morozov termed this concept *cyber utopianism*, a "naïve belief in the emancipatory nature of online communication that rests on a stubborn refusal to acknowledge its downside."[26] How many of us thought that the Arab Spring would continue to thrive based on people's growing access to good ideas? The ubiquity of information is only part of the picture. How audiences process messages and what they do in response are equally important. Morozov's sobering message is that while information can be a spark for positive change, regimes might also use it to continue their repressive control.

If we use sheer numbers as an arbiter, the alarmist side of cyber literature seems to be winning the debate over the cyber salvationists. Even a cursory review of popular literature on cyber power reveals a wide assortment of warnings about threats imposed by the technology and our related vulnerabilities. Richard Clarke, who served four separate presidential administrations as a counterterrorism expert, is very clear about the dangers of cyber power: "Cyber war is real. What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons. . . . What the United States and other nations are capable of doing in a cyber war could devastate a modern nation."[27] Consider the now-famous 2007 cyber attacks on Estonia. When the Estonian government pressed to remove the *Monument to the Liberators of Tallinn* (now informally nicknamed the Bronze Statue) from a prominent spot in its capital city, the Russian people (including Estonia's ethnic Russian population) were infuriated. To them, the statue was a symbol of sacrifice and honor. However, to many other Estonians, it was a reminder of oppressive Soviet occupation. Two years after joining the North Atlantic Treaty Organization (NATO), several members in the Estonian government called for removal of the monument.[28] On 15 February 2007, the Parliament passed a bill calling for a ban on *any* structure memorializing the Soviet occupation, but President Toomas Hendrik Ilves, perhaps in an attempt to find a peaceful solution to the tension, vetoed the measure.[29] Months later, the local government decided to move the Bronze Statue from its central location to a spot outside the city. The move sparked an outcry from Tallinn's ethnic Russians. On 27 April, the first cyber attacks targeted several important Estonian websites. Among them were the Estonian presidency, Parliament, most government ministries, political parties, three of the country's six big news organizations, two of the biggest banks, and major communications companies.[30] Many pointed to the Russian government as the most likely perpetrator of the attacks. In any case, the strikes constituted one of the first well-known political uses of cyber power in what appeared to be an interstate conflict. Even though no one

died as a direct result of the attacks, the social, political, and financial effects on Estonia were devastating, prompting the country to petition NATO for a military response.

States are not the only potential victims of cyber power's effects. One powerful example is the December 2014 cyber attack—allegedly by the North Koreans—on Sony Pictures in response to the theatrical release of *The Interview*, a comedy based on a plot to assassinate President Kim Jong-un. The attacks were so influential that Sony postponed the film's release. President Obama criticized Sony's capitulation: "If we set a precedent in which a dictator in another country can disrupt through cyber, a company's distribution chain or its products, and as a consequence we start censoring ourselves, that's a problem."[31] Although North Korea denied the attack, the government did threaten to engage in cyber attacks in the future. American pundits and politicians disagreed about how to characterize the strikes. Some, including President Obama, called it a form of cyber vandalism, but others characterized it as something far more sinister. In a Sunday morning talk show interview, Senator John McCain asserted that "it's more than vandalism. It's a new form of warfare that we're involved in and we need to react and we need to react vigorously."[32]

This recent example shows that even within the alarmist camp, there are disagreements about how to characterize the extent of the dangers. As with any exposure to a new technology or new experience, we tend to use analogies to aid in comprehension. Put another way, our framing of new ideas and new concepts is critical to our nascent understanding of them. Philip Ball put it best: "Science is driven by ideas, not numbers or measurements—and ideas only arise by people thinking about causative mechanisms and using them to frame good questions."[33] Yet, it is often our natural instinct to draw analogies to ideas or concepts with which we are familiar, similar to the way we use common language to describe them, even at the cost of creating problematic biases. In the cyber arena, a multitude of initial thinkers and writers explored society's early lessons with the airplane and airpower and used them as a blueprint (and in some cases a prediction tool) for our experiential journey through cyberspace and cyber power: "Airpower is similar to cyberpower because it is a domain dominated by technological advancements."[34] In many ways, the analogy can be helpful. Airpower, for example, started as a tool for reconnaissance and battlefield awareness but progressed into a fundamentally unique application of military force.[35] In other words, we could no longer think of airpower in the same way we thought of land power or sea power. Its three-dimensional nature and its ability to bypass or circumvent traditional battlefield considerations meant that airpower required a new way of *thinking* about warfare. The Center for Cyberspace Research at the Air Force Institute of Technology put it this way: "Cyberspace is a domain of military operations, and we need to begin growing a cyber culture. The challenge is that there is little or no published doctrine. . . . Nonetheless, we have to start somewhere. To a

great extent, we are in the same situation as [Billy] Mitchell and [Giulio] Douhet when discussing [the] application of airpower."[36] In this sense, our early experiences with airpower are instructive for our early steps in cyberspace.

The application of cyber power is in many ways, however, fundamentally different from that of any military power preceding it. Therefore, we need to spend time thinking about these unique characteristics rather than simply applying constructs from the physical domains. Libicki was one of the first to recognize that a different mind-set would be necessary to thrive in a digital world:

> Over time, radical changes in technology are understood to involve radical changes in the organization of work and society as well. Initially the electric motor did not help productivity compared to the belt-driven machines it replaced; in time, vertical factories designed to minimize the amount of belting gave way to horizontal factories designed to help the flow of men and material. Similarly, computers cannot help most firms very much until they reengineer their work processes to accord with the silicon logic. Conflict both conventional and unconventional will perforce follow the same path—accommodating change first by incorporation, and next by reinvention.[37]

This is the irony of using analogies in cyberspace. The only thing helpful about applying an analogy to cyber power is that it warns us to avoid common frameworks—like analogies.

Budding strategists exposed to cyber power must come to grips with how society experiences new technologies, both to wade through the polarization of initial thinkers and to use—but be wary of—analogies to past technologies.

Adapting to the Uncertainty Inherent in Cyberspace

The telescope . . . was powerful enough to make out those details that would ordinarily be beyond the commander's view, but not so powerful as to produce the administrative equivalent of Heisenberg's Uncertainty Law in physics, which says that subatomic particles can never be measured because the very attempt to measure them will cause them to change.

—Martin van Creveld

In *Command in War*, Martin van Creveld warns us that no matter how hard we try to create order from chaos, uncertainty is a timeless characteristic of war.[38] Cyberspace is our latest telescope. It offers us access to information that previously seemed unimaginable. Yet, even in an era of Big Data, uncertainty thrives. How should students of cyber strategy contend with this dilemma? As the definition of strategy at the beginning of this article reminds us, adaptation is the key. Successful adaptation depends on two endeavors: (1) understanding the dialectic nature of strategy and (2) gaining an appreciation of what—and how much—is still unknown.

The Strategy of Others

Boxing champion Mike Tyson is famously quoted as saying that "everyone has a plan until they get punched in the mouth."[39] If strategy is about optimizing competitive advantage, then students of strategy must acknowledge that a thinking, strategic opponent has a vote in determining the outcome of any engagement. This fact alone creates uncertainty for the strategist. Therefore, it is incumbent on students of strategy—particularly cyber strategy—to consider the most prominent actors in the domain today. As Timothy Thomas put it, "Cyber strategists will be wise to become familiar with the methods, definitions, and concepts of the most capable cyber nation-states."[40]

The United States and Western Europe got a head start in the development of cyberspace tools and technologies. One need only look at *Forbes* magazine's list of the three most valuable worldwide brands today—Apple, Microsoft, and Google—to see where innovation generated huge profits.[41] As Joseph Nye pointed out, in many ways, that head start had a huge impact on the geopolitical distribution of power:

> In the twentieth century, science and technology added dramatic new dimensions to power resources. . . . Subsequently, the leading role of the United States in the information revolution near the end of the century allowed it to create a revolution in military affairs. The ability to use information technology to create precision weapons, real-time intelligence, broad surveillance of regional battlefields, and improved command and control allowed the United States to surge ahead as the world's only military superpower.[42]

However, this gap is arguably shrinking. China, Russia, and other state actors are spending considerable percentages of their military budgets on the development of offensive and defensive cyber technologies. According to a recent *TechRepublic* report, "Peter W. Singer, director of the Center for 21st Century Security and Intelligence at the Brookings Institution, said 100 nations are building cyber military commands. . . . There are about 20 that are serious players, and a smaller number could carry out a whole cyberwar campaign."[43] The biases and frameworks that cyberspace's etymology creates in English can become even more problematic on the international stage:

> Yet even before addressing divergences in attitude and threat perception, there is the more basic problem of absence of a common terminology between the major players in cyberspace. The definitions of such terms as cyber conflict, cyber war, cyber attack, cyber weapon, etc. used by the UK, USA, Russia and China do not coincide—even where official or generally recognised definitions exist in each respective language. Furthermore, direct translations of specific terms from Russian and Chinese which resemble English-language terms, and vice versa, can complicate matters further by giving the misleading impression of mutual understanding, while in fact referring to completely different concepts.[44]

State powers are not the only actors joining the fight. Although attribution is still a challenge in cyberspace—as discussed below—several high-visibility cyber attacks

have been linked to nonstate actors.[45] As opposed to dominance in the physical domains, which may require either massive personnel numbers or sophisticated high-tech weaponry, cyber power's cost of entry is relatively low. Sophisticated knowledge is certainly a requirement, but the design of the Internet's architecture makes its users vulnerable to malfeasance from anywhere. Thus, students of strategy must ask the question, In terms of military power, do cyber capabilities serve as a leveling function for what used to be a hierarchical playing field? If so, how do militaries in an era of fiscal constraints prepare for the myriad of potential adversaries?

In addition, the strategist must attempt to comprehend—and appreciate—the way potential adversaries *think* about the use of power. For example, "China has a very long history of strategic thought. One need only access their military encyclopedia to get a feeling for the hundred or so Chinese terms that are defined and include the word *strategic*."[46] What does this mean for the Chinese use of cyber power, not just today but within the context of a much longer game plan? Moreover, perhaps more importantly, what security concerns would these decisions affect? The cyber strategist must use a combination of thoughtful research and freethinking imagination to tackle problematic questions like these in an effort to adapt to uncertainty caused by the presence of other actors in cyberspace.

The Cyber "Unknown"

Uncertainty in cyberspace is not just dependent on the presence of intelligent foes. In fact, cyber power's own characteristics bring forth a level of uncertainty with which strategists must contend. Two classic examples are (1) attribution/forensics and (2) classification/cooperation. Ironically, one is a product of technological progress while the other is caused by our own national policies.

In 2007 it was easy to blame Russia for the attacks on Estonia. Their timing, the Russian government's passionate outcries about the removal of the Bronze Statue, the temper of ethnic Russians in the Baltics, and the capabilities exhibited by the Russian government on previous occasions all pointed to Moscow as the prime suspect. The same can be said for the attacks on Sony Entertainment in 2014. Their timing, the pending release of *The Interview*, and public statements by the North Korean government (even considering its denials) still pointed to Pyongyang. However, all of those factors in a court of law would amount to nothing more than circumstantial evidence. It may be a far greater challenge to attribute responsibility for an act in cyberspace than to determine the source of a nuclear catastrophe. Organizations like the Defense Threat Reduction Agency now have highly sophisticated nuclear forensics programs that can identify the source of harmful material from radioactive debris, even potentially pinpointing the area of origin.[47] Phantom Internet protocol addresses and other techniques for operations in cyberspace still make attribution a concern for cyber practitioners and a more significant one for geopolitics. How can

leaders make national security decisions and endorse potential military-response actions without a clear picture of a perpetrator? For example, when Estonia petitioned NATO for a response to the attacks in 2007, NATO nations refused to act, not simply because of the confusion about whether the cyber attacks constituted acts of war but because they could not be *certain* that the attacks came from Russia (much less the Russian *government*). In essence, cyber operations have yet to reach the level of forensic sophistication that occurs in the physical domains. Consequently, uncertainty surrounding cyber acts can make even seemingly straightforward response decisions incredibly complex.

In time, cyber forensics may reach a level of sophistication comparable to that of the physical domains. Scientific research and development will pave the way. To a meeting of business executives on national security on 11 October 2012, then–secretary of defense Leon Panetta observed that "over the last two years, DoD [the Department of Defense] has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America."[48] At the time, many people questioned the validity of the statement and perceived the secretary's speech as more of a deterrent threat than an actual boast of improving capabilities. Although attribution in cyberspace is a difficult problem, improvements in cyber forensics are nevertheless developing.[49] Techniques to mask identity in cyberspace are evolving as well, so the attribution issue, at least in the near term, presents a problematic uncertainty to the cyber strategist.

Uncertainty caused by classification difficulties, however, is a human-made conundrum and the source of an interesting paradox between security and cooperation. The United States Presidential Website illustrates a prime example. On the one hand, the White House is very clear about the importance of protecting its classified information: "It's the classified military and intelligence networks that keep us safe." On the other hand, the same website trumpets the importance of international collaboration and cooperation: "Because cyberspace crosses every international boundary, we must engage with our international partners. We will work to create incentives for, and build consensus around, an international environment where states recognize the value of an open, interoperable, secure, and reliable cyberspace."[50] Anyone who has worked in a military cyber power capacity will tell you that the security classification procedures are incredibly robust—perhaps because of the perceived concept of *one-and-done* cyber weapons. In other words, if a cyber weapon exploits an enemy's particular network vulnerability and the enemy detects the act, he or she can do two things almost immediately: (1) patch the vulnerability to prevent similar weapons from having the same access and permitting the same damage and (2) use that same weapon in an offensive capacity against any other entity with the same vulnerability.

Thus, the concept of one-and-done weapons leads to two major behaviors. First, would-be users of the weapon may resist using it until absolutely necessary since they do not want to expose knowledge of the weaponry. This choice may in some ways reduce the likelihood of offensive attacks since actors may be incentivized to hold on to the potential use as long as possible—or at least until they feel they *really* need to use it. Second—and closely related—cyber actors want to keep a close hold on the capability to prevent that same awareness, so their tendency is to classify the capabilities (and the weapons themselves) at the highest possible level.

This situation presents a unique challenge to international cooperation efforts. Concern about the difficulty of maintaining classified information of any kind encourages actors to play their cyber cards incredibly close to their chests, leading to intensive (and sometimes exhaustive) security classifications. This behavior, however, runs completely counter to practices that facilitate international cooperation. Some examples of successful cooperation do exist—the NATO Cooperative Cyber Defence Centre of Excellence in Estonia stands out as a potential institutional blueprint. The center offers avenues for international information sharing and hosts international exercises and best-practice simulations. Such an agency, though, is only as effective as the information that member states choose to share with one another. In many cases, individual governments still classify their most advanced techniques at the highest national levels, prohibiting international sharing—even with their closest partner nations.

The US government's self-inspection after the attacks of 11 September 2001 offers an interesting framework. A report to the US Senate 10 years after the attacks pointed out that

> the attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes and secretive pockets of the nation's most valuable information. It may have worked in the Cold War, but it was not adequate to keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way.[51]

In a similar way, the asymmetric threats posed by cyber power today necessitate consideration of removing national stovepipes and traditional classification tendencies. This is not an argument for removing all national classifications from cyber tools and techniques, but strategists must recognize that cooperation without meaningful information sharing is akin to a paper tiger and ultimately may leave each member state more vulnerable.

Uncertainty is omnipresent in warfare. Cyberspace and its related technologies may have offered initial promise that robust access to information could create order from the chaos, but the opposite is closer to reality. Our present access to cyberspace in some ways has complicated the picture. The ubiquity of information, ironically,

increases uncertainty by forcing the strategist to concentrate much more on *prioritizing* available information rather than *gaining access* to it, making adaptation and flexibility more important than ever—particularly to the strategist.

Cyber Strategy Education in Action: A Few Examples

Over the last 20 years—and the last 10 in particular—several states have instituted cyber education programs to encourage strategic thinking about cyberspace and cyber power. A cursory review illustrates that many of these programs tend to focus more on tactical and operational skill training rather than on strategic thinking.

The United Kingdom offers an interesting example. In 2011 that country published its national cyber security strategy, highlighting four main strategy objectives:

- to make the UK one of the most secure places in the world to do business in cyberspace;
- to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace;
- to help shape an open, vibrant and stable cyberspace that supports open societies;
- to build the UK's cyber security knowledge, skills and capability[52]

Based on the definition of strategy provided previously in this article, one can argue that the United Kingdom values strategic cyber thinking, but its national goals seem overwhelmingly tactical in nature. Even the fourth objective, although referring to increasing knowledge, seems more slanted toward tactical training than strategic education. In 2013 a governmental review of the strategy "identified a shortage of cyber security skills as a key challenge. . . . If the UK is to be equipped to respond to cyber threats, and the cyber security sector is to grow, we need to strengthen the pipeline of cyber talent and help prepare students for entry-level security career opportunities."[53] This stance has led to the Higher Education Academy and other educational programs instituting aggressive training programs in cyber skills. Such training is certainly valuable and indeed necessary for national defense given the impact of the cyber domain, but deeper-level strategic education must also be included.

The US professional military education (PME) program is designed to arc across an individual's entire military career. The Air Force's PME goal, for example, is to produce "professionals educated in the profession of arms who possess an intuitive approach to joint war fighting built upon individual Service competencies. The aim is to produce graduates prepared to operate at appropriate levels of war in a joint environment and capable of generating quality tactical, operational, and strategic thought from a joint perspective."[54] At different key nodes within a service member's career, military education programs foster both a refresher about the unique responsibilities

of being a member of the profession of arms as well as an update of doctrine, tactics, and strategies involved with the employment of military power. At the Air Force Institute of Technology (AFIT), specific courses target both practitioners and supervisors of cyber power. In April 2015, AFIT invited the author to upgrade the strategy block of the curriculum for the Cyber 300 (upper-level supervisor) course. The course directors identified that their strategy block had been much more about national *policy* than national *strategy*. Thus, we have worked on broadening the lessons (and related exercises) to stimulate strategic thinking rather than simply review associated policies.[55]

NATO's Cooperative Cyber Defence Centre of Excellence is taking big steps to encourage strategic thought. Its website includes links to every member state's national strategies regarding cyberspace as well as any relevant legal documents.[56] The center may be best known, however, for a book it published in 2013. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is the first publication of its kind to attempt to codify international norms of cyber power.[57] Although not legally binding (NATO did not even formally review it), the manual at least establishes a framework by determining the extent to which cyber power fits within already-established legal standards for the physical domains. The *Tallinn Manual* was groundbreaking in that it was the first major attempt to codify international norms for cyber power. The center hosts tactical exercises that are gaining in popularity with member states each year and holds education programs in several areas, but its largest strategic education initiatives focus primarily on international legal issues.[58]

As demonstrated in this article, strategic thinking—particularly regarding cyberspace—requires a shift in mind-set. As Timothy Thomas puts it, "A holistic approach is required to develop a cyber strategist due to the global nature and blinding speed of digits."[59] The recent explosion of cyber training programs is a positive trend, showing that states are taking the effects of cyber technology seriously. However, *training* must be accompanied by *education*. If we are to cultivate future cyber strategists, then an introduction to cyber tools is just the beginning. A greater understanding of the dynamic cyber environment and a respect for the unexpected will be necessary elements of a more complete cyber strategy education.

Conclusion: The Journey Continues

As this article illustrates, thinking strategically about cyber power is no easy task. Teaching and learning strategy are complicated enough, particularly considering the varied definitions—and perceptions—of strategy itself. If strategy is ultimately dependent on understanding one's environment and adapting to uncertainty, then we clearly still have much work to do in the cyber domain. Understanding the environment of cyberspace is often hampered by biases and frameworks, many of which are

based on etymological foundations. In addition, contextual confusion often leads to a polarization in early literature and a tendency to use anachronistic analogies to aid in comprehension—both of which present challenges to strategic thinking. Uncertainty in cyberspace is a product of the dialectical nature of strategy and the limits to useful information—both organic and synthetic—inherent in cyberspace and in our application of cyber power. This situation makes adaptation critical to the cyber strategist.

Military practitioners face a daunting task. They are being asked to incorporate cyberspace and cyber power into an already complex suite of military applications. However, our nascent experience with the technology shows that we have yet to grasp fully the domain's intricacies. Students of cyber strategy must acknowledge and respect the enormity of the unknown. Designing and articulating a coherent strategy for cyber power will likely take several more years and require more intellectual rigor. In the interim, practitioners who desire to think strategically about cyber power must endeavor to understand the complex environment of cyberspace and be flexible enough to adapt to its ever-present uncertainties. Ultimately, cyberspace and cyber power are important subjects with which students of strategy must become familiar; reciprocally, however, this technology offers an intellectual harvest that when approached properly can assist in the development and cultivation of deeper strategic thought.

Notes

1. Special thanks to Dr. Thomas Hughes for this insightful phrase.

2. Lawrence Freedman, *Strategy: A History* (New York: Oxford University Press, 2013), xiv.

3. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 178.

4. B. H. Liddell Hart, *Strategy* (London: Faber and Faber, 1954), 323.

5. Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press of Harvard University Press, 1987), xii.

6. See also David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 229–30. He posits that five factors shape the nature of war, one of which is *paradoxical logic*, based on the presence of an intelligent foe.

7. William Gibson, *Neuromancer* (Princeton, NJ: John Wiley, 1984), 51.

8. Mark Forsyth, *The Etymologicon: A Circular Stroll through the Hidden Connections of the English Language* (New York: Berkley Books, 2011), 103.

9. *Dictionary of Etymology: The Origin of American English Words*, ed. Robert K. Barnhart (New York: HarperCollins, 1995), 181.

10. Adam Brate, *Technomanifestos: Visions from the Information Revolutionaries* (New York: Texere, 2002), 18.

11. Clausewitz, *On War*, 101.

12. Sun Tzu, *The Art of War*, trans. Ralph D. Sawyer (New York: Barnes and Noble, 1994), 179.

13. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 160.

14. The US Air Force publishes its mission statement on its public website, along with the organization's values, core competencies, and history. "Mission," US Air Force, accessed 9 May 2016, http://www.airforce.com/learn-about/our-mission/.

15. The concepts in this paragraph and the following two originated in an essay I wrote entitled "Four Dimensions to the Digital Debate," recently published as a chapter in Richard J. Bailey Jr., James W. Forsyth Jr., and Mark O. Yeisley, eds., *Strategy: Context and Adaptation from Archidamus to Airpower* (Annapolis: Naval Institute Press, 2016), 186–207.

16. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009), 26.

17. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 8–9.

18. Justin Cord Hayes, *The Unexpected Evolution of Language* (Avon, MA: Adams Media, 2012), 67.

19. Kate Kearns, *Semantics*, 2nd ed. (London: Palgrave Macmillan, 2011), 3.

20. Ibid., 6.

21. Professor Wendt used the scenario to argue that social threats are not natural but socially constructed phenomena. See Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (Spring 1992): 405.

22. James Gleick, *The Information: A History, a Theory, a Flood* (New York: Pantheon Books, 2011), 12.

23. Brate, *Technomanifestos*, 231.

24. Jim Hendler and Tim Berners-Lee, "From the Semantic Web to Social Machines: A Research Challenge for AI on the World Wide Web," *Artificial Intelligence* 174, no. 2 (February 2010): 156–61.

25. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), xiv. Author's note: In a telephone interview with the author in the summer of 2013, Professor Rid articulated that despite his book title, his position was not necessarily an optimistic one. He simply argues that cyber power offers a less violent alternative to the conflict mechanisms of sabotage, espionage, and subversion, and that this option may lessen the propensity for overall violence.

26. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011), xiii.

27. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 30–31.

28. The most vocal element of the Estonian government at the time was the Pro Patria and Res Public Union (IRL). For more information, please see Joel Alas, "Bill Paves Way for Statue Removal," *Baltic Times*, 15 November 2006, http://www.baltictimes.com/news/articles/16812/.

29. For the full news story, please see "Law to Remove Memorial Vetoed by Estonia's Leader," *South Bend Tribune*, 23 February 2007, http://articles.southbendtribune.com/2007-02-23/news/26801820_1_bronze-soldier-president-toomas-hendrik-ilves-soviet-war-memorial.

30. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, 16 May 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

31. Jethro Mullen, "North Korea and the Sony Hack: The War of Words Escalates," *CNN*, 22 December 2014, http://www.cnn.com/2014/12/22/world/asia/north-korea-us-sony-hack-who-says-what/index.html.

32. Ibid.

33. Philip Ball, "Machine Envy," *Aeon Magazine*, 7 January 2014, http://aeon.co/magazine/science/science-is-becoming-a-cult-of-hi-tech-instruments/.

34. Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, MA: Elsevier-Syngress, 2011), 27.

35. For an analysis of the different stages of US Air Force thinking—and branding—see Paula G. Thornhill, "*Over Not Through*": The Search for a Strong, Unified Culture for America's Airmen (Santa Monica,

CA: RAND Corporation, 2012), http://www.rand.org/content/dam/rand/pubs/occasional_papers/2012/RAND_OP386.pdf.

36. Dr. Robert F. Mills, Dr. Richard A. Raines, and Maj Paul D. Williams, *Developing Cyberspace Competencies for Air Force Professional Military Education* (Wright-Patterson AFB, OH: Center for Cyberspace Research, Air Force Institute of Technology, 2007), 1.

37. Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, McNair Paper 28 (Washington, DC: Institute for National Strategic Studies, National Defense University, 1994), 3.

38. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 142.

39. Mike Berardino, "Mike Tyson Explains One of His Most Famous Quotes," *Sun Sentinel*, 9 November 2012, http://articles.sun-sentinel.com/2012-11-09/sports/sfl-mike-tyson-explains-one-of-his-most-famous-quotes-20121109_1_mike-tyson-undisputed-truth-famous-quotes.

40. Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic," *Defence Studies* 14, no. 4 (28 August 2014): 382.

41. Kurt Badenhausen, "Apple, Microsoft, and Google Are World's Most Valuable Brands," *Forbes Magazine*, 5 November 2014, http://www.forbes.com/sites/kurtbadenhausen/2014/11/05/apple-microsoft-and-google-are-worlds-most-valuable-brands/.

42. Joseph S. Nye Jr., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), 18.

43. Steve Ranger, "Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar," *TechRepublic*, 24 April 2014, http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/.

44. Keir Giles and William Hagestad III, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *Proceedings: 5th International Conference on Cyber Conflict*, ed. K. Podins, J. Stinissen, and M. Maybaum (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 414–15.

45. For an in-depth look at the effects of nonstate actors in cyberspace, see Capt Johan Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4, no. 1 (2013), http://www.ida.liu.se/~g-johsi/docs/JMS_4-1_Sigholm_Non-State_Actors_in_CyberOps.pdf.

46. Thomas, "Creating Cyber Strategists," 381.

47. See "Nuclear Technologies," Defense Threat Reduction Agency and USSTRATCOM Center for Combating WMD and Standing Joint Force Headquarters-Elimination, accessed 10 May 2009, http://www.dtra.mil/Research/NuclearTechnologiesDepartment.aspx.

48. Secretary of Defense Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," US Department of Defense, 11 October 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

49. James Steinberg and Michael E. O'Hanlon, *Strategic Reassurance and Resolve: U.S.–China Relations in the Twenty-First Century* (Princeton, NJ: Princeton University Press, 2014), 176.

50. "Foreign Policy: Cybersecurity," White House, President Barack Obama, accessed 9 May 2016, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

51. Senate, *Statement of Zoe Baird Budinger and Jeffrey H. Smith, Senate Committee on Homeland Security and Governmental Affairs: Ten Years after 9/11; a Status Report on Information Sharing*, 112th Cong., 1st sess., 12 October 2011, https://www.fas.org/irp/congress/2011_hr/101211smith.pdf.

52. Cabinet Office, *The UK Cyber Security Strategy: Report on Progress and Forward Plans*, December 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

53. "Learning and Teaching in Cyber Security," Higher Education Academy, accessed 9 May 2016, https://www.heacademy.ac.uk/funding-call/learning-and-teaching-cyber-security.

54. Mills, Raines, and Williams, *Developing Cyberspace Competencies*, 3.

55. For a full description of AFIT's Cyber 200 and 300 courses, see "Cyberspace 200/300 Courses," AFIT Graduate School of Engineering and Management, 8 December 2015, http://www.afit.edu/CCR /programs.cfm?p=60&a=pd&page=162&tabname=Tab1A.

56. See "Cyber Security Strategy Documents," NATO Cooperative Cyber Defence Centre of Excellence, 3 August 2015, https://ccdcoe.org/strategies-policies.html.

57. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013).

58. For a list of available training and educational offerings at the center, see "Cyber Security Training events," NATO Cooperative Cyber Defence Centre of Excellence, accessed 9 May 2016, https://ccdcoe.org /events.html.

59. Thomas, "Creating Cyber Strategists," 390.

Uncertainty and Deterrence

Yakov Ben-Haim, PhD[*]

S trategic decisions of war or peace are surrounded by uncertainty arising from geopolitics, the adversary's intentions, third parties, doctrinal innovations, new technologies, and more. Due to surprising future developments, what looks like the better option may turn out much worse than a putatively worse choice. When one option looks better but is far more uncertain than another alternative, the planner may select the latter even though it is ostensibly less attractive. In making one's choices or when anticipating those of an adversary, one must consider both the estimated outcomes of the selections and the uncertainties of these estimates. Preference ranking of options may be reversed from their evident order due to uncertainty. This article develops an analytic framework for studying this reversal of preference in evaluating deterrence, without any probabilistic assumptions. It does not propose a theory of deterrence but a method for analyzing and choosing between options. The analysis is based on two concepts: the innovation dilemma and robustly satisfying critical requirements.

This study responds to two weaknesses in theories of deterrence. First, the treatment of uncertainty is inadequate. Deductive mathematical approaches from rational-choice theory often treat uncertainty as a probability that, even when labeled as subjective, is too structured to capture the richness of decision makers' ignorance. Inductive or case-based theories are vulnerable to Solomon's error of presuming that the rich diversity of the past characterizes the rich variability of the future.[1] In fact, the future is far more surprising and inventive than the past. Second, rational-choice theories of deterrence presume that the decision maker's goal is—and should be—to achieve the substantively best possible outcome. Doing so is not prescriptively feasible

---

under severe uncertainty. Rather, decision makers should prioritize their options according to robustness against surprise in attempting to realize critical or essential (but not necessarily optimal) outcomes.

A decision maker faces an *innovation dilemma* when choosing between a new and innovative option and the current state of the art.[2] The innovation dilemma is a paradigm, a metaphor—originating in the technological realm—that is relevant to decisions under uncertainty in all domains, including the strategic decision to initiate or refrain from war. Returning to the metaphor, one finds that new technologies often yield better outcomes than standard technologies. However, what is new is usually less thoroughly studied and less well understood than what is old. Hence, the new technology may entail unexpected and severely adverse consequences that could make it much worse than the current state of the art. The strategic planner who must choose between an innovative strategy and a more standard policy faces an innovation dilemma. The latter is a paradigm for the dilemmas of uncertainty that face the strategic planner, even when the options do not entail innovative technology. In many situations, the innovation dilemma is an instance of the security dilemma due to the great uncertainty surrounding the intentions and capabilities of a state's potential adversaries, as discussed elsewhere.[3]

To "satisfice" means to satisfy a critical or essential outcome requirement. The decision strategy called *robust satisficing* is motivated by severe uncertainty. Good outcomes are better than bad ones, suggesting that the best outcome is best. However, when an option must be selected despite severe uncertainty in the outcomes of all available options, the logic of outcome optimization is not implementable: we don't know which option will have the best outcome. In this situation, the strategic decision maker in a deterrent situation can ask what outcome must be attained or, equivalently, what the worst tolerable outcome is. Under severe uncertainty, the robust-satisficing planner chooses the option that will produce the required outcome over the widest range of deviation of future reality from current anticipation. As we will see, the robust-satisficing choice may differ from the outcome-optimizing choice.

The article shows how robust satisficing is used to manage an innovation dilemma in the context of strategic decisions of war or peace. As mentioned above, it does not propose a theory of deterrence but a method for analyzing and choosing between options. After critiquing deterrence theory, the article then presents a formal analysis of info-gap robust satisficing, the innovation dilemma, and the loss of deterrence.[4] The following section discusses a historical example. The goal here is not descriptive but illustrative: to demonstrate how decision makers could have implemented robust satisficing as a decision strategy. The article then considers a theoretical application, stressing prescription over description.

Three caveats are necessary. First, the study examines binary choices between war and no war. However, strategic choices are rarely binary. Nonetheless, the analysis

provides a conceptual framework for understanding and supporting real decision processes under uncertainty. Second, the discussion is limited (mostly) to conflict between two states. The world is never strictly bipolar although subconflicts, camps, or coalitions often emerge that resolve confrontations into bipolarity at some level. Extension to multistate conflict remains largely unexplored. Third, the article examines "the planner" or "the decision maker," while governments are rarely unitary actors. However, the analysis can be applied separately to individual protagonists, illuminating their positions. Moreover, the info-gap robust-satisficing methodology is a prescriptive tool for individual decision makers.

Critique of Deterrence Theories

This portion addresses both quantitative and qualitative treatments of uncertainty and the optimization of outcomes.

Treatment of Uncertainty: Quantitative Probabilistic and Game-Theoretic Approaches

In a series of articles, R. Harrison Wagner develops an approach to deterrence based on game theory, with incomplete information represented by subjective probabilities, primarily in the context of bipolar nuclear competition. He argues that bargaining between competing powers exists solely because of "lack of complete information about each other's values."[5] The bargaining hinges on assessments of credibility or probability of threat rather than certainty of threat. Wagner subsequently asserts that "the use of nuclear counterforce strategies . . . is not necessarily inconsistent with rational behavior."[6]

These game-theoretical arguments depend on incomplete information represented, for instance, by probabilities of strikes, counterstrikes, and levels of damage. Putative values of these probabilities can lead to rational prioritization among the options (e.g., counterforce strike or not). Wagner continues the exploration of game theory for "formalization of theories of deterrence that incorporate incomplete information, learning and the development of reputations" and studies "how much misperception by foreign decision-makers is consistent with rationality, in light of these new developments in game theory."[7] In a long section entitled "Deterrence and Uncertainty," he explains that each protagonist "must estimate the probability" that the other protagonist will act or not act in particular ways. Furthermore, "probability . . . can only be a subjective probability."[8] After characterizing subjective probability, Wagner comments on why it is not necessarily unique and shows that evaluation of probability can be quite involved. He also notes that there can be dispute over utility assignments.[9]

Responding to Wagner, Anatol Rapoport emphasizes the "formidable difficulty" in game theory of obtaining a "meaningful operational definition of subjective probability" and a "meaningful operational definition of utility," which "become insuperable in the context of nuclear deterrence."[10] Also responding to Wagner, Michael McGinnis criticizes the "implausibility of some of the underlying assumptions," especially the heavy computational burden required of decision makers to implement a game-theoretical analysis. He notes that "neither preferences nor beliefs can be directly observed, and yet knowledge of both is crucial to any determination of equilibrium conditions."[11]

Christopher Achen and Duncan Snidal reply, as would Wagner presumably, that rational deterrence theory does not suppose the agents actually implement the game-theory analysis—only that their behavior is consistent with its rational predictions.[12] This point suggests that game theory is useful as a descriptive tool for political scientists and historians, but it also indicates its limitations as a prescriptive tool for decision makers. McGinnis criticizes the use of game theory because it will "tightly constrain the range of uncertainty" while in fact agents may be uncertain about others' preferences and types and degrees of rationality. He adds that "crucial aspects of any empirical situation remain outside the formal structure" of game theory.[13]

Wagner's important contribution is incorporation of incomplete information in a game-theoretic treatment of deterrence. This incorporation is limited, however, to probabilistic representation of uncertainty. Although strict Bayesians maintain that all uncertainty and ignorance can be represented with subjective probability, Wagner expresses some reservations about Bayesian learning despite its attractive features.[14]

D. Marc Kilgour and Frank Zagare study deterrence and credibility of threats given "lack of information about the preferences of one's opponent."[15] They consider the prisoners' dilemma and modifications of it, recognizing that "the real world, of course, is not so simple or transparent. It is characterized by, among other things, nuance, ambiguity, equivocation, duplicity, and ultimately uncertainty. Typically, policymakers are unable to acquire complete information about the intentions of their opponents; at best, they can hope to obtain probabilistic knowledge of these key determinants of interstate behavior."[16]

Probabilistic analyses supply valuable insights although these depend on strong assumptions. For example, Philipp Denter and Dana Sisak show how loss of deterrence may result from "incomplete information" modeled as parametric uncertainties represented by probability densities on bounded finite intervals and other more explicit assumptions.[17]

Not all deductive theories rely exclusively on probability. Barry Nalebuff, for instance, recognizes that "in the presence of incomplete or imperfect information . . . there is no longer any guarantee that the calculations will provide a unique answer." This "indeterminacy" may lead to "a multiplicity of equilibria" that is not resolved

probabilistically.[18] Recognition that uncertainty may transcend probability is welcome and needed, to which we return subsequently. Nonetheless, Nalebuff uses strong probabilistic assumptions. His most important innovation is the study of expectations by each protagonist of other protagonists' behavior: "Each side starts with some expectation about the distribution of the other's parameter. For analytic convenience, we take the initial beliefs to be uniformly distributed between zero and one."[19] One wonders how such a model captures, for instance, Egyptian president Gamal Abdel Nasser's uncertain expectations in the mid-1960s about Saudi and Jordanian reaction to Egyptian involvement in the civil war in Yemen; Israeli reaction to Egypt's closing the Straits of Tiran; and Arab public reaction to forward deployment of Egyptian forces in Sinai.

The approach to uncertainty in the present article, based on info-gap theory, is nonprobabilistic and offers a potential supplement or alternative to probability. Info-gap models of uncertainty are well suited to representing ignorance—for instance, incomplete information about protagonists' preferences.[20] Similarly, the nonuniqueness of subjective probability or utility, mentioned by Wagner, can be captured with info-gap theory.[21] Most importantly, info-gap robust satisficing can be implemented conceptually without resorting to mathematics, as discussed subsequently.[22] The innovation dilemma developed here can lead to rational reversal of preference among the options in light of one's uncertainties, as we will explain. This study takes the view that ignorance and deception may preclude knowledge of probabilities or even full identification of the event space. Info-gap robust satisficing provides a response that is epistemically less demanding than probabilistic approaches.

Treatment of Uncertainty: Qualitative Historical Approaches

Studying the past refines one's judgment and insight about possible futures. The historical case-based school claims, rightly, that historical, political, psychological, and organizational factors underlie comprehensive understanding of human affairs. However, that very contextualization may limit the ability to anticipate and respond to surprising future contexts.

Authors from historical-inductive schools address uncertainties without employing probability. In case studies of deterrence in the Middle East, Janice Gross Stein emphasizes that success or failure of deterrence depends on leaders' judgments, suspicions, and fears regarding many diverse issues, including opportunities, vulnerabilities, challenges, political or psychological needs, balance of power, broad historic or intrinsic interests, and long-term strategic reputation. Furthermore, a leader's attention to issues may change over time as circumstances change.[23]

Similarly, Richard Ned Lebow and Stein claim that theories of deterrence based on rational choice theory "are incomplete and flawed" because judgments of "subjective expected utility will vary enormously depending on actors' risk propensity and

relative emphasis on loss or gain" and because they ignore factors such as domestic politics. They also point out that leaders' preferences will alter over time, asserting that "misperception and miscalculation arise from faulty evaluation of available information. Studies of deterrence and intelligence failures find that error rarely results from inadequate information but is almost always due to theory and stress driven interpretations of evidence."[24] In a subsequent publication, Lebow and Stein point out that "existing theories of deterrence rely on technical, context-free definitions of deterrence, but deterrence—and any other strategy of conflict management—takes on meaning only within the broader political context in which it is situated" and that historical context is also important. Furthermore, deterrence may be intertwined with other goals such as compellence.[25] (Compellence is an action or threat intended to *induce* an adversary to take a specific action, unlike deterrence, which aims to *prevent* a specific action.)

They write that "deterrence encounters are embedded in two kinds of contexts. The first . . . concerns the specific situation in which a deterrence encounter arises. The second is historical; it consists of the expectations that the adversaries have of each other, themselves, and third parties."[26] Similarly, Alexander George and Richard Smoke maintain that "deterrence at the substrategic levels of conflict is highly context-dependent [and that] there is a critical need in policy making for good situational analysis."[27]

As understanding becomes more contextually detailed, it becomes more contextually contingent and potentially less pertinent to the future. Scholars are well aware of the trade-off between contingency and generality, as George and Smoke illustrate with the concept of "conditional" or "contingent generalizations."[28] The info-gap robust-satisficing strategy discussed in this article is a tool for managing that trade-off. Solomon's error could be rephrased as saying that the worst that was, is as bad as it will ever get. Contextual understanding must support imaginative recognition that things will be different, possibly worse than before. One cannot know what is not yet devised or discovered, and guessing the future is usually infeasible. One can, however, prioritize one's options according to their robustness against future surprise while aiming to satisfy critical goals. This robust-satisficing approach can lead rationally to reversal of preference among options, especially when one faces an innovation dilemma, as we will see.

Optimization of Outcomes

Rational choice theory postulates that "actors . . . seek to optimize preferences in light of other actors' preferences and options."[29] Likewise, in discussing the role of expectations in rational deterrence theory, Nalebuff asserts the centrality of "maximizing behavior."[30] What is postulated is that actors attempt to optimize the substantive quality of the outcome. Paul Huth and Bruce Russett "assume that decision-makers

are rational expected utility maximizers. . . . We use 'rational' in the sense of being able to order one's preferences, and to choose according to that ordering and perceptions of the likelihood of various outcomes. . . . [This] does not require that perceptions be accurate, or that a given decision-maker's preferences be the same as other people's."[31]

George Downs explains that "the calculus [of rational deterrence theory] thrives on optimization, but it is compatible with the addition of numerous constraints that collectively dull the effects of the optimization assumption to the point where they are unrecognizable and quite mild."[32] We claim, however, that constraints limit the domain on which solutions are sought but do not alter the logic of seeking the substantively best outcome. This search may be infeasible and undesirable under severe uncertainty, as demonstrated later.

Zagare focuses on the incomplete knowledge and limited analytical capability of the decision maker. Citing Duncan Luce and Howard Raiffa, he studies the instrumentally rational actor "who, when confronted with 'two alternatives which give rise to outcomes, . . . will choose the one which yields the more preferred outcome.'"[33] However, under severe uncertainty, what looks like the more preferred option may turn out worse than the alternative. We show that, when one faces an innovation dilemma, this possibility can rationally lead to choosing the evidently less preferred option.

Zagare explains that "only two axioms, associated with the logical structure of an actor's preference function, are implicit" in instrumental rationality: connectivity and transitivity, pointing out that "connectivity simply means that an actor be able to make comparisons among the outcomes in the feasible set and evaluate them in a coherent way." Transitivity means that if option A is preferred to B, and B is preferred to C, then A is preferred to C. Zagare continues: "Surely these are minimal requirements for a definition of rationality. Without them, choice theory would be well-nigh impossible."[34]

Transitivity and connectivity imply that the agent chooses the option that is anticipated to yield the best outcome. However, sensible decision makers can hold nontransitive preferences, as illustrated by the Marquis de Condorcet's paradox in aggregating preferences over several voters.[35] Moreover, connectivity depends on identifying all relevant options—an often challenging or even infeasible task. Both axioms depend on the preferences being stable over time, which need not hold. James March has criticized the rigidity of such axioms as "strict morality," noting that "saints are a luxury to be encouraged only in small numbers."[36]

We claim that, prescriptively, it is better to optimize the reliability or confidence of achieving critical goals than to try to attain the highest possible goal. It is not optimization per se that is objectionable; we advocate optimizing the robustness. But robustness is an attribute of a decision, not a substantive "good" that is enjoyed at the

outcome. It is unrealistic, as shown subsequently, to try optimizing the substantive outcome under severe uncertainty.

Deterrence and Uncertainty

We distinguish between two aspects of the relationship between deterrence and uncertainty. First, uncertainty deters. Second, deterrence is uncertain.

On the first point, that *uncertainty deters,* Yehoshafat Harkabi writes that "deterrence, one can suppose, results not from certainty that the threat [of massive nuclear response] would be realized, but from uncertainty that it would not be realized. Thus, it is not certainty, but rather doubt, that deters."[37] In a similar vein, but not limited to the nuclear context, Thomas Schelling observes that the threat of a limited war "is a threat that all-out war *may* occur, not that it certainly will occur, if the other party engages in certain actions" (emphasis in original). Hence, "the supreme objective [of limited war] may not be to *assure* that it stays limited, but rather to keep the risk of all-out war within moderate limits *above zero*" (emphasis in original).[38] The other party is deterred by the uncertain possibility of all-out war.

The second point, that *deterrence is uncertain,* derives from myriad uncertainties in planning, preparing, and executing war. The difficulty is the tremendous uncertainty in anticipating the development of the conflict. Herman Kahn notes that "*history* [meaning the future] *has a habit of being richer and more ingenious than the limited imaginations of most scholars or laymen*" (emphasis in original).[39] He analogizes to an engineer's design of a building that must perform "under stress, under hurricane, earthquake, snow load, fire, flood, thieves, fools, and vandals. . . . Deterrence is at least as important as a building, and we should have the same attitude toward our deterrent systems. We may not be able to predict the loads it will have to carry, but we can be certain there will be loads of unexpected or implausible severity."[40]

The calculations and estimates that underlie deterrence are mostly deliberative, not quantitative, and always highly uncertain.[41] For example, evaluating the balance of local military power underlies deterrence assessment.[42] However, evaluating the balance of future local power is highly uncertain because it depends on many case-specific factors: geopolitics, adversary capability and commitment, extent of forward-deployed friendly combat power, the adversary's unknown future access-denial technologies, and so forth. Similarly, deterrence depends in part on "deciding what targets are most valuable in the state to be deterred."[43] In the Persian Gulf War of 1991, the US threat to remove Saddam Hussein's regime was an effective choice of target that, David Szabo argues, deterred the use of weapons of mass destruction by the Iraqi regime. In other situations, identifying high-value targets may be much more difficult and uncertain because they depend on unfamiliar cultural values of the adversary, as in a conflict with the Taliban or the Vietcong.

Assessing or planning deterrence depends on judgments based on the best available knowledge. However, this knowledge is inevitably wrong—sometimes substantially wrong—and the error may have "unexpected or implausible severity." This article concentrates on the implications of this principle for deterrence and its failure. Stated differently, even though uncertainty deters, we will demonstrate that deterrence can be lost because of uncertainty—not in the sense that enemies miscalculate but in the sense that prioritization of options (e.g., use or don't use weapons of mass destruction) is fundamentally altered under severe uncertainty. This phenomenon may be important in explaining the paradoxical or seemingly irrational breakdown of deterrence. Our emphasis, though, is prescriptive—how planners can manage uncertainty in deterrent situations. Info-gap robust satisficing is a generic decision methodology applicable to any deterrent situation such as conventional or nuclear war, asymmetric war, or terror.[44]

Innovation Dilemma: Formal Analysis

This section formulates the concept of an innovation dilemma—a paradigm for decision under severe uncertainty, through which we identify situations in which deterrence may fail. Following the presentation of a formal analysis of the innovation dilemma is a discussion of the relationship between the prisoner's dilemma and the innovation dilemma and a summary of the formal characteristics of the info-gap analysis of the innovation dilemma.

The choice and its dilemma. An analyst must choose between two alternatives with severely uncertain outcomes. One alternative is purportedly better, but also much more uncertain, than the other. This analysis is based on info-gap decision theory in which *uncertainty* means substantial lack of knowledge or understanding about essential aspects of the problem.

Consider a conflict between two states. We reason from the position of one side, and we must choose between two highly stylized strategies: either initiate war (IW) or do not initiate war (NIW). In the hypothetical example, NIW is more attractive than IW because available knowledge and understanding indicate that the other side won't initiate war, so war would not ensue. (Our analysis is also applicable to the reverse situation in which IW is more attractive.)

However, the available knowledge and understanding—referred to as our "model"—are highly uncertain. This uncertainty is especially acute regarding our adoption of NIW. The adversary's reasoning may differ from ours, and we may not fathom his thinking. For instance, regarding the Strategic Defense Initiative in the mid-1980s, David Windmiller comments that "the Soviets are fundamentally different from Americans in their politics, ideology, social system, the way they think about peace and security, and in their world outlook."[45] Attitudes may differ towards countervalue (civilian and economic targets) rather than counterforce (targeting retalia-

tory capability) as an IW strategy. Thus, NIW is accompanied by substantial uncertainty and might result in vastly greater damage than anticipated because the adversary might preempt with IW.

There is, of course, uncertainty about the outcome of adopting IW, for which the damage might be "severe" or perhaps "huge"—or maybe even "devastating." The range of this uncertainty, although significant, is much less than the uncertainty attendant upon NIW.

In summary, NIW is anticipated to have a better outcome than IW (based on our model in this stylized example), but the model is more uncertain regarding NIW; therefore, NIW could be worse than IW. This is an *innovation dilemma*: should we choose the purportedly better but more uncertain and hence potentially worse alternative (NIW), or should we choose the purportedly worse but more accurately predictable and potentially better alternative (IW)? The innovation dilemma induces a decision methodology based on robustness against uncertainty that is different, both normatively and prescriptively, from what is usually called optimization, as we now explain.

Models and outcomes. Here, the term *model* refers to our information, knowledge, and understanding—both quantitative as well as contextual, subjective, or intuitive. We refer to outcomes and suppose that better ones have less of something (like destruction) while poorer ones have more.

Model-based optimization of the outcome. Our model—assuming it is correct—indicates that NIW will lead to a better outcome (less destruction) than IW. The model indicates preference for NIW over IW—called "model-based optimization of the outcome." This choice is a good one when the model is pretty good. However, info-gap theory provides a critique of this decision strategy when one faces severe uncertainty, as we will see.

As things go wrong. According to our best understanding, NIW is better than IW, but we have good reason to believe that our understanding is substantially wrong—that is, the model is accompanied by severe uncertainty. This situation produces a fundamental trade-off, central in info-gap theory, that will ultimately lead to a mechanism for loss of deterrence that supports decision making under severe uncertainty. We first explain the idea intuitively.

Suppose we err just a little: our information and understanding are just a little bit wrong. What is the worst outcome that could happen with NIW or with IW? If the worst were to happen (assuming we err just a little), which strategy would we prefer? Since NIW is purportedly better than IW, it is reasonable to suppose that the worst outcome with NIW (with very small error) is still better than the worst outcome with IW. We would probably still prefer NIW over IW.

Nonetheless, the magnitude of the advantage of worst NIW over worst IW, at small error, is probably less than that of putative NIW over putative IW—because

NIW is much more uncertain than IW. NIW can go wrong in more ways, and more severely, than IW.

Now suppose we err a bit more. Worst NIW is perhaps still better than worst IW, but the advantage of NIW over IW is now even smaller.

At some horizon of uncertainty, the worst NIW just equals the worst IW. At an even greater horizon of uncertainty, the advantage switches over to IW: worst NIW is now worse than worst IW.

So which do we choose, NIW or IW? The choice depends on how wrong our model is, but this we don't know. Herein lies the innovation dilemma. A graphical metaphor and then a reinterpretation will lead us towards a solution that assists in choosing between alternatives.

Graphical representation. We now consider a useful graphical metaphor for the trade-off between the horizon of uncertainty and the worst possible outcome of a strategy. The graphs do not represent quantitative analysis; instead, they support judgment and deliberation to reach a decision, as we will see.

First consider figure 1, dealing only with the NIW option. The vertical axis is the horizon of uncertainty in our model, so the lowest point on that axis is labeled "no uncertainty." Higher points on the vertical axis represent greater uncertainty, such as "small" or "large" uncertainty. The horizontal axis represents the worst possible outcome of NIW for each corresponding horizon of uncertainty. The point at which the curve intersects the horizontal axis—at no uncertainty—is the purported no-war estimate of damage, based on our model, of the outcome of NIW. The worst possible outcome gets worse (larger: more destruction) as the horizon of uncertainty increases. Thus, the curve slopes up and to the right. The positive slope represents an irrevocable *trade-off*: the worst that can happen gets progressively worse as the horizon of uncertainty increases.
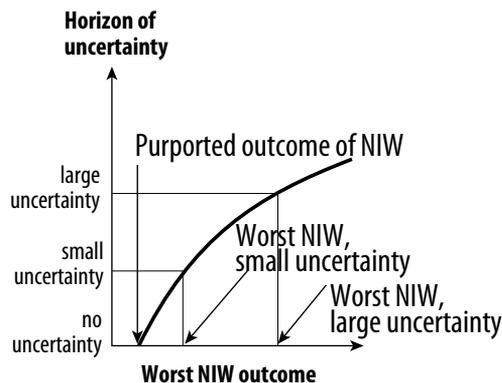

Figure 1. Uncertainty versus worst outcome for NIW

Figure 2 shows uncertainty versus worst outcome for both strategies. We see that the purported outcome for NIW is better (smaller destruction) than the pur-

ported outcome for IW, as indicated by the relative positions of the horizontal inter-
cepts of the two curves. We also see that, at small uncertainty, the worst NIW out-
come is still better than the worst IW outcome: the short solid vertical line is to the
left of the short dashed vertical line. However, the curves cross each other because the
IW curve is steeper than the NIW curve since NIW is accompanied by greater un-
certainty than IW. This intersection of the curves results in the fact that, at large un-
certainty, the worst NIW outcome is now worse than the worst IW outcome: the
long solid vertical line is to the right of the long dashed vertical line (the reverse of
the short vertical lines at small uncertainty). In other words, at large uncertainty, IW
is predicted to have a better worst-outcome than NIW. At large uncertainty, we would
prefer IW over NIW while at small uncertainty, we preferred NIW over IW when
considering worst possible outcomes. The preference between the strategies is not
universal; it changes, depending on the level of uncertainty we consider or, equiva-
lently, the level of destruction we accept. Before continuing to explore the implica-
tions of this preference reversal, we should offer a different interpretation of the axes
in figures 1 and 2.
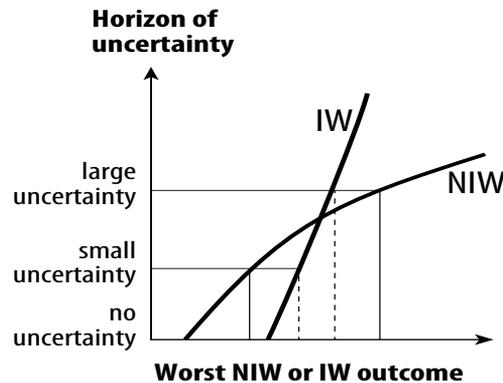
Figure 2. Uncertainty versus worst outcome for NIW and IW

The trade-off: robustness versus performance. The curve in figure 3 is the same as
the one in figure 1: starting at any specified uncertainty on the vertical axis, the arrows
across and down lead us to the corresponding worst possible outcome of NIW at that
horizon of uncertainty. Figure 4 is the same as figure 3 except that we now reverse the
direction of reasoning. Looking at the horizontal outcome axis, we ask, What is the
worst outcome we can tolerate? What is the maximum tolerable damage? Let's de-
note the worst outcome that is still tolerable (the critical or greatest acceptable dam-
age) by D_c. Now we ask the *robustness question*: what is the greatest horizon of uncer-
tainty that we can tolerate? What is the greatest horizon of uncertainty up to which
we are sure that the outcome will not be worse than D_c? The arrows up and to the left
in figure 4 lead us to the answer. The resulting point on the vertical axis is the greatest
tolerable uncertainty of the NIW strategy for this outcome requirement. We will call

this point the *robustness to uncertainty* of NIW for this choice of critical damage. The robustness is large when vast uncertainty is tolerable; small robustness implies great vulnerability to uncertainty.

We can now understand the trade-off mentioned earlier in this section. As the required outcome becomes less demanding (further to the right, accepting greater damage), the intervention is more robust to ignorance. Conversely, the positive slope of the robustness curve in figure 4 implies that robustness-against-uncertainty decreases as the outcome requirement becomes more demanding (further to the left, lower critical damage). This trade-off between robustness and the outcome requirement is intuitively obvious, but it has important implications for choosing a strategy, especially when one faces an innovation dilemma, as we now explain.
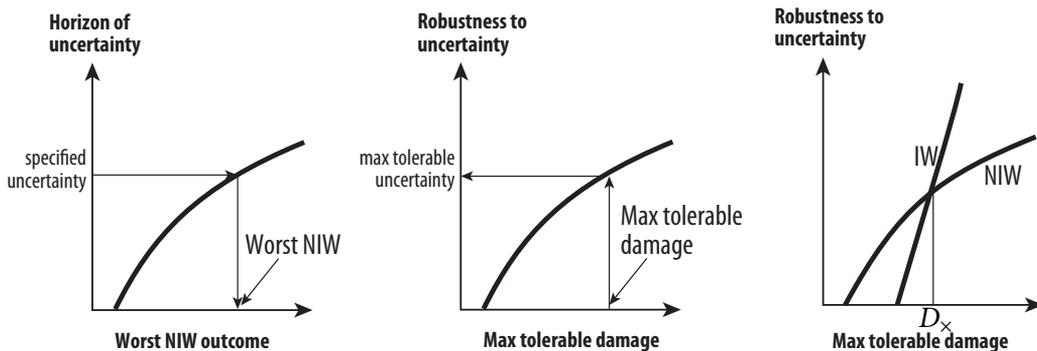

Figure 3. Uncertainty versus worst outcome for NIW

Figure 4. Robustness versus maximum tolerable damage for NIW

Figure 5. Robustness versus maximum tolerable damage for NIW and IW

Preference reversal and the innovation dilemma. Figure 5 plots the robustness curves for IW and NIW. These curves cross each other, just as in figure 2. The intersection between the robustness curves in figure 5 expresses the innovation dilemma. Comparing NIW and IW in this figure, we see that NIW is purportedly better (horizontal intercept further left) but more uncertain (lower slope) than IW. The greater uncertainty of NIW causes the robustness of NIW to increase more slowly as the critical requirement is relaxed: the curve for NIW rises more slowly than the curve for IW as we move right on the horizontal axis (greater critical damage). Hence, their robustness curves intersect because NIW hits the horizontal axis to the left of IW. The graphical manifestation of the innovation dilemma, and of the resulting preference reversal, is that the robustness curves of the two alternatives intersect in figure 5. NIW is more robust—thus preferred over IW—if the outcome requirements are very demanding (the performance requirement is less than D_x on the horizontal axis). For less demanding outcome requirements (the performance requirement exceeds D_x), then IW is more robust than NIW and therefore IW is preferred.

The purported preference is for NIW over IW, implying that war would (purportedly) be avoided. However, if the acceptable level of damage is large enough (exceeding D_x), then IW is preferred over NIW, implying that war occurs and deterrence has failed. In other words, uncertainty leads to the possible loss of deterrence even though the apparent preference of both parties is for the avoidance of war. This mechanism acts even though the robustness curves in figure 5 are schematic and cannot be evaluated quantitatively. The value of D_x is unknown, but deterrence can fail as a result of uncertainty even though the best knowledge and understanding of both parties indicate that no war is preferred.

Robust satisficing: summary. The decision strategy described above entails two elements. The first is called "satisficing": the decision maker must satisfy an outcome requirement. Second, more robustness against uncertainty is preferred over less robustness. Taken together, robust satisficing is the decision strategy that chooses between alternatives to produce the required outcome as robustly as possible. Robust satisficing attempts to satisfice the requirements over the widest range of deviation of reality from the model.

Conceptually different from outcome optimization, robust satisficing may lead to different decisions from outcome optimization. The model-based, outcome-optimal choice is for NIW over IW, as illustrated by the horizontal intercepts in figure 5: NIW is predicted by our model to be better than IW. The robust-satisficing choice is the same if the critical requirement, D_c, is less than the crossing level D_x. On the other hand, robust satisficing and outcome optimization disagree if D_c exceeds D_x. Outcome optimization and robust satisficing may, or may not, agree in managing an innovation dilemma. However, even when they agree on the decision, they disagree on the reason for the decision. That is, outcome optimization and robust satisficing are normatively and prescriptively different: the standard of what constitutes a good decision is different, and the actual decision that is made can be different. We illustrate how robust satisficing is operationalized in a subsequent historical example.

Summary of Formal Conclusions and Comparison to the Prisoner's Dilemma

The prisoner's dilemma has been fruitfully applied to deterrence and other military decisions under uncertainty.[46] The prisoner's dilemma and the innovation dilemma both deal with choice under uncertainty, but they illuminate different aspects of the challenge despite a superficial similarity.

In the prisoner's dilemma (see the table below), if both prisoners remain silent, they are both fined lightly. If they both testify, they are both fined heavily. If one testifies and the other remains silent, then the first goes free and the second is hanged. For each prisoner, testifying is the choice that minimizes the worst outcome, given the unknown choice of the other prisoner. This minimum-maximum (min-max) outcome (heavy fine) is worse than the light fine they would receive if both remain silent.

The dilemma for each prisoner is that remaining silent is the most dangerous choice (one could get hanged), yet it would have a fairly good outcome if both remain silent (light fine).

Table. Prisoner's dilemma

		Prisoner B	
		Testify	Silent
Prisoner A	Testify	A: heavy fine B: heavy fine	A: freedom B: hanged
	Silent	A: hanged B: freedom	A: light fine B: light fine

An innovation dilemma is the choice between two options, one of which—the purportedly better option—could be worse than the other one. This scenario is different from the prisoner's dilemma in which the potentially best option (testifying and going free) is *not* also the potentially worst option (remaining silent and being hanged). So the prisoner's dilemma is not an innovation dilemma, and an innovation dilemma is not a prisoner's dilemma—but the difference is not only structural.

The info-gap analysis of an innovation dilemma begins by recognizing the severe uncertainty of one's knowledge (what we have called the model), leading to three conclusions. First, model-based predictions are unreliable; hence, prioritization of the options according to model-based predictions is also unreliable (represented by the horizontal intercepts of the robustness curves in figure 5). Second, as a consequence, the decision maker must ask what is the worst acceptable outcome (different from asking what is the best outcome consistent with one's knowledge). Third, if the putatively better option is also more uncertain, then the other option will be more robust to uncertainty if the outcome requirement is not too demanding (the robustness curves in figure 5 cross one another). Again, the innovation dilemma is a choice between two options, one of which—the purportedly better option—is more uncertain and could be worse than the other one. The info-gap resolution of the dilemma is to select the option that most robustly satisfies the decision maker's outcome requirement.

The prisoner's dilemma highlights the difference between individual and collective rationality or between selfish and altruistic behavior. The prisoner's dilemma demonstrates how uncertainty can inhibit cooperation that otherwise would be mutually beneficial. The innovation dilemma reveals the reversal of preference between options resulting from the robust advantage of the suboptimal option for achieving some critical outcomes. The info-gap analysis of robustness shows that outcome optimization can be more vulnerable to uncertainty than suboptimal satisficing of a critical goal.

Both the prisoner's dilemma and the innovation dilemma highlight deficiencies of the min-max or worst-case decision strategy, but in different ways. In the prisoner's dilemma, the worst that can happen if one testifies is a heavy fine, which is less onerous than the worst that can happen if one keeps silent (being hanged). Testifying minimizes the maximum penalty and is the min-max choice. That choice, though, differs from the collaborative selection that would result in a better outcome for all (light fine). The altruistic or group-conscious decision maker should not use the min-max strategy, assuming all other decision makers are like-minded.

One can understand the min-max choice for an innovation dilemma by referring to figure 2. At large uncertainty, the worst that happens with IW is better than the worst that happens with NIW, so IW minimizes the worst outcome and is the min-max choice. However, that choice may not be the most robust one for attaining a specified outcome. For example, suppose that the analyst agrees that the uncertainty is large. But suppose that the decision maker must deliver an outcome that is better (smaller) than the value on the horizontal axis at which the curves intersect in figure 2. The min-max choice is IW while NIW is more robust against uncertainty for achieving the required quality of outcome. In this case, the min-max optimum and the robust optimum do not agree. The decision maker charged with producing an outcome better than the crossing value should not use the min-max strategy even though the uncertainty is large.

Historical Example of Uncertainty and Deterrence: Six-Day War (Israeli Decision to Attack)

A historical case demonstrates how the innovation dilemma provides a prescriptive model for decision making. Figure 5 is the graphical paradigm. NIW is the preferred option based on the best available but highly uncertain information and understanding. If this information and understanding (the model) were correct, then IW would entail greater loss. However, the model is uncertain—and more so for NIW than for IW. Thus, while NIW is purportedly better, it could lead to a worse outcome than IW. This dilemma is portrayed in the graphical metaphor of figure 5 by the crossing robustness curves. The dilemma is resolved by choosing the option that would lead to an acceptable outcome over the widest range of unknowns—by choosing the option that most robustly satisfies the critical outcome requirement.

The Israeli decision to initiate war on 5 June 1967 against an array of Arab states provides a good example of decision making in the face of an innovation dilemma. We analyze the options to initiate war (IW) or to not initiate war (NIW) from the perspective of Israeli decision makers. The claim is not that the decision makers actually reasoned this way but that this reasoning is implementable and instrumentally justifiable.

The Model in Support of IW

Tensions grew among Israel, Syria, Egypt, and subsequently Jordan and other Arab countries in mid-May 1967. Exchange of fire between Israel and Syria in the north had occurred repeatedly over the years and intensified in April due to Israeli and Syrian disputes over agricultural use of demilitarized zones, Syrian support of terrorist actions against Israel, and operations to divert sources of the Jordan River in Syrian and Lebanese territory to bypass Israel. Egyptian president Nasser responded, in support of Syria, with a series of threatening actions on Israel's southern border. On 18 May, Egypt demanded the immediate departure of the United Nations Emergency Force stationed in the Sinai desert since the end of the 1956 Sinai war, to which UN secretary-general U Thant acquiesced with little resistance. Egypt then began a massive buildup of infantry, armor, and airpower in the Sinai, partly deployed offensively and close to the Israel-Egypt border. Syria and Jordan mobilized massively, together with significant troop movements to the theater from Iraq and other Arab countries. On 22 May, Egypt announced the closure of the Straits of Tiran to Israeli shipping. The United States tried to enlist maritime countries in the Regatta Plan to sail through the Straits of Tiran, accompanied by destroyers from the Sixth Fleet, asserting international rights of free passage. Regatta never materialized. On 30 May, Egypt and Jordan signed a mutual defense pact allowing Egyptian forces to operate from Jordan and placing Jordanian forces under Egyptian command, creating a strategic threat close to the main Israeli population centers.[47] Arab public opinion and leadership pronouncements vigorously expressed the desire to change the status quo: to liberate Palestine and to eliminate the State of Israel.[48]

The Model in Support of NIW

The Egyptian force buildup in the Sinai during May 1967 seemed closely parallel to Operation Retama in February 1960. Egypt brought two divisions to the Sinai following escalation between Syria and Israel in early 1960. In response, Israel rushed reinforcements to the south, placed its air force on alert, and began diplomatic exchanges to assure all parties that Israel had no offensive intentions against Syria or Egypt. Tensions ran very high until Nasser removed Egyptian forces from Sinai late in February 1960 and declared that he had saved Syria from war with Israel, thereby strengthening his stature as a pan-Arab leader. The situation in May 1967 looked similar, and Egyptian moves were widely understood—at least at first—as demonstrative but not expressing actual desire for war. Furthermore, Israeli strategy in 1967 was predicated on big-power support. President Charles de Gaulle rebuffed Israeli approaches, and President Lyndon Johnson repeatedly asserted that "Israel will not be alone unless it decides to go it alone," clarifying US unwillingness to support an Israeli initiation of war either verbally or materially, thus supporting NIW.[49] Finally,

Israeli strategy sought to maintain the status quo by virtue of the existence of a vast deterrent force. As long as Israeli deterrence is effective, NIW is preferred.[50]

Uncertainty, the Innovation Dilemma, and Analysis of Robustness

If the model of NIW is correct, then IW would initiate an unnecessary war, so NIW is seemingly preferable. In figure 5, the robustness curve for NIW intersects the horizontal axis at a lower (better) value of "maximum tolerable damage" than the curve for IW.

The uncertainty in the NIW model is prodigious, especially regarding Egyptian intentions in 1967 and the strength of the parallel to Operation Retama in 1960. The Arab military deployment in 1967 far exceeded that in 1960, so even if this reflected Nasser's hand being forced by circumstances in 1967, the possibility of an Arab IW was not negligible. An Arab IW on the small number of highly vulnerable Israeli airfields could be disastrous for Israeli ability to repulse a three-front invasion.[51] In other words, the actual damage resulting from even moderate error in the NIW model could far exceed the putative damage of the alternative—IW.

The uncertainty in the IW model hinges on uncertainty about foreign support and on the Israeli assessment that a surprise Israeli attack would succeed rapidly. Quick success would obviate the need for diplomatic support (primarily from the United States) and for materiel from foreign powers (primarily France and Britain) during the conflict. Confidence in such success eroded somewhat as time passed and the Arab military deployment strengthened. The Arab deployment was enormous, but deficiencies in Egyptian logistics, training, and command structure supported the Israeli assessment. Uncertainty about foreign, especially US, support was prominent.

The uncertainty in the IW model is substantially less than in the NIW model. In figure 5, the IW robustness curve is much steeper than the NIW curve, indicating that IW is less vulnerable to uncertainty. Thus, even at moderate uncertainty, the maximum damage that could result is less from IW than from NIW. The innovation dilemma is that NIW is ostensibly better but more uncertain and hence potentially worse than IW. Graphically, the dilemma is reflected in the robustness curves crossing one another in figure 5.

Israeli defense minister Moshe Dayan, Israeli chief of staff Yitzhak Rabin, and most members of the Israel Defense Force General Staff supported a preemptive strike against Egyptian forces to gain the advantage of air superiority by eliminating the Egyptian air force and crippling the massive offensive Arab deployment. On 4 June, 12 of 14 Israeli cabinet ministers voted to initiate war the following morning.[52] This decision follows the logic of robust satisficing: choosing the option that will lead to an acceptable outcome despite vast uncertainty. One can imagine, counterfactually, that the cabinet would have chosen NIW if it had felt that the model supporting this option was fairly certain. However, this putative first choice was rejected (after several

agonizing weeks) in favor of the IW option that would lead (or so Israel hoped) to lower loss despite the surprises yet to be encountered. We are not imputing a specific mode of reasoning to the Israeli decision makers. Rather, the claim is that the robust-satisficing methodology was an implementable method of analysis that could have been used in this historical case.

Theoretical Application:
Does Uncertainty Increase the Propensity for War?

In the previous section, we saw how decision makers could have used info-gap robust satisficing in a historical situation. We now consider how the info-gap robust-satisficing decision strategy can guide theoretical analysis in support of decision making.

A state must choose between two prototypical strategies: NIW (no initiation of war) or IW (initiation of war). The purported optimal preference—based on the available model—is for NIW over IW. The propensity for war increases if the propensity for preference reversal from NIW to IW is increased by uncertainty. Suppose that one or both protagonists' perceptions change between an overall low level to an overall high level of uncertainty. For example, when the United States discovered a small number of nuclear warheads in Cuba in 1962, US uncertainty regarding Soviet intentions increased greatly. We examine how an increase in uncertainty influences the robustness curves for these two strategies.

Consider, first, a special case: uncertainty of NIW increases without increased uncertainty of IW. New nuclear capability in unstable countries, for example, raises the possibility of IW on their part, so NIW by a traditional power has more uncertain outcome.[53] The uncertainty is severe because a small regional power with limited nuclear capability might argue that a superpower would "deter itself from using nuclear weapons because of the prospect of collateral damage to the region."[54] NIW can also become uncertain if new defensive technology is ambiguous and could be interpreted offensively by an adversary. For instance, President Ronald Reagan's Strategic Defense Initiative could protect US offensive missiles or US cities. The former is defensive: missiles are protected for use in retaliatory strikes. The latter is offensive: missiles are not defended because they are intended for first strikes and cities are defended against retaliation. The ambiguity could make adversarial IW more likely.[55] In these examples, uncertainty surrounding IW by the traditional power is not changed.

Figure 6 shows robustness curves for this situation. The robustness of IW is unchanged, but that of NIW is reduced because of increased uncertainty of NIW. The maximum acceptable damage up to which NIW is robust-preferred is reduced: D_x^{hi} is smaller than D_x^{lo}. Consequently, a reversal of robust preference from the reputed

optimum—NIW—to robust preference for IW occurs at a lower damage threshold due to increased uncertainty in NIW. The latter condition causes greater tendency for the selection of IW and therefore an increased tendency for war. This tendency is further strengthened because, over the range of critical damage for which NIW is more robust than IW, the robustness of NIW is lower because of high uncertainty.
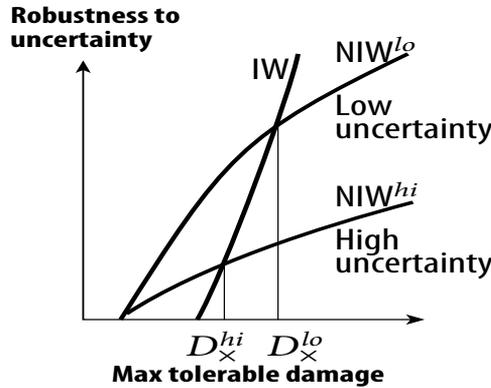
Figure 6. Robustness curves: increased uncertainty of NIW

Now consider the reverse special case: increased uncertainty of IW without increased uncertainty of NIW (fig. 7). Comparing this graph with figure 6 shows a reverse direction of change. In figure 7, the threshold for preference reversal from NIW to IW *increases* as uncertainty increases: D_x^{hi} is larger than D_x^{lo}—the reverse of figure 6. Furthermore, in figure 7, when NIW is more robust than IW, the robustness advantage *increases* because uncertainty in IW increased, unlike the depiction in figure 6.
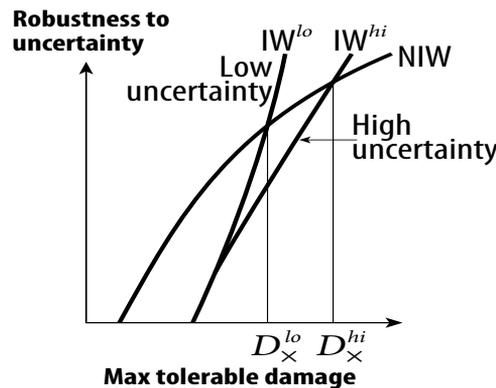
Figure 7. Robustness curves: increased uncertainty of IW

In summary, we cannot conclude that greater uncertainty will necessarily strengthen, or necessarily weaken, the propensity for preference reversal from NIW

to IW and thus increase the propensity for war, as is sometimes claimed. IW and NIW are influenced in opposite directions by uncertainty. However, the analysis identifies those aspects of a scenario determining the impact of uncertainty. The analyst must assess the counteracting effects of uncertainty on the two options—NIW and IW.

Our discussion is purely qualitative; magnitudes of these tendencies cannot be deduced. Nonetheless, the monotonicity and shifts of the robustness curves, due to elevated uncertainty, are unambiguous. The tendencies that we deduced hold for all robustness curves.

Conclusion

We summarize our analysis by returning briefly to the stylized example discussed earlier. Consider conflict between two states. One state, initially deterred from war, must choose between NIW and IW when this choice is an innovation dilemma: NIW purportedly has a better outcome than IW, but NIW is far more uncertain. Reversal of preference to IW reflects loss of deterrence by the other state. The info-gap robust-satisficing decision methodology for managing an innovation dilemma is to choose the option that is more robust-to-uncertainty for realizing a specified goal.

Figure 5 is the schematic graphical representation of this dilemma in terms of robustness curves when NIW is purportedly the better choice so that preference reversal constitutes loss of deterrence. The graphs do not represent quantitative analysis. They are a metaphor of the concept of preference reversal that can arise in response to uncertainty. The graphs support judgment and deliberation in reaching a decision.

If the analyst requires that the level of damage be less than the value at which the two options are equally vulnerable to uncertainty (D_x where the robustness curves in fig. 5 cross one another), then NIW is preferred over IW. In this case, the purported optimum, NIW, is also the more robust option. However, if the analyst is willing to accept greater damage, then greater robustness to uncertainty is achieved with IW. The putatively better option is not necessarily the most robust (and hence preferred) option. The anticipated best option is not necessarily the most robust for reaching specified goals.

The robustness curves in figure 5 are schematic, and we don't expect analysts to be able to evaluate them numerically or to make a quantitative comparison between a numerical value of D_x and an explicit value for maximum acceptable damage. The innovation dilemma is real even though it is not quantitative, and the choice of an option can rationally be made by qualitative verbal deliberation. We can expect that in some situations, an analyst will choose IW over NIW—as in the Israeli decision in 1967—by arguing that this action is the most reliable and responsible in light of the vast uncertainties, especially those associated with NIW. In such situations, deter-

rence has been lost due to the impact of uncertainty. In other situations, the purportedly better but more uncertain option, NIW, may be chosen. Finally, in some situations, no decision is made, or conflicting decisions are adopted for institutional or other reasons.

A theoretical paradigm, such as info-gap robust satisficing, is neither sufficient nor necessary for military success, as Harold Winton concludes in his study of Gen George Patton and Gen Ulysses Grant.[56] However, "to a mind that artfully combines discipline with intuition, theory offers the opportunity to roam freely back and forth between the general and the particular."[57] Theory supports deliberation and decision.

Deliberation takes place, conceptually, on both axes of schema such as figure 5. The analyst makes judgments about how bad an outcome one can accept (or, equivalently, how good an outcome is required) and about how much uncertainty is tolerable. These judgments use models: historical precedent, theoretical insight, contextual understanding, data, social or organizational values and goals, and decisions about reliability or uncertainty of the previous elements. This analysis is particularly useful when one faces an innovation dilemma: one option seems better than another (based on available models), but the apparently better option is also more uncertain. Like all dilemmas, an innovation dilemma has horns, but these can be managed systematically with an info-gap robust-satisficing analysis.

Notes

1. "That which was, will be; that which was done, will be done again; there is nothing new under the sun." Eccles. 1:9.

2. Yakov Ben-Haim, Craig D. Osteen, and L. Joe Moffitt, "Policy Dilemma of Innovation: An Info-Gap Approach," *Ecological Economics* 85 (2013): 130–38.

3. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214; and Yakov Ben-Haim, "Strategy Selection: An Info-Gap Methodology," *Defense & Security Analysis* 30, no. 2 (2014): 108–9.

4. Yakov Ben-Haim, *Info-Gap Decision Theory: Decisions under Severe Uncertainty*, 2nd ed. (London: Academic Press, 2006).

5. R. Harrison Wagner, "Deterrence and Bargaining," *Journal of Conflict Resolution* 26 (1982): 339, 343.

6. R. Harrison Wagner, "Nuclear Deterrence, Counterforce Strategies, and the Incentive to Strike First," *American Political Science Review* 85 (1991): 746.

7. R. Harrison Wagner, "Rationality and Misperception in Deterrence Theory," *Journal of Theoretical Politics* 4, no. 2 (1992): 115.

8. Ibid., 119.

9. Ibid., 119, 124.

10. Anatol Rapoport, "Deterrence Theory Discussion: III; Comments on 'Rationality and Misperceptions in Deterrence Theory,'" *Journal of Theoretical Politics* 4, no. 4 (1992): 481.

11. Michael D. McGinnis, "Deterrence Theory Discussion: I; Bridging or Broadening the Gap? A Comment on Wagner's 'Rationality and Misperception in Deterrence Theory,'" *Journal of Theoretical Politics* 4, no. 4 (1992): 446, 447.

12. Christopher H. Achen and Duncan Snidal, "Rational Deterrence Theory and Comparative Case Studies," *World Politics* 41, no. 2 (1989): 160, 164.

13. McGinnis, "Deterrence Theory Discussion," 448.

14. Wagner, "Rationality and Misperception," 138–39.

15. D. Marc Kilgour and Frank C. Zagare, "Credibility, Uncertainty, and Deterrence," *American Journal of Political Science* 35, no. 2 (May 1991): 306.

16. Ibid., 312.

17. Philipp Denter and Dana Sisak, "The Fragility of Deterrence in Conflicts," *Journal of Theoretical Politics* 27, no. 1 (2015): 43–57, doi: 10.1177/0951629813511712.

18. Barry Nalebuff, "Rational Deterrence in an Imperfect World," *World Politics* 43, no. 3 (1991): 313, 328.

19. Ibid., 320.

20. Yakov Ben-Haim and Keith W. Hipel, "The Graph Model for Conflict Resolution with Information-Gap Uncertainty in Preferences," *Applied Mathematics and Computation* 126 (2002): 319–40.

21. Wagner, "Rationality and Misperception," 119; and John K. Stranlund and Yakov Ben-Haim, "Price-Based vs. Quantity-Based Environmental Regulation under Knightian Uncertainty: An Info-Gap Robust Satisficing Perspective," *Journal of Environmental Management* 87 (2008): 443–49.

22. Ben-Haim, "Strategy Selection." See also Yakov Ben-Haim, "Dealing with Uncertainty in Strategic Decision-Making," *Parameters* 45, no. 3 (Autumn 2015): 63–73.

23. Janice Gross Stein, "Extended Deterrence in the Middle East: American Strategy Reconsidered," *World Politics* 39, no. 3 (1987): 329–31, 333.

24. Richard Ned Lebow and Janice Gross Stein, "Rational Deterrence Theory: I Think, Therefore I Deter," *World Politics* 41, no. 2 (1989): 208–9, 211, 214, 217.

25. Richard Ned Lebow and Janice Gross Stein, "Deterrence: The Elusive Dependent Variable," *World Politics* 42, no. 3 (1990): 351–52, 353, 355.

26. Ibid., 353, 355.

27. Alexander L. George and Richard Smoke, "Deterrence and Foreign Policy," *World Politics* 41, no. 2 (1989): 180.

28. Ibid., 171.

29. Achen and Snidal, "Rational Deterrence Theory," 150.

30. Nalebuff, "Rational Deterrence," 321.

31. Paul Huth and Bruce Russett, "What Makes Deterrence Work? Cases from 1900 to 1980," *World Politics* 36, no. 4 (1984): 499.

32. George W. Downs, "The Rational Deterrence Debate," *World Politics* 41, no. 2 (1989): 235.

33. Frank Zagare, "Rationality and Deterrence," *World Politics* 42 (1990): 240; and Duncan R. Luce and Howard Raiffa, *Games and Decisions: Introduction and Critical Survey* (New York: Wiley, 1957), 50.

34. Zagare, "Rationality and Deterrence," 241.

35. Ken Binmore, *Rational Decisions* (Princeton, NJ: Princeton University Press, 2009); and Steven J. Brams, *Mathematics and Democracy: Designing Better Voting and Fair-Division Procedures* (Princeton, NJ: Princeton University Press, 2008).

36. James G. March, "Bounded Rationality, Ambiguity, and the Engineering of Choice," in *Decision Making: Descriptive, Normative, and Prescriptive Interactions*, ed. David E. Bell, Howard Raiffa, and Amos Tversky (Cambridge, UK: Cambridge University Press, 1988), 51.

37. Yehoshafat Harkabi, *War and Strategy* (Tel Aviv: Maarachot Publishers, 1990), 221–22 (in Hebrew).

38. Thomas C. Schelling, *Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 191, 193.

39. Herman Kahn, *On Thermonuclear War*, 2nd ed. (Princeton, NJ: Princeton University Press, 1961), 137.

40. Ibid., 138.

41. Colin S. Gray, "Deterrence Resurrected: Revisiting Some Fundamentals," *Parameters*, Winter 2010–11, 100.

42. Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age," *Parameters*, Autumn 2009, 32–48.

43. David Szabo, "Disarming Rogues: Deterring First-Use of Weapons of Mass Destruction," *Parameters*, Winter 2007, 82.

44. Amir Lupovici, "The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda," *International Studies Quarterly* 54, no. 3 (2010): 718–20.

45. David E. Windmiller, "SDI: A Strategy for Peace and Stability or the End to Deterrence?," *Parameters*, Summer 1986, 21. See also John M. Weinstein, "Soviet Civil Defense and the US Deterrent," *Parameters*, March 1982, 70.

46. Frank C. Zagare, "Toward a Reformulation of the Theory of Mutual Deterrence," *International Studies Quarterly* 29, no. 2 (1985): 155–69; Harkabi, *War and Strategy*, 299; and Kilgour and Zagare, "Credibility, Uncertainty, and Deterrence."

47. Ami Gluska, *Eshkol, Give the Order! Israel's Army Command and Political Leadership on the Road to the Six Day War, 1963–1967* (Tel Aviv: Maarachot Publishers, 2004), 47 (in Hebrew).

48. Ibid., 199.

49. Michael B. Oren, *Six Days of War: June 1967 and the Making of the Modern Middle East* (New York: Ballantine Books, 2003), 157.

50. Gluska, *Eshkol, Give the Order!*, 199, 401.

51. Ibid., 60.

52. Oren, *Six Days of War*, 157–58.

53. Frederick R. Strain, "Nuclear Proliferation and Deterrence: A Policy Conundrum," *Parameters*, Autumn 1993, 85–86.

54. Ibid., 87.

55. Windmiller, "SDI," 20.

56. Harold R. Winton, "An Imperfect Jewel: Military Theory and the Military Profession," *Journal of Strategic Studies* 34, no. 6 (December 2011): 870.

57. Ibid., 874.

Enable and Enhance—That's It?

European Union Peace Building and the Enable and Enhance Initiative

Witold Mucha, PhD[*]

With the rise of the Islamic State of Iraq and Syria (ISIS), Germany's decision to militarily support Kurdish Peshmerga in northern Iraq revealed the increased importance of the Enable and Enhance Initiative (E2I) as discussed by European Union (EU) member states. In addition to Berlin, policy makers in London and Paris, among others, also followed the rationale of taking responsibility in foreign affairs without being directly involved in military combat. However, as recent initiatives have shown (e.g., in Mali), the E2I approach comes with limitations. Based on recent EU peace-building initiatives in South Sudan and Mali, this article analyzes the challenges faced by any "getting fit initiative." In a brief literature review, it demonstrates the lack of scholarly attention towards the ambivalent scores that EU peace-building approaches have had in the past. The article then presents its analysis framework and introduces the cases of South Sudan and Mali, followed by an empirical analysis conducted on the basis of three categories: scope, design, and unintended effects. Finally, it addresses implications for future research and policy making.

Analysis Framework

This article broadly defines peace building as a range of activities to solidify peace and avoid a relapse into violent conflict.[1] For more than 20 years, peace-building actors such as the United Nations (UN) and/or bilateral donors have been dominated by a liberal peace framework.[2] Although early generation approaches were state- and power-centered (i.e., with a focus on security, territoriality, and the Westphalian state concept), since 1990 peace-building initiatives seek to attain security and institutional development based on externalized forms of intervention. For instance, international transitional administrations such as those in Bosnia and Kosovo

---

[*]The author is a political scientist with a policy-development background in Latin America and sub-Saharan Africa. Based at the Heinrich Heine University, Düsseldorf, Germany, he is interested in peace and conflict studies with a focus on counterterrorism, intelligence, and transnational migration.

have been heralded as role models for future interventions in places where local input was limited at best.[3]

Oliver Richmond, Annika Björkdahl, and Stefanie Kappler differentiate among three types of liberal peace building: conservative, orthodox, and emancipatory.[4] The conservative peace-building model is mainly associated with top-down approaches (i.e., coercive and intrusive). One achieves peace by external military force, not by negotiation. The cases of Afghanistan, Iraq, and Somalia are mentioned in this regard.[5] The orthodox approach differs from the conservative model in that the emphasis is on conditionality to build functional state institutions for liberal-market-oriented states (i.e., partly top-down and cooperative). Establishing democratic institutions and reforming governance frameworks are prioritized. As such, consensual negotiations are mostly based at the elite level; however, local ownership remains limited. The cases of Bosnia-Herzegovina and Kosovo as well as East Timor are dealt with in this respect.[6] The conservative and orthodox approaches resemble the top-down perspective of most peace-building practices by donors, organizations, and institutions. However, after a controversial debate in recent years, critics of liberal peace building have tried to transcend the weakness of the prevalent top-down approaches.[7] The emancipatory approach favors a nonstate-led model shaped by private actors and social movements (i.e., bottom-up and noncoercive). Richmond, Björkdahl, and Kappler effectively summarize the critique and the need for emancipatory views on peace building:

> In many post-conflict environments different groups, often locally constituted, perceive liberal peacebuilding to be ethically bankrupt, subject to double standards, acultural, unconcerned with social welfare, and unfeeling and insensitive towards its subjects. It is tied to the state, to institutions, to the elites that control them, and not to the local context, to civil society or to deeper layers of society. Instead, liberal peacebuilding in post-conflict environments such as the one in Bosnia-Hercegovina has effectively begun to reinstate social and economic class systems, undermined democracy, caused downward social mobility, been built on force rather than consent, failed to recognize local cultural norms and traditions and created a virtual peace in its many theatres.[8]

At best, EU peace-building strategies match the orthodox approach. Given the EU's goal of reforming and transforming future member states, regional integration, harmonization, and standardization constitute the major means. In light of the EU's polycentric structure, however, there is no explicit peace-building strategy on the part of the union as a whole or the European Commission as the unitary actor in charge. However, a variety of elements across EU documents, policies, principles, and speeches includes both goals pursued (e.g., human rights and good governance) and the policy means applied in the process (e.g., trade and rule-of-law missions).[9] In sum, the different means pursue a liberal script of governance reform.

The first EU security strategy, drafted in 2003, called upon the member states to engage in a number of peace activities such as conflict prevention, crisis management, and postconflict rehabilitation. In 2009 the Lisbon Treaty specified the goals of "preserving peace, preventing conflicts and strengthening international security."[10] Sandra Pogodda and her colleagues explain the unique character of the EU as a peacebuilding actor compared to other stakeholders:

> The EU's governance approach in conflict areas ranges from conflict resolution to society-appeasing strategies, while largely abstaining from the pursuit of a mediated, high-level settlement between political leaders or supporting a ceasefire through peacekeeping activities. By interacting with conflict parties at multiple levels—state, sub-state, private sector and civil society—and across a variety of policy areas—economic, social, political, cultural, environmental, infrastructural etc.—the EU's role in conflicts has been more pervasive and often indirect.[11]

The indirect approach of engagement is well reflected by the E2I. In December 2013, the European Council emphasized the importance of empowering global partners to take more responsibility for regional security. The E2I aims to strengthen crisis prevention through the provision of training, advice, and, if necessary, equipment.[12] The concept of capacity building—understood as the provision of advice, training, and equipment to strengthen partners' own capabilities—has been practiced by the UN for many years (e.g., in security sector reforms). Similarly, the EU has supported military and civilian capacity building through missions such as those in Somalia and the Democratic Republic of the Congo.[13] The major argument of the E2I is that police and military training adds little value if the requisite equipment is lacking. The first test cases the EU chose in 2014 to apply the E2I all turned out to be in Africa, starting with Mali and Somalia: "In Africa in particular, programmes that aim to build partners' crisis management and stabilization capacities have long been an integral part of the toolbox."[14]

Some studies have dealt with the lack of effectiveness of EU peace building.[15] Only little attention has been paid to negative spillover effects.[16] At this point, the analysis comes into play. Given the recent formal adoption of the E2I into official documents on the EU council level, only a few cases serve as an empirical basis for analysis. This article deals with EU engagements in armed conflicts in Mali (2012–ongoing) and South Sudan (2013–ongoing) (figs. 1 and 2).
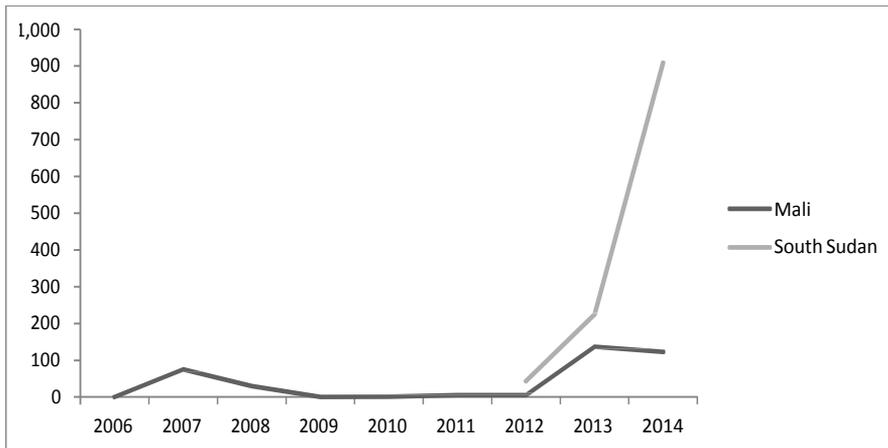
Figure 1. Terrorist events in Mali and South Sudan, 2006–14. (Based on "Global Terrorism Database," National Consortium for the Study of Terrorism and Responses to Terrorism, accessed 18 May 2016, https://www.start.umd.edu/gtd/.)
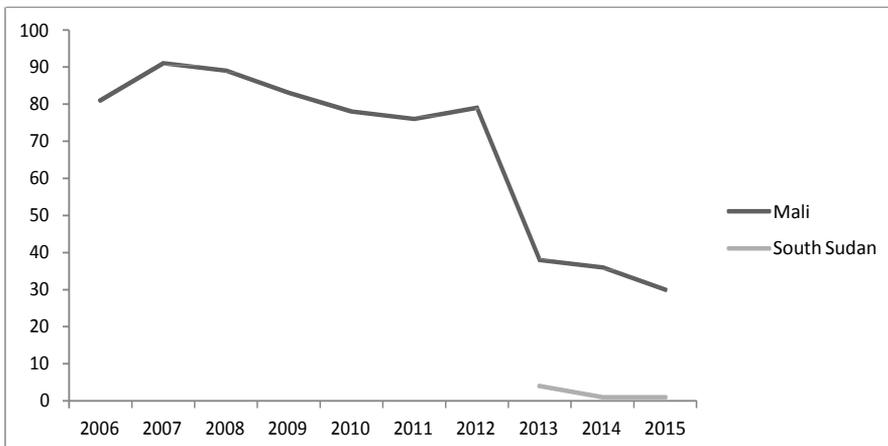
Figure 2. Rankings of Mali and South Sudan as fragile states, 2006–15. (Based on "Fragile States Index," Fund for Peace, accessed 18 May 2016, http://fsi.fundforpeace.org/rankings-2015.)

Analysis

With the German government pushing forward, the E2I was integrated into the final declaration of the EU Summit in December 2013:

> The European Council emphasises the importance of supporting partner countries and regional organisations, through providing training, advice, equipment and resources where appropriate, so that they can increasingly prevent or manage crises by themselves. The European Council invites the Member States, the High Representative and the Commission to ensure the greatest possible coherence between the Union's and Member States' actions to this effect.[17]

Regardless of this formal acknowledgement, recent EU peace-building activities show that any E2I is bound to limitations. The following presents the major challenges on the basis of the cases of South Sudan and Mali.

Scope

Peace-building initiatives are usually criticized for constrained funding.[18] In South Sudan, the EU is the second-largest donor (after the United States). From 2010 to 2013, it has allocated €285 million in development funds, mostly targeting the agricultural sector, education, judiciary, and health infrastructure.[19] As of 2011, assistance to Sahel countries (i.e., Mali, Niger, and Mauritania) totaled more than €600 million. Compared to programs implemented in South Sudan, the focus in the Sahel was on governance reforms (i.e., decentralization, economic development of peripheral areas, etc.) or ad hoc humanitarian assistance to food crises.[20] Given other EU peace-building initiatives such as those in Kosovo (1.8 million people) where external assistance has been transferred since 1999, the question is to what extent the EU and its member states will remain committed to South Sudan (11.6 million) and Mali (14.5 million) in terms of financial volume as well as long-term engagement. Figure 3 illustrates the dimensions.
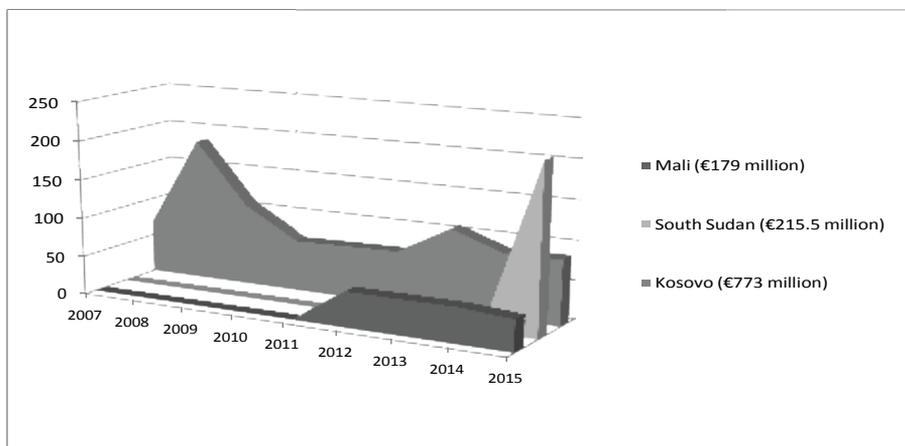
Figure 3. European Commission, technical and financial cooperation, 2007–15. (Based on "Technical and Financial Cooperation," European Commission, accessed 24 May 2016, http://eeas .europa.eu/delegations/kosovo/eu_kosovo/tech_financial_cooperation/index_en.htm; "Fact Sheet: The EU and South Sudan," European Union External Action, 10 July 2014, http://eeas.europa.eu /statements/docs/2014/140514_04_en.pdf; and "ECHO Factsheet: Mali Crisis," European Commission: Humanitarian Aid and Civil Protection, April 2016, http://ec.europa.eu/echo/files/aid/countries /factsheets/mali_en.pdf.)

Besides the ever-criticized underfunding of peace building and foreign aid initiatives, many external measures have been questioned with respect to the waste of

resources.[21] For instance, the May 2013 EU Border Assistance Mission (EUBAM) in Libya was criticized for its rudimentary scope. In light of the local security vacuum in major parts of the country and state authorities existing largely on paper, doubts were cast on whether the border services training could ever be successful without first demobilizing militias and implementing security sector reforms.[22]

This waste of resources sheds light on a related scope issue: capacity-building initiatives are only seldom accompanied by robust mandates. In most cases, external agents fulfil technical functions and lack executive power. For instance, the European Union Aviation Security Mission in South Sudan (EUAVSEC) was established to support the strengthening of security at Juba International Airport: "EUAVSEC will train and mentor security services, provide advice and assistance on aviation security, as well as support the coordination of security activities related to aviation."[23] According to Head of Mission Lasse Christensen, airport security was improved (e.g., mobile airport perimeter control, screening of passengers and luggage, etc.). However, as EUAVSEC was reduced to a technical and advisory role only, no leverage could be made use of against the local warring factions that drove the escalation of violence in South Sudan.[24]

One can make a similar observation when analyzing the European Union Training Mission in Mali (EUTM). According to the mandate, "The restoration of security and lasting peace . . . is a major issue for the stability of the Sahel region, and in the wider sense, for Africa and Europe."[25] As such, the task is to train and advise the military of Mali. EUTM personnel shall not be involved in combat operations and do not have an executive mandate.[26] The mandates of EUAVSEC and EUTM are limited to durations of no longer than 15 months. Given this brief time and scarce personnel resources, a relapse into state failure and escalation of violence is likely. Against this background, Claudia Major, Christian Mölling, and Judith Vorrath argue that external peace builders face a choice: "Either [they accept] that the outcome of many years of development and reform efforts is being called into question, along with confidence in the Federal Government; or attempts are made to avoid this scenario, if necessary by military means."[27] For instance, what if Mali's security forces are not fully operational by now and security sector reforms do not have a significant effect? Would EU member states guarantee stability in case previous peace-building initiatives failed? Again, EU involvement in Kosovo or the International Security Assistance Force (ISAF) mission in Afghanistan speaks volumes about the necessity of long-term and resourceful engagement—notwithstanding the controversy over the latter's peace-building record (table 1).[28]

Table 1. Peace-building/state-building missions

Mission	Technical Staff	Military Staff	Duration
EUAVSEC	64		Jun 2012–Oct 2014
EUTM		550	Oct 2012–Jan 2014
EULEX*	2,000		Feb 2008–ongoing
ISAF		130,000	Dec 2001–Dec 2014

Sources: "European Union Aviation Security Mission (EUAVSEC) in South Sudan," European Union External Action, February 2014, http://www.eeas.europa.eu/archives/csdp/missions-and-operations/euavsec-south-sudan/pdf/factsheet_euavsec_south-sudan_en.pdf; "EU Training Mission in Mali (EUTM Mali)," European Union External Action, December 2015, http://www.eeas.europa.eu/archives/csdp/missions-and-operations/eutm-mali/pdf/factsheet_eutm_mali_en.pdf; "What Is EULEX?," European Union External Action, accessed 24 May 2016, http://www.eulex-kosovo.eu/?page=2,16; and "ISAF's Mission in Afghanistan (2001–2014) (Archived)," North Atlantic Treaty Organization, 1 September 2015, http://www.nato.int/cps/de/natohq/topics_69366.htm.

*European Union Rule of Law Mission in Kosovo

The cost-intensive engagement in Afghanistan brings to mind two things: first, neighboring third states and regional organizations need to be integrated into peace-building initiatives (see below). Second, international coalitions increase the scope of engagement in terms of duration and resources. For instance, local security and political stability are more likely to be achieved in the case of EUTM when organizations such as the African Union can rely on long-term and substantial assistance by the EU and UN. Ownership on the ground depends on external resources.[29]

Design

Closely related to the importance of a broad coalition of local and external allies, the partnership concept determines the credibility of the E2I. Who is supposed to be a reliable partner state? What criteria must a state meet to be considered reliable "enough" for (military) training services and/or arms supplies? In the case of South Sudan, except for Kenya, neighboring countries such as Ethiopia, Chad, Central African Republic, Democratic Republic of the Congo, and Uganda suffer from authoritarian rule and weak statehood (fig. 4). The Polity IV Project illustrates the autocratic legacies on which these countries have been built. For each year and country, a "polity score" is determined that ranges from -10 to 10, with -10 to -6 corresponding to autocracies, -5 to 5 corresponding to anocracies, and 6 to 10 to democracies.[30]
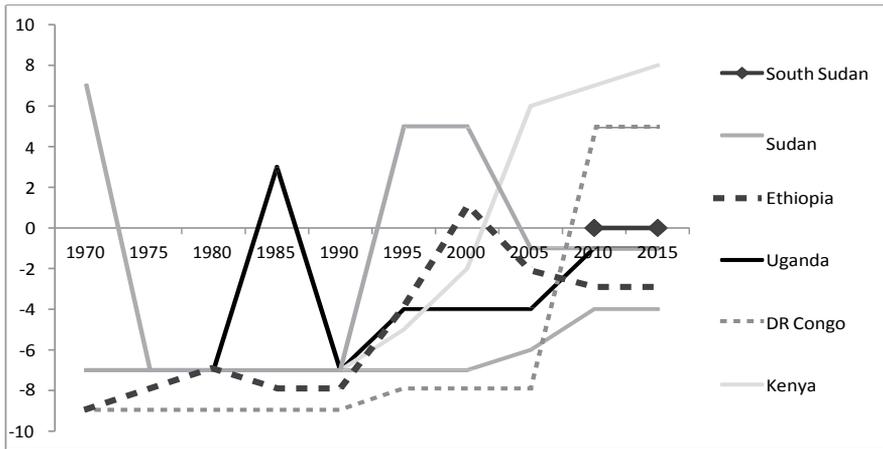
Figure 4. Authority trends, South Sudan neighborhood, 1970–2015. (From "The Polity Project," Center for Systemic Peace, accessed 19 May 2016, http://www.systemicpeace.org/polityproject .html.)

Against this background, external peace builders face a dilemma. On the one hand, regional partners are more likely to increase local legitimacy and ownership in the long run. On the other hand, the stakes are high that military goods and equipment are not under the control of responsible institutions. In the worst case, the transfer of knowledge and arms might even be used against the local opposition. Is regional stability the greater good then? For example, recent, controversial debates were held about military cooperation with Egypt under President Abdel Fattah al-Sisi or the monarchs in Saudi Arabia.[31] As figure 5 shows, the case of Mali speaks differently to this perspective. Neighboring countries such as Algeria, Senegal, or Niger have been praised for political stability.[32]
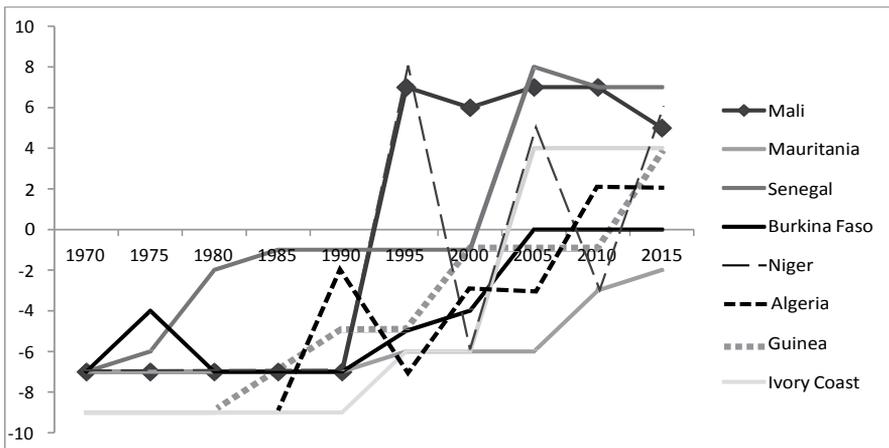

Figure 5. Authority trends, Mali neighborhood, 1970–2015. (From "The Polity Project," Center for Systemic Peace, accessed 19 May 2016, http://www.systemicpeace.org/polityproject.html.)

On the operational level, EU peace-building initiatives face two major challenges. First, given the EU's polycentric (foreign) policy-making architecture, the need for consensus among the different institutions and member states constrains quick responses.[33] Second (closely related), the external agencies confront similar obstacles on the ground. Country office decisions have to be communicated back and forth via the headquarters. The same holds true for the different national ministries (e.g., state department, defense, economy, interior, etc.).[34] The negative effects caused by the lack of coordination, cooperation, and coherence among the different agents on local, national, and international levels (i.e., UN, NATO, World Bank, etc.) have been extensively discussed in the foreign aid literature.[35] Mutual understanding found at conferences in Paris (2005), Accra (2008), and Busan (2011) on the matter can similarly be applied to the peace-building realm.[36]

Despite the agreement among external stakeholders on the need for comprehensive peace-building approaches, a close look at the strategies reveals security-driven agendas. That is, in March 2011 the EU Council endorsed the Strategy for Security and Development in the Sahel. Focusing on Mali, Niger, and Mauritania, the strategy's assistance to governance reform (i.e., decentralization, budget support, etc.) was meant to help "the states and legitimate non-state actors."[37] However, security concerns come first. These include arms proliferation, organized crime, terrorism, and the protection of EU interests and citizens. As of July 2014, adoption of the EU Capacity Building Mission in Niger (EUCAP) did not come as surprise. According to 50 international experts, the EUCAP mandate is to give advice and training to support Nigerien authorities' efforts to strengthen their security capabilities. Although the mission has relatively few personnel, its goals resemble those of EUTM.[38] While EUCAP Sahel Niger supports the fight against organized crime and terrorism in Niger, EUTM contributes to restructuring of the Malian armed forces through training and advice. The critique against the dominance of security concerns feeds into the ever-discussed controversy over the international approach to peace building. A major review addresses external agents' policies for concentrating too much on "top-down approaches of institution-strengthening at (central-) state level, mainly involving government elites."[39] For instance, in the case of the mentioned Sahel strategy document, policy makers explicitly stressed the need to take the local context into consideration:

> In Mali, the setting up of the security and development poles in Northern Mali should muster strong political engagement of the central authorities while benefiting from a higher level of dialogue with the local civil society, in order to consolidate trust to avoid the deployment of security agencies in the North being interpreted by local and traditional leaders as undoing the engagements under the national pact.[40]

To some extent, EU peace-building initiatives in South Sudan followed bottom-up approaches. Brussels funded EU-based nongovernmental organizations to coop-

erate with local communities in cross-border dialogue activities in Sudan and South Sudan.[41] However, the scope of initiatives in South Sudan or Mali in terms of financial and personnel resources was and still is limited. Without a sufficient presence of EU representatives and staff in places such as Juba or Bamako, it is most likely that any intervention into the political process is primarily directed at elites: "In the end, the extension of state authority is a major goal of EU support for these countries, putting into question whether the EU has done enough to foster dialogue with 'legitimate non-state actors' as is . . . foreseen in the Strategy."[42]

Unintended Effects

In autumn 2013, Germany, Denmark, and Portugal circulated an off-the-record paper that addressed the need for the E2I in light of growing maritime insecurity in the Gulf of Guinea.[43] As the problem was characterized earlier, training and arming security services do not guarantee the "right" use of the equipment and learned capacities. The same holds true for enabling regional partners such as Côte d'Ivoire, Nigeria, or Congo. In other words, neither the official E2I approach nor that paper addresses the need for control of military goods and trained capacities.[44] What if Western arms supplies eventually end up in the wrong hands? In particular, the case of Mali highlights the dilemma. To many external observers, the three-year-long armed conflict (2012–15) escalated in January 2012 because of the military professionalization of the National Movement for the Liberation of Azawad. Tuareg-based, the movement fought a campaign against the Malian government for greater autonomy for northern Mali. Apparently, factions of the movement had fought in the Libyan civil war of 2011 and at some point seized military equipment that has been recently used in the struggle against the Malian government.[45] That military equipment did not entirely originate from former president Mu'ammar Gadhafi's arsenal. An unknown but significant quantity of military goods came from those arms supplies that were provided by Washington, London, and Paris via Qatar to the Libyan rebel forces.[46]

The bitter irony is twofold. First, the external military supplies enhanced the military capabilities of the anti-Gadhafi forces. However, after his fall, the different militias made use of these very weapons in the recent civil war.[47] Second, against the background of state erosion in Libya, the illegal arms transfer via Algeria, Niger, and Chad allowed for militarization of insurgent groups in Mali and elsewhere:

> There is a risk that if a government changes or is overthrown, well-trained forces and equipment can fall into the hands of actors who are opposed to the goals being pursued by . . . the EU in the context of security sector reform. In Mali in 2013, for example, soldiers trained by the US deserted to Islamist groups and then fought French troops deployed with Operation Serval. A very large number of weapons circulating on the black market in West Africa come from official stocks, having been sold illegally by the security forces.[48]

In light of the principal-agent dilemma, it is surprising that enabling local proxies remains a major strategy applied by governments in the West as well as the East. Before the following discussion of the implications for future research and policy making, table 2 summarizes the major critique against current EU peace-building missions.

Table 2. European Union peace-building critique

Scope	Design	Unintended Effects
Lack of resources and long- term engagement	Polycentric structure and operational incoherence on the local and international levels	Proxy myth: local and regional destabilization
Lack of executive power; no robust mandate	Top-down	
Waste of resources	Security first	
	Vague partner concept	

Conclusion

The analysis of EU peace building in South Sudan and the Sahel has revealed a number of shortcomings. The *scope* of many initiatives is insufficient. Most of the missions are mandated for a short duration between 12 and 15 months. They are prolonged if deemed necessary and backed by the political willingness of major (external) stakeholders. The lack of long-term engagement comes with insufficient funding in terms of personnel and equipment. In accordance with the E2I approach, most missions lack executive power and are designed without a robust mandate. Local state authorities are to be supported via training and policy advice only; direct confrontations with warring parties are avoided entirely. On the one hand, the limited scope allows for local ownership. On the other hand, a relapse into violent conflict becomes more likely. Besides the absence of engagement in terms of funding and political willingness, the waste of resources by peace builders has been neglected in the literature. The case of EUBAM in Libya well illustrates the deficits. Apparently, EUBAM was never really capable of meeting the mandate in light of the security vacuum in major parts of the country. Doubts proved true that the border services training could not be successful without first demobilizing militias and implementing security sector reform.

Peace-building *design* deficits are closely related to the question of limited scope. Given its polycentric structure, the EU and its member states constantly face veto-player situations when it comes to decisions concerning the Common Security and Defense Policy. Quick responses to crisis situations abroad are thus unlikely. Making matters worse, on the operational level a variety of agents are involved in the peace-

building process. This multitude can constrain the effectiveness of missions. For example, peace-building headquarters in Brussels or capital cities need to coordinate with country offices, allied Western partners, international stakeholders (UN, NATO, African Union, etc.), as well as local state authorities. Frictions can also arise on a national level when different ministries (e.g., state department and ministry of economy) pursue varying interests in the intervened country. Regardless of operational aspects, peace-building missions still suffer from top-down approaches. Despite a controversial debate on (post)liberal peace building and the so-called local turn, peace building on the ground is still driven by interveners in the first place. Similarly, interventions are directed primarily at elites despite official strategy papers mentioning the need for the inclusion of local and traditional leaders in a comprehensive peace-building framework. The same holds true for the priority of security concerns over other sectors such as agriculture, education, health, or the judiciary. Yet another major critique is directed at the vague partnership concept of EU peace-building initiatives in general and the E2I approach in particular. No strategy in sight defines how to identify legitimate actors for cooperation on local ground—be they state authorities and/or neighboring governments.

The difficult assessment of (regional) partners' contribution sheds light on the risks of *unintended effects* of "enable and enhance" approaches. Basically, neither the E2I proposal nor any other strategy document has elaborated on the need for control over enabled actors on the ground. Given the principal-agent-dilemma considerations, "sending" countries such as Germany and France in Mali are not capable of guaranteeing how the training and (military) equipment eventually will be used.

In terms of the critique, it seems that EU peace building has failed and that reforms on the conceptual and operational levels are more necessary than ever. If so, what kind of measures can scholars of peace and conflict recommend? The categories of scope, design, and unintended effects provide a feasible basis in this regard. For instance, the critique against waste of resources is legitimate. The analysis of EUBAM in Libya shows that border training services would have been more successful if security sector reforms had been realized first. However, the argument is ambivalent since critics might stress that the post-Gadhafi security vacuum is probably going to take longer than expected. In that case, a limited peace-building mission might be better than no presence at all. Advocates of robust mandates also have to consider the different implications for sending nations. Besides the ever-valid budget argument, popular support of EUTM in Mali would probably be less if German and/or French soldiers were mandated to take part in armed combat. The likelihood of soldiers killed in action and/or civilian casualties would jeopardize single missions as well as general peace-building approaches in the West. The US experience in Iraq and Afghanistan speaks volumes to war-weary electorates.

Similar ambivalence is found in the critique against the design of peace-building missions. For instance, if senders' resources are limited in any way, then cooperating with prevalent elites seems a pragmatic choice. The same holds true for the priority of security reforms over other sectors. The case of post–Arab Spring Egypt under al-Sisi demonstrates the survival of the old system and donors' willingness to continue the relationship despite the increasingly authoritarian character of the regime in place. The case of Egypt well shows the dilemma. After President Mohamed Morsi's ousting in June 2013, calls by Western policy makers and scholars for sanctions and conditionality (e.g., cutting military cooperation) fell on deaf ears in Cairo as Saudi Arabia promised to compensate for any losses. With the rise of ISIS in Libya and terrorist attacks reaching Tunisia, by 2015 al-Sisi had been invited to talks at European capital cities such as Berlin and elsewhere. Al-Sisi's increased international legitimacy reflects why the E2I partnership concept is vaguely defined: the less rigid the profile, the more flexible the selection of partners by Western governments that have to make political decisions on an ad hoc basis. In a similar vein, the policy makers' perspective needs to be taken into account when questioning the "proxy myth" mentioned above. Despite ambivalent experiences with the mujahedin in Afghanistan in the 1980s and unbound militias in contemporary Libya, governments in the West and East keep making use of proxies, be they in northern Iraq (Kurdish Peshmerga), Mexico (self-defense militias), or Ukraine (Russian separatists). Again, the alternatives for EU peace-building architects are scarce. Our own soldiers will not be sent for the above-mentioned reasons, and a substantial EU drone program has not yet evolved.

Despite the legitimate criticism of EU peace building in general and E2I in particular, scholars likewise seem to have failed in recommending feasible policy options for improvement. Development studies seem to be ahead. The operational aspects of intervention, for example, have been extensively discussed under the rubric of harmonization, coordination, and alignment. In light of the ad hoc nature of crisis situations and Western peace builders' reactive (instead of curative) approach, proposals for operational reform offer a starting point for academic input in this regard. Identifying those specific bolts in the peace-building machine would make scholars' voices better heard than universal critiques and calls for fundamental change.

Notes

1. Michael Barnett et al., "Peacebuilding: What Is in a Name?," *Global Governance: A Review of Multilateralism and International Organizations* 13, no. 1 (2007): 35–58; Roland Paris, "International Peacebuilding and the 'Mission Civilisatrice,'" *Review of International Studies* 28, no. 4 (2002): 637–56; and A. B. Fetherston, "Peacekeeping, Conflict Resolution and Peacebuilding: A Reconsideration of Theoretical Frameworks," *International Peacekeeping* 7, no. 1 (2000): 190–218.

2. Edward Newman, Roland Paris, and Oliver Richmond, eds., *New Perspectives on Liberal Peacebuilding* (Tokyo: UNU Press, 2009); Oliver Richmond, "UN Peace Operations and the Dilemmas of the Peacebuild-

ing Consensus," *International Peacekeeping* 11, no. 1 (2004): 83–101; Susanna Campbell, David Chandler, and Meera Sabaratnam, eds., *A Liberal Peace? The Problems and Practices of Peacebuilding* (London: Zed Books, 2011); and Roland Paris, "Saving Liberal Peacebuilding," *Review of International Studies* 36, no. 2 (2010): 337–65.

3. Richmond, "UN Peace Operations"; Roberto Belloni, "Civil Society and Peacebuilding in Bosnia and Herzegovina," *Journal of Peace Research* 38, no. 2 (2001): 163–80; Oliver Richmond, Annika Björkdahl, and Stefanie Kappler, "The Emerging EU Peacebuilding Framework: Confirming or Transcending Liberal Peacebuilding," *Cambridge Review of International Affairs* 24, no. 3 (2011): 449–69; and Andrea Kathryn Talentino, "Perceptions of Peacebuilding: The Dynamic of Imposer and Imposed Upon," *International Studies Perspectives* 8, no. 2 (2007): 152–71.

4. Richmond, Björkdahl, and Kappler, "Emerging EU Peacebuilding Framework."

5. Toby Dodge, "Intervention and Dreams of Exogenous Statebuilding: The Application of Liberal Peacebuilding in Afghanistan and Iraq," *Review of International Studies* 39, no. 5 (2013): 1189–1212; Olivier Roy, "Development and Political Legitimacy: The Cases of Iraq and Afghanistan," *Conflict, Security & Development* 4, no. 2 (2004): 167–79; Richard J. Ponzio, "Transforming Political Authority: UN Democratic Peacebuilding in Afghanistan," *Global Governance: A Review of Multilateralism and International Organizations* 13, no. 2 (2007): 255–75; and Volker Franke, "The Peacebuilding Dilemma: Military Cooperation in Stability Operations," *International Journal of Peace Studies* 11, no. 2 (2006): 5–25.

6. Astri Suhrke, "Peacekeepers as Nation-Builders: Dilemmas of the UN in East Timor," *International Peacekeeping* 8, no. 4 (2001): 1–20; Charles T. Call and Susan E. Cook, "On Democratization and Peacebuilding," *Global Governance* 9 (2003): 233–46; Hansjörg Strohmeyer, "Making Multilateral Interventions Work: The U.N. and the Creation of Transitional Justice Systems in Kosovo and East Timor," *Fletcher Forum of World Affairs* 95, no. 1 (2001): 107–28.

7. Oliver Richmond, "Becoming Liberal, Unbecoming Liberalism: Liberal-Local Hybridity via the Everyday as a Response to the Paradoxes of Liberal Peacebuilding," *Journal of Intervention and Statebuilding* 3, no. 3 (2009): 324–44; John Heathershaw, "Unpacking the Liberal Peace: The Dividing and Merging of Peacebuilding Discourses," *Millennium: Journal of International Studies* 36, no. 3 (2008): 597–621; Kristoffer Lidén, "Building Peace between Global and Local Politics: The Cosmopolitical Ethics of Liberal Peacebuilding," *International Peacekeeping* 16, no. 5 (2009): 616–34; David Chandler, "The Uncritical Critique of 'Liberal Peace,'" *Review of International Studies* 36, no. 1 (2010): 137–55; Roger Mac Ginty and Oliver Richmond, "Myth or Reality: Opposing Views on the Liberal Peace and Post-war Reconstruction," *Global Society* 21, no. 4 (2007): 491–97; Roger Mac Ginty and Oliver Richmond, "The Local Turn in Peace Building: A Critical Agenda for Peace," *Third World Quarterly* 34, no. 5 (2013): 763–83; and Timothy Donais, "Empowerment or Imposition? Dilemmas of Local Ownership in Post-conflict Peacebuilding Processes," *Peace & Change* 34, no. 1 (2009): 3–26.

8. Richmond, Björkdahl, and Kappler, "Emerging EU Peacebuilding Framework," 454.

9. Sandra Pogodda et al., "Assessing the Impact of EU Governmentality in Post-conflict Countries: Pacification or Reconciliation?," *European Security* 23, no. 3 (2014): 228.

10. Ibid.

11. Ibid.

12. Jana Puglierin, Sebastian Feyock, and Yvonne van Diepen, "Ertüchtigen statt wegsehen: Eine deutsche Initiative soll das Krisenmanagement der GSVP verbessern," *Internationale Politik* 2 (March 2014): 60.

13. Claudia Major, Christian Mölling, and Judith Vorrath, *Train + Equip = Peace? Stabilization Requires more than Capacity Building* (Berlin: German Institute for International Affairs, 2015), 2.

14. Ibid.

15. Ana E. Juncos, "Member State-Building versus Peacebuilding: The Contradictions of EU State-Building in Bosnia and Herzegovina," *East European Politics* 28, no. 1 (2011): 57–58; Joachim Krause and Natalino Ronzitti, eds., *The EU, the UN and Collective Security: Making Multilateralism Effective* (Abingdon: Routledge, 2012); Claudia Morsut, "The UN and EU in the DRC: Effective Multilateralism? EU-UN Cooperation in the DRC, 2003–2006," *International Peacekeeping* 16, no. 2 (2009): 261–72; Isabelle Ioannides

and Gemma Collantes-Celador, "The Internal-External Security Nexus and EU Police/Rule of Law Missions in the Western Balkans," *Conflict, Security & Development* 11, no. 4 (2011): 415–45; Catherine Lynch, "Evaluating the Peace-Building Impact of Structural Funds Programmes: The EU Programme for Peace and Reconciliation in Northern Ireland," *Evaluation* 13, no. 1 (2007): 8–31; Pogodda et al., "Assessing the Impact," 227–49; and Emil Kirchner, "Common Security and Defence Policy Peace Operations in the Western Balkans: Impact and Lessons Learned," *European Security* 22, no. 1 (2013): 36–54.

16. Michael Schulz and Fredrik Söderbaum, "Theorising the EU's Role in Regional Conflict Management," *European Security* 19, no. 3 (2010): 361–76; Stefanie Kappler, "Divergent Transformation and Centrifugal Peacebuilding: The EU in Bosnia and Herzegovina," *International Peacekeeping* 19, no. 5 (2012): 612–27; Patricia Justino, Tilman Brück, and Philip Verwimp, eds., *A Micro-level Perspective on the Dynamics of Conflict, Violence, and Development* (Oxford, UK: Oxford University Press, 2013); and Claudia Major and Christian Mölling, "Towards an EU Peacebuilding Strategy: The Effects of the Lisbon Treaty on the Comprehensive Approach of the EU in the Area of Civilian Crisis Management," *European Foreign Affairs Review* 18 (2013): 45–62.

17. European Council, EUCO 217/13, Brussels, 20 December 2013, 3, https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf.

18. Rory Domm, "Europeanisation without Democratisation: A Critique of the International Community Peacebuilding Strategy in Bosnia and Herzegovina," *Southeast European and Black Sea Studies* 7, no. 1 (2007): 159–76; Jenny Pearce, "The International Community and Peacebuilding," *Development* 48, no. 3 (2005): 41–49; Necla Tschirgi, "Strategic Frameworks and Peacebuilding: Current Trends and Critical Directions," *Journal of Peacebuilding & Development* 5, no. 2 (2010): 1–5; and Terrence L. Jantzi and Vernon E. Jantzi, "Development Paradigms and Peacebuilding Theories of Change: Analysing Embedded Assumptions in Development and Peacebuilding," *Journal of Peacebuilding & Development* 5, no. 1 (2009): 65–80.

19. Marco Overhaus and Mateja Peter, *The EU and Peacebuilding: South Sudan and the Sahel Indicate That the Union Is Rethinking Its Concepts but Not Yet Changing Its Policies* (Berlin: German Institute for International Affairs, 2012), 3; and Mark Furness and Frank Vollmer, *EU Joint Programming: Lessons from South Sudan for EU Aid Coordination* (Bonn: German Development Institute, 2013).

20. Overhaus and Peter, *EU and Peacebuilding*, 3; and "International Donor Conference: €3.25 Billion Mobilised by International Community to Rebuild Mali," press release, European Commission, 15 May 2013.

21. James K. Boyce, "Aid Conditionality as a Tool for Peacebuilding: Opportunities and Constraints," *Development and Change* 33, no. 5 (2002): 1025–48; Anne Le More, *International Assistance to the Palestinians after Oslo: Political Guilt, Wasted Money* (Abingdon: Routledge, 2008); and Susan L. Woodward, "The Political Economy of Peacebuilding and International Aid," in *Routledge Handbook of Peacebuilding*, ed. Roger Mac Ginty (Abingdon: Routledge, 2013), 325–35.

22. Major, Mölling, and Vorrath, *Train + Equip = Peace?*, 3; Tim Haesebrouck and Melanie Van Meirvenne, "EUFOR RCA and CSDP Crisis Management Operations: Back on Track?," *European Foreign Affairs Review* 20, no. 2 (2015): 267–85; and Alistair J. K. Shepherd, "The European Security Continuum and the EU as an International Security Provider," *Global Society* 29, no. 2 (2015): 156–74.

23. "EUAVSEC South Sudan," European Union External Action, accessed 19 May 2016, http://www.eeas.europa.eu/archives/csdp/missions-and-operations/euavsec-south-sudan/index_en.htm.

24. Christopher Zambakari, "South Sudan and the Nation-Building Project: Lessons and Challenges," *International Journal of African Renaissance Studies: Multi-, Inter- and Transdisciplinarity* 8, no. 1 (2013): 5–29; Alex de Waal and Abdul Mohammed, "Breakdown in South Sudan: What Went Wrong—and How to Fix It," *Foreign Affairs*, 1 January 2014, https://www.foreignaffairs.com/articles/sudan/2014-01-01/breakdown-south-sudan; and Alex De Waal, "When Kleptocracy Becomes Insolvent: Brute Causes of the Civil War in South Sudan," *African Affairs* 114, no. 456 (2014): 347–69.

25. "EU Training Mission in Mali (EUTM Mali)," European Union External Action, December 2015, http://eeas.europa.eu/csdp/missions-and-operations/eutm-mali/pdf/2015-december-factsheet_eutm_mali_en.pdf.

26. Daniel Göler, "Zwischen Security Provider und Security Consultant: Veränderungen im Leitbild der strategischen Kultur der Europäischen Union," *Zeitschrift für Außen- und Sicherheitspolitik* 7, no. 3 (2014): 323–42; Rachel Dicke, "The European Union Training Mission in Mali: A Case Study," *Croatian International Relations Review* 20, no. 71 (2014): 91–119; and Thierry Tardy, *CSDP: Getting Third States on Board* (Brussels: European Union Institute for Security Studies, 2014).

27. Major, Mölling, and Vorrath, *Train + Equip = Peace?*, 2–3.

28. Astri Suhrke, "Waging War and Building Peace in Afghanistan," *International Peacekeeping* 19, no. 4 (2012): 478–91; Marissa Quie, "Peace-Building and Democracy Promotion in Afghanistan: The Afghanistan Peace and Reintegration Programme and Reconciliation with the Taliban," *Democratization* 19, no. 3 (2012): 553–74; Chuck Thiessen, *Local Ownership of Peacebuilding in Afghanistan: Shouldering Responsibility for Sustainable Peace and Development* (Lanham, MD: Lexington Books, 2014); Jonathan Goodhand and Mark Sedra, "Rethinking Liberal Peacebuilding, Statebuilding and Transition in Afghanistan: An Introduction," *Central Asian Survey* 32, no. 3 (2013): 239–54; and Anna K. Jarstad, "Unpacking the Friction in Local Ownership of Security Sector Reform in Afghanistan," *Peacebuilding* 1, no. 3 (2013): 381–96.

29. Timothy Donais, *Peacebuilding and Local Ownership: Post-conflict Consensus-Building* (Abingdon: Routledge, 2012); Christoph Zürcher et al., *Costly Democracy: Peacebuilding & Democratization after War* (Stanford, CA: Stanford University Press, 2013); and Lise Philipsen, "When Liberal Peacebuilding Fails: Paradoxes of Implementing Ownership and Accountability in the Integrated Approach," *Journal of Intervention and Statebuilding* 8, no. 1 (2014): 42–67.

30. James Raymond Vreeland, "The Effect of Political Regime on Civil War: Unpacking Anocracy," *Journal of Conflict Resolution* 52, no. 3 (June 2008): 404.

31. Richard W. Bulliet, "Monarchs and Mamluks, or How Do You Say 'Thank You' for $20 Billion?," *Middle East Law and Governance* 7, no. 1 (2015): 16–24; and Oz Hassan, "Undermining the Transatlantic Democracy Agenda? The Arab Spring and Saudi Arabia's Counteracting Democracy Strategy," *Democratization* 22, no. 3 (2015): 479–95.

32. Rem Korteweg, "Treacherous Sands: The EU and Terrorism in the Broader Sahel," *European View* 13, no. 2 (2014): 251–58; and Lawrence A. Ammour, "Regional Security Cooperation in the Maghreb and Sahel: Algeria's Pivotal Ambivalence," *Africa Security Brief* 18 (2012): 1–8.

33. Emma J. Stewart, "Capabilities and Coherence? The Evolution of European Union Conflict Prevention," *European Foreign Affairs Review* 13, no. 2 (2008): 229–53; Paula M. Pickering, "The Constraints on European Institutions' Conditionality in the Western Balkans," *Europe-Asia Studies* 63, no. 10 (2011): 1939–44; Richard Youngs, "Democratic Institution-Building and Conflict Resolution: Emerging EU Approaches," *International Peacekeeping* 11, no. 3 (2004): 526–43; and Stephanie C. Hofmann, "Overlapping Institutions in the Realm of International Security: The Case of NATO and ESDP," *Perspectives on Politics* 7, no. 1 (2009): 45–52.

34. Adam Burke, "Peacebuilding and Rebuilding at Ground Level: Practical Constraints and Policy Objectives in Aceh," *Conflict, Security & Development* 8, no. 1 (2008): 47–69; Krause and Ronzitti, *EU, the UN and Collective Security*; and Thorsten Benner and Philipp Rotmann, "Learning to Learn? UN Peacebuilding and the Challenges of Building a Learning Organization," *Journal of Intervention and Statebuilding* 2, no. 1 (2008): 43–62.

35. Stephen J. H. Dearden, "Introduction: European Union Development Aid Policy: The Challenge of Implementation," *Journal of International Development* 20, no. 2 (2008): 187–92; Cedric De Coning and Karsten Friis, "Coherence and Coordination: The Limits of the Comprehensive Approach," *Journal of International Peacekeeping* 15, nos. 1–2 (2011): 243–72; Robert Picciotto, "The Evaluation of Policy Coherence for Development," *Evaluation* 11, no. 3 (2005): 311–30; and Jörg Faust and Dirk Messner, *Organizational Challenges for an Effective Aid Architecture: Traditional Deficits, the Paris Agenda and Beyond* (Bonn: German Development Institute, 2007).

36. Maurizio Carbone, "International Development and the European Union's External Policies: Changing Contexts, Problematic Nexuses, Contested Partnerships," *Cambridge Review of International Affairs* 26,

no. 3 (2013): 483–96; and Stephan Hensell, "Coordinating Intervention: International Actors and Local 'Partners' between Ritual and Decoupling," *Journal of Intervention and Statebuilding* 9, no. 1 (2015): 89–111.

37. "Strategy for Security and Development in the Sahel," European Union External Action Service 2011, 8, http://eeas.europa.eu/africa/docs/sahel_strategy_en.pdf.

38. See European Union External Action Service, accessed 19 May 2016, http://eeas.europa.eu/index _en.htm.

39. Overhaus and Peter, *EU and Peacebuilding*, 2.

40. "Strategy for Security and Development in the Sahel," 6.

41. Joost van der Zwan, *Evaluating the EU's Role and Challenges in Sudan and South Sudan* (London: International Alert, September 2011), 18, http://www.ifp-ew.eu/pdf/092011IfPEWSudan.pdf.

42. Ibid., 4.

43. Puglierin, Feyock, and Van Diepen, *Ertüchtigen statt wegsehen*, 61.

44. Ibid., 64.

45. Major, Mölling, and Vorrath, *Train + Equip = Peace?*, 3; and Francesco Strazzari and Simone Tholens, "'Tesco for Terrorists' Reconsidered: Arms and Conflict Dynamics in Libya and in the Sahara-Sahel Region," *European Journal on Criminal Policy and Research* 20, no. 3 (2014): 343–60.

46. Scott Shaw, "Fallout in the Sahel: The Geographic Spread of Conflict from Libya to Mali," *Canadian Foreign Policy Journal* 19, no. 2 (2013): 199–210; Stephen Zunes, "Lessons and False Lessons from Libya," *Peace Review: A Journal of Social Justice* 25, no. 4 (2013): 590–95; and Francesco Strazzari, "Libyan Arms and Regional Instability," *International Spectator: Italian Journal of International Affairs* 49, no. 3 (2014): 54–68.

47. Strazzari, "Libyan Arms and Regional Instability."

48. Major, Mölling, and Vorrath, *Train + Equip = Peace?*, 3. See also Yehudit Ronen, "Libya, the Tuareg and Mali on the Eve of the 'Arab Spring' and in Its Aftermath: An Anatomy of Changed Relations," *Journal of North African Studies* 18, no. 4 (2013): 544–59; Nathaniel D. Danjibo, "The Aftermath of the Arab Spring and Its Implications for Peace and Development in the Sahel and Sub-Saharan Africa," *Strategic Review for Southern Africa* 35, no. 2 (2013): 16–34; Georg Klute, "Post-Gaddafi Repercussions in Northern Mali," *Strategic Review* 35, no. 2 (2013): 53–67; and Strazzari, "Libyan Arms and Regional Instability."

The Role of International Courts and Tribunals in Global Environmental Governance

Steinar Andresen[*]

Tremendous progress has taken place in international environmental law and politics over the last few decades. Important achievements have also been made in many areas in terms of the increasing problem-solving effectiveness of international environmental institutions. However, some mismatch exists between the significant efforts invested and the results produced on the ground.

The main components of the international environmental governance system are multilateral environmental agreements (MEA), but a number of softer political instruments have also been established. This article focuses on the role of international courts and tribunals (ICT) in this governance system. More specifically, have they so far increased the effectiveness of international environmental governance? Currently there is no issue-specific International Environmental Court (IEC). What are the chances that one will be established? Which actors want it? Who does not? What are the respective groups' arguments? If one is established, would it enhance the effectiveness of this governance system? The article discusses these questions in relation to approaches used and insights gained from studies of the international environmental regime establishment and their effectiveness.

With this caveat, the outline of the article is as follows. First it briefly presents the main schools of thought regarding international regime establishment before discussing the concept of effectiveness. It then briefly overviews the development of

international environmental politics. That is, what are the existing dispute-settlement mechanisms? How are they used? What is the status in terms of compliance? How effective are MEAs? The answers to these questions indicate whether or not there is a need for an IEC. The article then turns to the role that some of the ICTs have played in international environmental governance, examining it through the lenses of international relations / political science. The article principally emphasizes the International Court of Justice (ICJ) and the dispute-settlement mechanisms under the Law of the Sea Convention, which is said to be particularly important for environmental issues.[1] The study does not address the use of dispute-settlement procedures in the World Trade Organization (WTO) with consequences for the environment since this area has been extensively discussed by political scientists.

Before concluding, the article turns to the prospect of a new IEC, arguments for or against such an institution, the political feasibility of establishing it, and its possible role in affecting international environmental governance. The author relies primarily on secondary sources but uses primary sources from some of the relevant cases as well.

From Regime Creation to Regime Effectiveness

In the 1970s and 1980s, international relations scholars began studying the creation of international regimes. Why did they form in some issue areas but not in others? What did it take for regimes to be established? Different schools had different answers. The following discussion offers a crude and simplified overview.

The realist school of thought emphasized the significance of a so-called hegemon or a very dominant player. For a regime to form, it had to be in the interest of a hegemon willing to bear the brunt of the costs of establishing the relevant institution. This approach closely mirrors political realities in the early postwar period when the United States generally displayed the role of hegemon in key issue areas. Creation of the North Atlantic Treaty Organization as well as the General Agreement on Tariffs and Trade fits well into this perspective. It follows that the relevant institutions had little or no independent influence. They simply mirrored the interest of the most powerful actors.[2] The gist of the realist argument is still valid in the sense that power plays a dominant role in international politics—a fact demonstrated daily in various issue areas. However, the hegemon approach is less relevant in the more recent multipolar world, and it has been documented that the hegemonic approach has limited relevance in explaining the establishment of most environmental regimes.[3]

Members of the liberal school of thought also stress the significance of states, their power, and self-interests, but they also underline the role of nonstate actors in regime creation. They maintain that, through various mechanisms, states may see that the establishment of regimes and institutions is in their best interest.[4] This school also emphasizes the significance of various forms of leadership in the process of regime

creation, arguing that these institutions are more than the sum of the interests of the major parties and may therefore have an independent effect.

Finally, the "softest" approach is the social constructivist one, which promotes the role of ideas and knowledge in the creation of international regimes. In contrast to the two other schools of thought, advocates of this approach do not consider national interest fixed since it may be shaped by the institution in question. Social constructivism is also far less state-centric than the two other approaches, underlining the significance of so-called epistemic communities in regime creation.[5]

Effectiveness studies commenced in the 1990s, and the main empirical focus has been on international environmental regimes.[6] The emphasis on the effectiveness of these institutions mirrors real-world development. When some of these organizations reached "adulthood" in the 1990s, it made sense to study whether they made a positive difference in relation to the problem they were set up to solve. Unless we know something about their effect, it does not make much sense to establish them.

Initially some analysts used goal attainment as an indicator of effectiveness. Doing so makes sense, given a consensus regarding the goal among the members of the institution and the clarity and specificity of the goal. However, because these two conditions are often not met, goal attainment is no longer used by most analysts. Consider the following examples, which illustrate the problems of applying a goal as an indicator of effectiveness. The goal of the World Health Organization is quite simple—health for all—but no easy task to measure, to put it mildly. Regarding consensus—or the lack of such—about the goal, suffice it to mention the International Whaling Commission, whose goals both pro-whaling and anti-whaling forces interpret in fundamentally different ways.

Over time, a consensus has emerged that (the dependent variable) effectiveness can be coined in terms of output, outcome, and impact.[7] Outputs deal with rules, regulations, and programs adopted by the institution in question—for example, the Kyoto Protocol within the climate regime. The more stringent and sophisticated the rules and regulations, normally the more effective the institution. Still, because rules do not always inspire compliance, output, essentially, is only potential effectiveness. We also need to know what happens on the ground. The outcome indicator, therefore, focuses on the institution's effect on the behavior of key target groups. Careful process tracing is needed to establish causality between the regime in question and behavior on the ground. For example, the massive reductions of greenhouse gas emissions in the "economies in transition" countries in the 1990s were not caused by the United Nations (UN) climate regime but by economic recession. Finally, impact deals with the direct effect of the institution on the problem at hand. To what extent has the problem been solved as a result of the regime? This indicator is the most important because it shows us the problem-solving ability of the institution in question. How-

ever, due to the high number of intervening variables and long, complex chains of causality, this indicator is difficult to use in practice.

Turning then to the question of how these concepts can be applied in relation to the study of ICTs, this does not represent much of a problem regarding the establishment of international courts. It is more problematic in studying their effectiveness. Regarding delineation of the dependent variable in terms of output, outcome, and impact, output would be the decision made by the relevant ICTs, outcome would be the effect the decision had on the behavior of the parties in question, and impact would be the wider consequences for the problem at hand. To translate directly, is the decision potentially "environmentally friendly"? Do the parties change behavior in a more positive environmental direction as a result of the court's decision? Will the relevant environmental problem be affected in a beneficial manner? The longer the causal chain, the more difficult it is to measure precisely. Here we do not go beyond the output indicator.

However, the historical and arguably still the most important task of international judicial procedures is to secure the peaceful settlement of disputes between states.[8] Thus, it is *not* the goal of ICTs to improve the environment but to resolve disputes through interpreting existing relevant laws, making dispute resolution the most relevant indicator of effectiveness. Although the use of goals as an indicator of environmental regime effectiveness is often not very meaningful, it is highly relevant for ICTs. However, we will also discuss the extent to which their decisions point in a productive direction for the environment.

International Environmental Governance: Structure and Effectiveness

This portion of the article, quite elementary for experts on international environmental governance, is written primarily for readers who are not. As noted, the backbone of the international environmental governance structure is the MEAs. They began to be established in the 1960s, and their growth has been astonishing. The most substantial growth occurred in the 1990s but has now subsided somewhat, and there are now hundreds of MEAs, mostly regional and bilateral. A convention or a treaty is a starting point, a framework in which more detailed rules are often included through one or more protocols. To become legally binding, a treaty needs to be ratified by a stipulated minimum number of countries. MEAs usually have a permanent secretariat to organize and facilitate the process of negotiations. State parties generally convene at annual or biannual conferences of the parties, the supreme decision-making body. Global environmental conventions usually have subsidiary specialized bodies dealing with such issues as scientific advice, implementation, and compliance. Many MEAs also have close ties with the United Nations Environment Program,

assisting and advising the parties in various ways. Important in terms of implementation of commitments, primarily for the developing countries within key global MEAs, is the Global Environmental Facility. Some MEAs also have a separate fund to facilitate implementation in developing countries. A number of soft-law instruments and partnerships are also established at various governance levels.

In short, multilateral environmental politics are built on a rather sophisticated and elaborate institutional framework that has evolved over time. The overall goal of this "environmental regime complex" is—separately and jointly—to improve the environment on Earth, from the local to the global level. Some people find this regime complex too fragmented and argue that it reduces its effectiveness, claiming we therefore need a World Environment Organization (WEO).[9] Since many proponents of an IEC argue that such an institution should be linked to a WEO, we will return to this point below. Nevertheless, considering this advanced institutional setup, we find that it is not self-evident that one or more specialized courts are needed. However, a key argument for establishing an IEC is that the existing system is ineffective.[10] Legal scholars base this assessment on a very narrow definition of effectiveness—dispute-settlements procedures. In line with our perspective, we will cast the net wider.

The picture is mixed regarding the problem-solving effectiveness of international environmental regimes. In the 1970s, treaty crafters confined themselves to agree that a problem existed and established an MEA to deal with it, with no further specifications. In the 1980s, targets and timetables to measure progress or the lack of such were added, and in the 1990s differential obligations and concerns about cost-effectiveness were added; subsequently, market mechanisms have also been applied.[11] Considering the growth of population and economic output over the last three decades and using a counterfactual argument, one has no doubt that the overall state of the environment would have been much worse in the absence of these MEAs.

Still, none of the major global environmental challenges have been fully solved by these regimes, and true success stories are rare. According to the 2012 edition of the United Nations Environment Programme's Global Environmental Outlook (GEO 5), *Environment for the Future We Want*, among the 90 environmental and sustainability goals of the UN, only a handful can be described as success stories, but considerable achievements have been made in quite a few of them.[12] Research confirms that there are notable variations in the achievements of the relevant MEAs.

Overall, the system for the compliance of MEAs is weak, the rules are often vague, and sanctions are hardly ever used. The major exceptions to this rule are the ozone regime, the Kyoto Protocol, and the Aarhus Convention.[13] In general, though, the level of compliance says little about the problem-solving effectiveness of the MEAs because the rules are usually too weak to address the matter. When it comes to dispute settlement in MEAs, one finds hardly any research on this issue among

international relations scholars. The most obvious explanation is that they have little significance since in practice, dispute settlement under MEAs is not utilized.[14]

The Role of Courts
in International Environmental Governance

Over the last few decades, ICTs in international politics have experienced strong growth, and specialized courts have been established in a number of issue areas. As noted, no specialized environmental court has been founded, but other courts and tribunals have tried cases in which the environment plays a role. Below we concentrate mostly on main patterns and trends without going into specific cases because doing so lies beyond our area of expertise. Compared to MEAs, these courts and tribunals play a marginal role—illustrated by the fact that two of the court processes still considered most important in this issue area are the *Trail Smelter Dispute* and the *Fur Seal Arbitration*. These date back to 1941 and 1892, respectively—long before the field came to be dominated by the MEAs. To our knowledge, no similar "milestone" court cases have taken place after the MEAs began to arise. We pay greatest attention to the ICJ as the most important general-purpose court and the law-of-the-sea tribunals since it is considered the most important court for environmental issues.[15] First we present a brief overview of some of the other relevant ICTs.

There is one exception to the generally marginal role played by ICTs in international environmental politics—the Court of Justice of the European Community. Some analysts use this institution as an illustration of the increasing importance of ICTs.[16] However, this article maintains that such a stance is a reflection of the stronger role of the "rule of law" in Europe / the European Union and not representative of the state of the art of international politics more generally. The world may not be quite as anarchic as the realists claim, but it is certainly very different for the politically and institutionally tightly knit European Community.

What about environmental issues within human rights courts and the International Criminal Court (ICC)? As to the relevance of human rights courts, most international regimes and instruments avoid the "right-base" language—probably very consciously to avoid being challenged by such courts. The latter have not had much relevance either for environmental issues or the development of international law. The same goes for the ICC. Individuals and corporations causing environmental damage have long been subject to criminal sanctions under domestic legal systems, but no similar development has taken place internationally. The Permanent Court of Arbitration (PCA), created for the maintenance of general peace, has existed for more than 100 years. It has not had much significance for environmental issue areas in that only five such cases have been brought before it, mostly between smaller Western European countries. In view of the light environmental caseload, in 2001 new opera-

tional rules for the environment were established. Interestingly, these have not been used by either the PCA or any other arbitral tribunal.[17]

The International Court of Justice

In general the environment has been fairly high on the international political agenda over the last two decades. Has this growing awareness also resulted in greater interest in interstate environmental litigation? Are states willing to give authority to an international court like the ICJ to solve their disputes? We have found no clear definition of an "environmental case" in the literature. We have defined it as a case brought before the ICJ marked by the fact that one of the objectives of the proceedings is environmental protection and that the claim of one of the applicants is (at least in part) based on international environmental law.

The caseload of the ICJ dealing with environmental issues has increased slightly, but the number of cases is very small. Interestingly, the first case with some environmental connotations occurred in 1973, just as the environment had entered the international political agenda through the 1972 Stockholm Conference. In the 1990s, there were four cases and the same number after 2000.[18] Most of them are rather low-profile issue areas, primarily between Latin American countries, so the ICJ has not played a key role in high-level, politicized environmental issue areas. The only partial exception is the recent whaling case between Australia and New Zealand versus Japan.[19] However, the first case was also a highly political issue although not primarily associated with the environment—the nuclear test case among France, Australia, and New Zealand in 1973. Despite the absence of a ruling, France stopped these tests and removed the program underground. Whether it did so because of the publicity brought about by this case or the fact that the other nuclear states also changed practice in a similar direction we do not know.

According to analysts of these cases, most rulings did not favor the parties claiming to be hurt by transboundary pollution.[20] However, some examples indicate that the ICJ process may have contributed to the initiation of negotiations and solved previously deadlocked problems. Still, most cases have not contributed much to the development of international environmental law, with one exception—the case concerning *Pulp Mills on the River Uruguay*. Argentina claimed that Uruguay had breached its obligations under the 1975 bilateral statute of the River Uruguay when it authorized and constructed two pulp mills on the river. Argentina claimed that this action would affect the quality of the water and the areas influenced by the river. This dispute is said to have been the most important environmental case decided by the ICJ until now.[21] In this matter, the ICJ was thought progressive in considering several environmental arguments in depth, particularly the need for conducting environmental impact assessments. However an important critique of this case was that the ICJ

did not apply independent scientific expertise to this highly complex scientific issue, instead basing its decision only on information from the parties.[22]

Also interesting is the whaling case—the only time when a state brought a case before the ICJ for a global public interest since it did not claim that its own rights were breached; rather, it was about the interpretation of the International Convention for the Regulation of Whaling.[23] Whether the ICJ used external scientific expertise in this highly contested issue we do not know. However, if this matter indicates a new trend for parties to involve the ICJ in more general global affairs, it may become more important and relevant over time. The ICJ, though, seems reluctant to use environmental law, especially MEAs, in its decisions although parties in some of the cases have referred to them. One interpretation may be that international environmental law is often vague due to political compromises made, and they are therefore difficult to apply. Thus, the fact that environmental law is not applied may not be due to a cautious stance by the ICJ but to a weakness of international environmental law. Attempts have been made to make the ICJ more relevant for environmental issues, but, similar to the experiences of the PCA, this effort failed. In 1993 the ICJ established a seven-member permanent environmental chamber. In a press release, the court stated that it needed the chamber in light of recent developments in international law.[24] However, the chamber was *never* used, and it was abolished in 2006.[25] The vagueness of the relevant rules may have contributed to its demise. Another explanation may be that cases are rarely "purely" environmental and that other elements are also involved. Probably most importantly, parties may find other mechanisms, such as negotiations and diplomacy, more relevant to resolve their conflicts. This interpretation is supported by the fact that parties do not utilize the dispute-settlement mechanisms of the MEAs.

Finally, as noted, only a few small and medium-sized powers use the ICJ, illustrating that major powers are not willing to accept binding adjudication that threatens their national sovereignty.[26] The only partial exception is Japan.[27] This point is illustrated by the minority of states that have accepted the ICJ's compulsory jurisdiction. Neither the United States nor most emerging economies have done so.[28]

The United Nations Convention on the Law of the Sea

The key document here is the United Nations Convention on the Law of the Sea. The treaty was opened for signature in 1982 and came into force in 1994. There are four different dispute means under the convention: the International Tribunal for the Law of the Sea (ITLOS), the ICJ, an arbitral tribunal constituted in accordance with Annex VII to the convention (from now on referred to the Arbitral Tribunal), and a special arbitral tribunal constituted in accordance with Annex VIII to the convention. The ITLOS has a number of chambers for specific functions. Between 1996

and 2014, the ITLOS and/or the Arbitral Tribunal dealt with a total of 22 cases, but according to our understanding of an environmental issue, few cases were somewhat related to environmental issues.[29] Similar to cases before the ICJ, the ones here have mainly been low-profile issue areas between small states. Consequently, neither the ITLOS nor the Arbitral Tribunal has played a significant role in high-level, politicized environmental issue areas.

In only two of the six environmental cases did the ITLOS / Arbitral Tribunal reach a ruling.[30] In the other cases, it did not issue a judgment because the tribunal claimed it lacked jurisdiction to rule on the case, the parties resolved the dispute themselves, or one of the parties withdrew the case.[31] For example, in the *Swordfish* case, the ITLOS never ruled because the parties found agreement among themselves, but it may be that the ITLOS contributed to the process to reach an agreement. The European Union and Chile had been engaged in disagreements over the swordfish fisheries in the South Pacific for a decade and did not reach an agreement before bringing the case to the ITLOS and WTO.

The most important case brought to the ITLOS is said to be the one regarding the *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area.* In this case, the Council of the International Seabed Authority requested an advisory opinion from the Seabed Dispute Chamber on the legal responsibilities and obligations of states parties to the convention with respect to the sponsorship of activities in the area.[32] The advisory opinion has resulted in a clearer understanding of the responsibility of the sponsoring state with respect to the area. Cathrin Zengerling considers the advisory opinion the clearest and most important by the ITLOS in the application and development of international environmental law.[33] The case is important because it is about both environmental protection and fair and equitable resource exploitation. In other words, it is about the sustainable management of a global commons.

Only four bilateral disputes related to environmental issues have been brought to the ITLOS / Arbitral Tribunal, including small or medium-sized countries—the same trend that we saw in the ICJ cases.[34] Based on practice until 2014, the ICJ and the tribunals under the United Nations Convention on the Law of the Sea have not played an important role in international environmental politics.

A New International Environmental Court?

Primarily two groups—nongovernmental organizations and lawyers—have argued for the establishment of an IEC, but a few other actors have also supported the idea.[35] The idea emerged at the end of the 1980s during a time when the environment was very prominent on the international political agenda. In the spirit of the "environmental enthusiasm" at the time, an international (nongovernmental) conference in

the Hague in 1989 called for a "new institutional authority" within the UN system. This body would address the problem of global warming and should be equipped with decision-making and enforcement powers. The idea went nowhere, and no UN body has since supported it.[36]

A more sustained effort was initiated in Italy, and an IEC was first proposed in 1988 by a committee in Rome. In 1989 the National Academy of Lincei, Rome, organized an international Congress on a More Efficient International Law on the Environment and Setting Up an International Court for the Environment within the United Nations. The academy set up the International Court of the Environment Foundation (ICEF), recognized in Rome in 1992 as a nonprofit foundation. It was accredited with the UN Economic and Social Council as well as some other international organizations, but it has had no practical significance and has not been accepted by any states. Since 1992 the ICEF has organized a number of conferences to further elaborate the idea of an IEC. A number of lawyers from other countries were also involved in this process. Its representatives attended the 1992 UN Conference on Environment and Development and the 2002 Johannesburg Summit. The last ICEF International Conference took place in Rome in May 2010.[37]

In 2008 another initiative was established in the United Kingdom—the International Court for the Environment (ICE). It campaigned for an IEC in the buildup to the UN Framework Convention on Climate Change (Conference of the Parties 15) in Copenhagen in 2009.[38] The core elements of an IEC as advocated by the ICE Coalition are essentially the same as those for an IEC. Another initiative in this regard was the United Nations University (UNU) *Report on International Sustainable Development Governance*, prepared for the Johannesburg Summit. More recently the International Bar Association has also become engaged in the issue. Although no influential political actors have taken this position, an interesting exception is the WTO's earlier general secretary, who has expressed support for the idea of an IEC modeled after the WTO's dispute-settlement mechanism.[39] So far no official statement of political support for an IEC has been issued by any state, but Børge Brende, the previous Norwegian minister of environment, supported the idea.[40] Linking back to the various schools of thought regarding regime creation, one finds that based on this experience, the social constructivist approach receives little support.

Let us turn to some of the arguments in favor of establishing an IEC. Perhaps the most thorough and interesting ideas have been presented in the UNU report, which asserts that states might be more willing to grant compulsory jurisdiction to a specialized rather than a universal court. Furthermore, such an IEC might be more acceptable as a judicial branch of a proposed new WEO, similar to the WTO institutional setup. The political body of the new WEO could exercise control over the IEC, just as the WTO dispute-settlement body does for the WTO panels and appellate body. Alternatively, it was suggested that a new IEC could be a part of any other

structure coordinating the existing MEAs.[41] The UNU report argues in favor of establishing some form of filter to prevent frivolous, publicity related, or politically motivated cases.[42] The authors propose a judicial branch of international environmental law that would complement existing monitoring systems, suggesting two ways of doing so with judicial review: either extending current compliance procedures through a second stage of third-party adjunction or establishing a distinct process of judicial settlement that comes into play when compliance procedures fail to resolve a case.[43]

Some of these ideas are interesting and rather "sober" as they want to coordinate a new institution closely with the existing system. However, in the concluding section we return to some basic flaws in the argument.

A new, interesting actor arguing in favor of an IEC is the International Bar Association, which includes 200 bar associations worldwide and has more than 55,000 members. For the first time, a legal organization of this size has engaged in the issue. In a report, it highlights that climate change disproportionately affects those who have contributed the least to the problem and do not have the resources to respond, adding that current laws are not sufficient to redress this imbalance. The International Bar Association applies a human rights perspective. The report recommends that until that court is established, countries should recognize the jurisdiction of the ICJ and the PCA in the Hague.[44]

What other general arguments have been presented in favor of an IEC? As mentioned above, one main point is that it is needed because current international regimes are ineffective with weak dispute-settlement procedures. Advocates of an IEC also find evidence of this deficiency in decisions from the ICJ. To a large extent, this finding is confirmed in our studies of the ICJ and ITLOS. Consequently, they argue that a special court able to hear only environmental disputes would give the environment the special attention it needs.[45] There is also a procedural critique of the existing system highlighting the lack of understanding of environmental issues among traditional "generalist" international judges.[46]

Other arguments in favor of establishing an IEC are access to nonstate actors as well as private citizens, faster resolutions of problems and disputes, lower costs of litigating international environmental disputes, better enforcement of environmental treaties, better scientific procedures, provisions to avoid forum shopping, compulsory jurisdiction, and a clear and enforceable language. In short, advocates of a new court cite the necessity of one international entity that can promote uniformity among environmental laws, both foreign and domestic.[47] Some individuals also call for the full implementation of Principle 10 of the Rio Declaration and the importance of establishing an IEC outside the "usual suspect" cities like New York, Geneva, and the Hague.[48]

Concluding Discussion

Many good arguments urge the establishment of a new IEC, but no single state in the world has supported the idea. Therefore, it will not be established in the foreseeable future. That is, the "score" in terms of political feasibility is close to nil. Some of the more interesting suggestions involve linking an IEC to the existing institutional structure. The idea of associating an IEC with a WEO, however, illustrates how far-fetched the idea is under real-world circumstances. The notion of establishing a WEO was a particularly "hot" issue in the run-up to the 2002 Johannesburg Summit. The strongest supporters were some of the European countries, but the idea has never gotten sufficient traction. Major developing countries do not want a new institution specifically designed for the environment because they prefer to concentrate on the broader sustainability issues. The United States is also against this "top-down" idea, arguing instead for the need for bottom-up approaches and competition among environmental institutions.[49] The likelihood of establishing a WEO is therefore also close to zero. Considering that this organization would be a much less intrusive body than an IEC, the situation illustrates how far the international community is from establishing such an institution.

It also seems a bit out of place in relation to the present discourse to argue for an environmental court when the broader sustainability concept has overtaken the narrower concept of environment. As we have demonstrated, it is very difficult to single out issue areas that are exclusively environmental. That may be one reason why the Environmental Chamber of the ICJ as well as a similar body of the PCA was never applied—and why the existing courts are very rarely used to solve disputes. More fundamentally, the bilateral approach of the ICJ does not fit the complex realities of environmental issues in which collective-action problems for a large number of actors are the name of the game. Essentially, courts are set up to solve disputes between two parties—not to solve the broader challenges posed by environmental problems.

It has been demonstrated that the effectiveness of the existing system is mixed, that important achievements have been made, but that difficult problems are rarely solved. MEAs are the backbone in this system, and the role of international courts is marginal. It is hard to foresee that an IEC would contribute much to enhance the effectiveness of the system or to settle disputes because most actors prefer to resolve these through political means rather than litigation. Many of the suggestions for an IEC also seem quite unrealistic, characterized more by wishful thinking than by sober calculations. We therefore tend to agree with Ole Kristian Fauchald in his conclusion that "the establishment of an international environmental court in my opinion should be far down on the list of priorities."[50]

Notes

1. Tim Stephens, *International Courts and Environmental Protection* (Cambridge, UK: Cambridge University Press, 2009).

2. John Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (1995): 5–49.

3. Oran Young and Gail Osherenko, "Testing Theories of Regime Formation: Findings from a Large-Scale Collaborative Research Project," in *Regime Theory and International Relations*, ed. Volker Rittberger et al. (Oxford, UK: Clarendon Press, 1993), 223–36.

4. Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, NJ: Princeton University Press, 1984).

5. Peter Haas, "Introduction: Epistemic Community and International Policy Coordination," *International Organization* 46 (1992): 1–35.

6. Edward Miles et al., *Environmental Regime Effectiveness: Confronting Theory with Evidence* (Cambridge, MA: MIT Press, 2002).

7. Ibid.

8. Cathrin Zengerling, *Greening International Jurisprudence: Environmental NGOs* [nongovernmental organizations] *before International Courts, Tribunals and Compliance Committees* (Leiden: Martinus Nijhoff Publishers, 2013).

9. Frank Biermann and Steffen Bauer, eds., *A World Environmental Organization: Solution or Threat for Effective International Environmental Governance?* (Aldershot, Hants, England: Ashgate, 2005).

10. Ole W. Pedersen, "An International Environmental Court and International Legalism," *Journal of Environmental Law* 24, no. 3 (2012): 547–58.

11. Steinar Andresen, Elin Boaasson, and Geir Hønneland, eds., *International Environmental Agreements* (New York: Routledge, Taylor and Francis Group, 2011).

12. United Nations Environmental Programme, Global Environmental Outlook 5 (GEO 5), *Environment for the Future We Want* (Valletta, Malta: United Nations Environmental Programme, 2012).

13. Zengerling, *Greening International Jurisprudence.*

14. Geir Ulfstein, ed., *Making Treaties Work: Human Rights, Environment and Arms Control* (Cambridge, UK: Cambridge University Press, 2007).

15. Stephens, *International Courts and Environmental Protection.*

16. Karen J. Alter, *The New Terrain of International Law: Courts, Politics, Rights* (Princeton, NJ: Princeton University Press, 2014).

17. Zengerling, *Greening International Jurisprudence.*

18. For an overview of the cases, see Zengerling, *Greening International Jurisprudence*; "Nuclear Tests Case (New Zealand v. France) (Interim Protection), Order of 23 June 1973," Summaries of Judgments, Advisory Opinions and Orders of the International Court of Justice, *ICJ Report* (1973), 88–89, http://www.icj-cij.org/docket/files/59/6117.pdf; "Nuclear Tests Case (New Zealand v. France): Judgement of 20 December 1974," Summaries of Judgments, Advisory Opinions and Orders of the International Court of Justice, *ICJ Report* (1974), http://www.icj-cij.org/docket/files/59/6161.pdf; "Request for an Examination of the Situation in Accordance with Paragraph 63 of the Court's Judgment of 20 December 1974 in the Nuclear Tests (New Zealand v. France) Case: Order of 22 September 1995," Summaries of Judgments, Advisory Opinions and Orders of the International Court of Justice, *ICJ Report* (1995), http://www.icj-cij.org/docket/files/97/7557.pdf; International Court of Justice, "Constitution of a Chamber of the Court for Environmental Matters," press release, 19 July 1993, http://www.icj-cij.org/presscom/files/7/10307.pdf; International Court of Justice, "Pulp Mills on the River Uruguay (Argentina v. Uruguay), Summary of the Judgment of 20 April 2010," press release, 20 April 2010, http://www.icj-cij.org/docket/files/135/15895.pdf; and International Court of Justice, *Declarations Recognizing the Jurisdiction of the Court as Compulsory* (Hague, the Netherlands: International Court of Justice, 2014), http://www.icj-cij.org/jurisdiction/?p1=5&p2=1&p3=3.

19. Cymie R. Payne, "Australia v. Japan: ICJ Halts Antarctic Whaling," *ASIL* [American Society of International Law] *Insights* 18, issue 9 (8 April 2014), http://www.asil.org/insights/volume/18/issue/9/australia-v-japan-icj-halts-antarctic-whaling.

20. Zengerling, *Greening International Jurisprudence*; and Stephens, *International Courts and Environmental Protection.*

21. Zengerling, *Greening International Jurisprudence*, 183.

22. James Harrison, "Reflections on the Role of International Courts and Tribunals in the Settlement of Environmental Disputes and the Development of International Environmental Law," *Journal of Environmental Law* 25, no. 3 (2013): 501–14.

23. Alan Boyle and James Harrison, "Judicial Settlement of International Environmental Disputes: Current Problems," *Journal of International Dispute Settlement* 4, no. 2 (2013): 245–76.

24. International Court of Justice, press release, 19 July 1993, 4.

25. Stephens, *International Courts and Environmental Protection.*

26. Joseph Sinde Warioba, "Monitoring Compliance with and Enforcement of Binding Decisions of International Courts," *Max Planck Yearbook of United Nations Law*, vol. 5 (London: Kluwer Law International, 2001): 41–52.

27. Whaling may be important as a matter of principle for Japan, but because it has next to no economic significance, it can hardly be considered an issue of key national interest. Moreover, Japan has since moved its scientific whaling operations elsewhere, so the ICJ decision had no practical significance.

28. Boyle and Harrison, "Judicial Settlement."

29. Other analysts cast the net wider and include prompt releases of fishing vessels. Zengerling, *Greening International Jurisprudence.*

30. The Straits of Johor Case (Malaysia v. Singapore); and Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area Case (advisory request by the International Seabed Authority).

31. The Southern Bluefin Tuna (New Zealand v. Japan, Australia v. Japan); the MOX Plant Case (Ireland v. United Kingdom); and the Swordfish Case (Chile v. the European Union).

32. The area is the seabed beyond national jurisdiction.

33. Zengerling, *Greening International Jurisprudence.*

34. Warioba, "Monitoring Compliance."

35. Pedersen, "International Environmental Court," 547.

36. Steinar Andresen and Siri Hals Butenschøn, "Norwegian Climate Policy: From Pusher to Laggard?," *International Environmental Agreements: Politics, Law and Economics* 1, no. 3 (2001): 337–56.

37. Zengerling, *Greening International Jurisprudence*, 304.

38. Pedersen, "International Environmental Court," 549–50.

39. Ole Kristian Fauchald, "Bør etableringen av en internasjonal miljødomstol være et prioritert mål?" [Should establishment of an International Environmental Court be a priority goal?] (preprint version, 2005), https://www.jus.uio.no/ior/personer/vit/olefa/dokumenter/internasjonal-miljodomstol.pdf.

40. Aasmund Willersrud, "Brende vil gi FNs miljøorgan makt" [Brende will give UN's environmental organization power], *Aftenposten*, 8 June 2004, http://www.aftenposten.no/nyheter/iriks/Brende-vil-gi-FNs-miljoorgan-makt-5592020.html; and Ole Mathismoen, "Ber om ny Brundtland-kommisjon" [Asks for New Brundtland Commission], *Aftenposten*, 14 April 2007, http://www.aftenposten.no/nyheter/iriks/Ber-om-ny-Brundtland-kommisjon-5591228.html.

41. Zengerling, *Greening International Jurisprudence*, 306.

42. Ibid., 307.

43. Ibid.

44. Will Nichols, " 'International Court on the Environment Needed for Climate Justice,' Lawyers Say," *BusinessGreen*, 22 September 2014, http://www.businessgreen.com/bg/news/2371371/international-court-on-the-environment-needed-for-climate-justice-lawyers-say.

45. Pedersen, "International Environmental Court," 550.

46. Ibid.

47. Murray Carroll, "It's High Time for an International Environmental Court," *Policy Innovations*, 24 April 2013, http://www.policyinnovations.org/ideas/innovations/data/000240.

48. Stephen Hockman, "The Case for an International Court for the Environment," *Effectius Newsletter*, issue 14 (2011), http://effectius.com/yahoo_site_admin/assets/docs/InternationalCourtForTheEnvironment _StephenHockmanQC_Effectius_Newsletter14.21260322.pdf.

49. Steinar Andresen, "Key Actors in UN Environmental Governance: Influence, Reform and Leadership," *International Environmental Agreements: Politics, Law and Environment* 7, no. 4 (2007): 457–68.

50. Fauchald, "Bør etableringen av en internasjonal miljødomstol være et prioritert mål?" (translated from the Norwegian).

The Implications of Climate Change for the Military and for Conflict Prevention, Including through Peace Missions

Shirley V. Scott, PhD[*]

Shahedul Khan

> *Climate change constitutes a serious threat to global security, an immediate risk to our national security, and make no mistake, it will impact how our military defends our country.*
>
> —President Barack Obama, 20 May 2015

People increasingly recognize that climate change needs to be included in defense and security planning. More than 50 percent of countries now incorporate specific mention of climate change in their defense policies.[1] The United States has been a leader in this regard, senior figures in the Pentagon having argued for such inclusion since at least 2007, when CNA Corporation published an influential report on climate security.[2] In the lead-up to the major climate change conference held last year in Paris, the French Ministry of Defense organized an international conference of defense ministers and senior officials on the premise that global warming "is as much a peace and security issue as an environmental issue," and follow-up events are planned.[3]

This article canvasses five potential effects of climate change for the military, relevant at both the national level and the highest level of international security cooperation: the United Nations Security Council (UNSC). Given that at a national level, one finds considerable acceptance that the military has an important role to play

---

[*]Shirley Scott is a professor in the School of Social Sciences, University of New South Wales (UNSW) Australia; Research Chair of the Australian Institute of International Affairs; and a member of the Advisory Council of the Asian Society of International Law. She is currently undertaking a project with Prof. Charlotte Ku on the potential of the United Nations Security Council contributing to the global governance of climate change. Edward Elgar will publish the volume in 2017.

Shahedul Khan served as a peacekeeper in the United Nations mission in Sudan and was appointed chief of operations in Juba, South Sudan. He is currently completing a PhD in the School of Social Sciences, UNSW Australia, on peacekeepers addressing climate change adaptation.

in helping societies prepare and adapt to climate change, increasing recognition is likely to occur at the international level of climate change adaptation as an important dimension of conflict prevention. The UNSC has already debated the security consequences of climate change but as yet has passed no resolution on the subject. This article suggests that one of the most practical and potentially useful responses to climate change by the council would be to explicitly incorporate a climate change adaptation role into the work of peace missions.

Effect on Military Installations and Equipment

Perhaps the most direct and obvious significance of climate change for the military is its impact on military infrastructure. Low-lying military installations such as naval bases are particularly susceptible to rising sea levels and intense weather events. Norfolk, Virginia, home to the US Navy's Atlantic Fleet, for example, is facing both rising sea levels and sinking ground.

Not only coastal facilities may be affected. Extreme heat may impact training, and changes to ocean buoyancy caused by melting ice may influence submarine operations.[4] The 2010 US *Quadrennial Defense Review* was the first to identify climate change as a threat to national security. The 2014 review provided for "a comprehensive assessment of all installations to assess the potential impacts of climate change on [US] missions and operational resiliency, and develop and implement plans to adapt as required."[5] The subsequent *Climate Change Adaptation Roadmap* detailed how the Department of Defense was to set about this task.[6]

The United Kingdom has sought to improve the environmental resilience of its defense infrastructure from risks such as coastal erosion or infrastructure overheating. For example, the Chinook helicopter engine has been improved to be able to perform at high temperatures. The UK's Ministry of Defence (MOD) is one of the country's largest land owners. It is MOD policy that environmental issues be fully integrated with operational and training requirements as well as with safety issues.[7] To do so, the ministry receives advice from environmental specialists, representatives from conservation organizations, MOD personnel, and expert volunteers.[8]

Reduction of the Military's Environmental Footprint

Military operations, including those by planes, tanks, and ships, involve enormous amounts of energy derived from fossil fuel sources. This fact is particularly true of the US military because of the sheer scale of its operations. During missions in Afghanistan and Iraq, it spent over $20 billion annually on air-conditioning for troops.[9] The US Department of Defense has made significant strides towards reducing its reliance on fossil fuels, thus lessening its environmental impact and its vulner-

ability from the perspective of energy security. The US military has invested in en-
ergy-saving activities and in the adoption of new sources of energy such as solar and
wind.[10]

The UK MOD has a *Sustainable Development Strategy* as a *Sub-strategy of the
Strategy for Defence, 2011–2030*.[11] This document articulates two sustainable devel-
opment principles: first, that "defence must be resilient to current and future environ-
mental, social and economic threats (adaptation)"; and second, that "defence must
realise the positive and minimise the negative impacts that defence activities can have
on the environment, people and the economy in the UK and overseas (mitigation)."[12]
The strategy outlines objectives for minimizing these effects, including cutting green-
house gas emissions from estate and business-related transport, reducing reliance on
fossil fuels for operational energy, and decreasing the number of business travel
flights.[13] Italy has significantly lowered its dependence on fossil fuels; it now has 1.5
million square meters of photovoltaic panels, and its navy is carrying out trials of
biofuels compatible with the North Atlantic Treaty Organization's fuel specifica-
tions.[14]

In 2012 the United Nations Environment Programme (UNEP) issued policy
recommendations designed to improve the environmental performance of peace-
keeping operations, as well as to capitalize on the peace-building potential of natural
resources "while minimizing their possible contribution to conflict relapse and inse-
curity."[15] UNEP subsequently assisted the UN Institute for Training and Research
and the International Institute for Sustainable Development to devise three e-training
modules that would support UN peace missions in better managing the environment
and natural resources.[16]

Factoring Climate Change into Planning by Military Strategists

Although the preeminent global military power is feeling pressure to reduce its
carbon footprint, the military is generally less likely to play a major role in mitigating
climate change than in allaying conflicts related to climate change. One of the key
messages of individuals who emphasize the security-defense nexus is that the conse-
quences of climate change are altering geostrategic realities with significant security
implications and with necessary consequences for military operations and planning.

One recognizes growing awareness of the potential for geostrategic tensions in
Antarctica and even more so, particularly in the midterm, in the Arctic as ice recedes
and a new ocean appears; furthermore, increasing competition exists for the resources
below. Experts now believe that the Arctic may have ice-free summers before mid-
century; there are tensions over "shipping routes and rights of passage through spe-
cific waterways that some countries argue are sovereign and others view as interna-

tional shipping lanes"; and concerns are intensifying among Arctic Council members over hydrocarbon fields.[17]

It has been notoriously difficult for intelligence communities to predict historic events such as Pearl Harbor or 9/11; consequently, military planners must often proceed without full information.[18] Unsurprisingly, then, in military, policy, and political planning circles, one finds widespread acceptance that climate variability and related developments—including an increase in extreme weather events and rising sea levels—will affect future conflict.

President Obama has declared that the consequences of climate change accelerate the risk of instability and conflict, increase competition for resources, produce climate-change refugees as a result of rising sea levels, and have the potential for mass migration.[19] People now widely believe that severe drought helped create the instability in Nigeria exploited by the Boko Haram and that crop failures and high food prices fuelled the civil unrest in Syria that descended into civil war.[20]

Worth noting is the fact that scholars remain divided on the question of whether it is possible to prove a causal relationship between climate change and conflict. Debate on the issue has been a subset of a broader scholarly discussion of whether it is useful to think in terms of environmental security. For example, Michael Brzoska and Christiane Fröhlich have emphasized the difficulty of proving a causal link between climate change and mass migration.[21] Brzoska has concluded, somewhat cynically, that rather than constitute a basis for any fundamental shift in military planning, climate change serves a justificatory role for militaries to continue along their established paths and to seek additional resources for doing so.[22]

The Military's Response to
Threats to Human Security and Natural Disasters

Climate change means that more demands will likely be placed on the military for activities beyond war: in particular for humanitarian responses to natural disasters and for climate change adaptation. The Royal Moroccan Armed Forces are already heavily involved in rescue and assistance operations to populations affected by extreme climate events, both domestically and internationally.[23] Morocco has signed an agreement with Spain and France allowing for exchange of best practices and greater interoperability in responding to natural disasters.[24] A greater role in humanitarian disaster response is evident even for the armed forces of a developed country such as Australia. Climate change is causing an increase in the intensity of floods, bushfires, droughts, and extreme heat—typically summer phenomena—so Australian Defence Force planning includes having force elements ready to be deployed at short notice in response to natural disasters in Australia.[25]

In future military operations, military information and intelligence, surveillance, and reconnaissance (ISR) capabilities are set to have a far greater impact on humanitarian assistance and disaster-relief activities. ISR assists civil agencies as well as government and nongovernmental organizations in assessing the nature and quantity of supplies needed, based on the number of victims, available resources, and determining priorities.[26] During the Haiti earthquake on 12 January 2010, the US military received orders to assist the disaster-relief efforts of the US Agency for International Development.[27] Navy P-3 aircraft, RQ-4 Global Hawk remotely piloted aerial vehicles, and satellites were used to collect images that helped determine the status of roads, bridges, seaports, humanitarian needs, and routes by which to transport relief supplies.[28]

The military will probably play an enhanced role in responding to other climate-related threats to human security, such as higher rates of infectious diseases transmitted by insect vectors and through contaminated water. At an international level, military assistance has proved critical in containing the spread of the Ebola virus. Approximately 5,000 military personnel from the United States, United Kingdom, China, Canada, France, and Germany were deployed to the virus-affected areas.[29] United States Africa Command was formed following President Obama's announcement on 16 September 2014 that sought to reduce the impact of the Ebola outbreak on the society and economy of the region. A similar effort was initiated by the UK government through Operation Gritrock.[30] On 18 September 2014, the UNSC declared the Ebola outbreak "a threat to international peace and security" and adopted Resolution 2177.[31] Afterward, the General Assembly unanimously adopted Resolution 69/1, and on 19 September 2014 the UN Mission for Ebola Emergency Response was established, ending on 31 July 2015. It had the unique mission of engaging the military to act in accordance with other international organizations in humanitarian assistance. The United Nations Humanitarian Air Service, the World Food Programme, the UN Mission in Liberia, and the UN Department for Field Support cooperated in the provision of air services, medical screening, and so on.

The Military's Contribution to Conflict Prevention, Including through Climate Change Adaptation

The second peacetime climate-change-related activity in which militaries are increasingly being deployed is climate change adaptation. At a national level, for example, the armed forces of Chad participate in programs such as (1) reforestation projects that combat environmental threats caused in part by the desert moving 150 kilometers south over recent decades and (2) Lake Chad shrinking by almost 90 percent.[32] The Republic of Haiti has created a defense force that contributes to climate change adaptation, construction of resilient infrastructure, and emergency re-

sponse to natural disasters. Perhaps the core concern for planners working on climate security is "not in direct links between climate and violent conflict, but in the ability of climate change to disrupt those systems that underlie stability and human security more generally."[33] In other words, one must emphasize building resilience, not only of natural systems but also of governance and institutional structures and systems, including most particularly those at the local level.

This initiative ties in closely with the UN's concentration over the last decade on initiatives aimed at conflict prevention. Given the interrelationship between the activities understood to reduce risk of conflict and those needed for climate resilience, UN Resolution 1625 (2005) on conflict prevention offers a basis for building an explicit role for the UNSC in climate change adaptation. Paragraph 3(b), for example, requests the secretary-general to "assist countries at risk of armed conflict in performing strategic conflict risk assessments, in implementing the measures agreed by the concerned countries, in enhancing national dispute management capacities, and in addressing the root causes of armed conflict."[34]

Given the importance of climate change adaptation as an aspect of conflict prevention, one operational means by which to realize this end would be through peacekeeping and peace building—activities that involve both military and nonmilitary personnel. During the Cold War, peacekeeping was visualized as a "temporary activity, taking place between a ceasefire and a political settlement, and designed to help conflict parties to gain the trust and confidence necessary for a peace accord."[35]

Since the end of the Cold War, however, peacekeeping has become multidimensional and can include monitoring, rebuilding, disarmament, and capacity-building activities to create a stable and sustainable environment for civilians.[36] Interestingly, in the report *An Agenda for Peace*, the late UN secretary-general Boutros Boutros-Ghali defined peace building as an "action to identify and support structures, which will tend to strengthen and solidify peace in order to avoid a relapse into conflict."[37] Hence, over the years the concept of peacekeeping has been intertwined with peace building, both of which emphasize capacity and institution building—the very tools that are recognized as important to climate change adaptation.

Current peace building and peacekeeping incorporate activities of direct relevance to climate change adaptation. The United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA) was established on 10 April 2014 after a cease-fire between the Seleka rebels and "antibalaka" militias. With the support of UNEP, the Environmental Cooperation for Peacebuilding—the organization that "offers risk assessments, technical advice, targeted training, and a neutral platform for stakeholder dialogue"—conducted a study on MINUSCA.[38] It found that the mission could be the largest energy consumer in the Central African Republic, triggering tension in the region. UNEP therefore recommended a range of energy efficiency measures by which to improve the management

of liquid and hazardous waste.[39] It helped MINUSCA adapt better to its local environment and frame policy objectives to eliminate the exploitation and trafficking of natural resources.

The United Nations Multidimensional Integrated Stabilization Mission in Mali is the first UN stabilization mission that received a formal mandate from the UNSC to manage camp design, waste management, water use, and energy generation. In 2014 at the request of Martin Kobler, special representative of the secretary-general, UNEP conducted a ground-breaking study of violence in the Democratic Republic of Congo. The study surmised that the main reason for crises in the region shifted from political insurgency to smuggling and laundering operations. Estimating the value of exploitation at US $1.24 billion each year, the report helped reshape the mandate of the United Nations Organization Stabilization Mission in the Democratic Republic of Congo's (MONUSCO) through Security Council Resolution 2211 on March 2015. MONUSCO now concentrates on environmental crimes, especially those involving criminal networks.[40]

Next Steps? More Activities of Peacekeepers and Peace Builders

Working in conjunction with other agencies and local civil society, peacekeeping and peace-building missions could possibly contribute much more to climate change adaptation. By way of example, the latter could be included as a topic in the predeployment training of UN personnel alongside existing subjects such as gender, human rights, child protection, and HIV/AIDS. Similarly, peacekeeping operations regularly submit reports from the field stations to UN headquarters in New York. It would be worth considering whether this reporting system could include data relevant to planning climate change adaptation efforts and building resilience.

Peacekeepers usually receive a mandate to reestablish democratic values and good governance, including capacity building and extensive training activities for members of civil society, scholars, ex-combatants, and members of the security services. Such mandates could conceivably incorporate the development of policies on the environment, internally displaced people, and natural resources—issues that may cause a relapse into conflict.

During a postconflict period, victim states fall short of knowledge and technical know-how to foresee the complex interconnection between climate change and refugees. Following the mass genocide in 1994, the government of Rwanda had to resettle more than two million refugees. Many of these distressed populations were forced to leave Rwanda for the neighboring Great Lake regions of Africa, including the Democratic Republic of Congo and Tanzania. Many of these refugees were living outside Rwanda for years.[41] On their return, considerable numbers were resettled in marshy areas, on steep hillsides, and even in protected areas—unfortunately contrib-

uting to an ecological disaster. If equipped with the appropriate knowledge and skills, peacekeepers could assist postconflict governments to ensure that environmental considerations are integral to policy planning.

Mitigating complex intrastate tension demands building the capacity of different local and international institutions. Building capacity of the local community and organizations is regarded as a core peacekeeping activity. The UN Police (UNPOL) are heavily engaged in reforming and restructuring existing institutions through integrating individual personnel, organizational units, and broader institutions. During these phases, "gender," "human rights," and "corruption" are fundamental policy principles. Integrating climate change adaptation into the policy framework could potentially strengthen the UN's conflict-resolution strategy in fragile states.[42]

Community policing has been a success story for UNPOL. Through this activity, the UN has generated public trust towards police, and it was effective in Bosnia and Herzegovina, helping link different communities and the police.[43] It was also successful in capacity building and integration activities to improve the overall status of human rights.[44] UNPOL's continuing community police activities could incorporate climate sensitization programs to raise awareness of the issue.

The devastation of climate change and its aftermath should be taken into consideration during disarmament, demobilization, and reintegration. The experience of Sierra Leone shows that not doing so may prolong human suffering. After the civil war in Sierra Leone, approximately 70,000 rebels were disarmed and demobilized.[45] The reintegration process proved extremely challenging and resulted in unemployment, which—followed by postwar trauma and distress—instigated the youth and ex-combatants to engage in activities such as drug trafficking, smuggling, and deforesting.[46] This rapid pace of deforestation destroyed huge watersheds, damaging the overall environment. Today, Sierra Leone has only 5 percent of the forest it once had.[47] If the UN had taken climate change and related environmental concerns into account before the reintegration process took place, the situation might have been different.

Maintaining law and order is a critical role for peacekeepers, especially for UNPOL units.[48] Their roles in conflict regions are multifarious, including protecting civilians through maintaining law and order, promoting human rights, safeguarding human security, reducing violence during the electoral process, monitoring and facilitating mobilization and reintegration, and training the local population and indigenous forces.[49] Members of UNPOL regularly organize training for local police forces to promote professionalism as an integral segment of security sector reform.[50] They also promote human security, improve the quality of local policing, and build capacity to perform security duties.[51] Inclusion of climate change adaptation in UNPOL's "cohesive strategic guidance framework" could potentially strengthen efforts towards sustainable peace and security.[52]

Council Debates on Climate Change to Date

The UNSC is no stranger to the concept of climate security. During its presidency of the council in 2007, the United Kingdom initiated a debate "exploring the relationship between energy, security and climate."[53] Much of the debate concerned whether the UNSC was the appropriate forum in which to address climate change. The European Union and a number of Pacific small island developing states (SIDS) agreed that the UNSC could play an important role in addressing climate change although there were differences in the extent to which they perceived a useful role for the council. The United Kingdom stressed the need to utilize the debate as a forum to raise awareness; France and Germany emphasized active prevention; and the SIDS insisted that the UNSC become more involved in climate change since it posed a direct threat to international peace and security. Russia, China, and the Group of 77 coalition of developing countries argued that the General Assembly, Economic and Social Council, and the United Nations Framework Convention on Climate Change would be more appropriate forums in which to address climate change.

In 2009, following a campaign by the SIDS, the General Assembly passed Resolution 63/281, emphasizing its deep concern about the adverse effects of climate change and its security implications. Furthermore, it "invited the relevant organs of the United Nations, as appropriate and within their respective mandates, to intensify their efforts in considering and addressing climate change, including its possible security implications." A subsequent report by the secretary-general identified climate change as a "threat multiplier."[54] A 2011 debate again met with resistance from Russia, China, and the Group of 77 although the United States was this time far more positively inclined towards the issue. According to Susan Rice, US ambassador to the UN, "It is past time for the Security Council to come into the 21st century and assume our core responsibilities."[55] At the closing of the debate, a presidential statement of the Security Council expressed grave concern that in the long run, threats to international peace and security might be aggravated by climate change.[56]

A 2013 Arria-Formula Meeting was cosponsored by the United Kingdom and Pakistan; another, in 2015, was cosponsored by Spain and Malaysia. Emphasis remained on the role of climate change as a threat multiplier. Members of the SIDS emphasized sea-level rise and its effect on their citizens. A number of African G77 states argued that "desertification and heat waves created economic and social disruption that creates a breeding ground for recruitment into radical organizations, such as Boko Haram."[57] The subject arose again when in July 2015 New Zealand hosted a debate on peace and security challenges facing SIDS.

Conclusion

The military cannot avoid addressing climate change and, indeed, is already doing so. The relationship between military activities and climate change is bidirectional. On the one hand, the military may be part of the solution in responding to climate change while on the other hand, the military may itself exacerbate the problem. In many cases, the military is the only organization able to respond on the scale necessary, for example, to natural disasters rendered more frequent by climate change and to instigate postconflict development that is environmentally sustainable. At the same time, the traditional role of the military is affected through opening up potential new theaters of conflict. The military must tackle new challenges yet at the same time reduce its own environmental footprint and adapt to the climate change threats to its own infrastructure and modes of operation.

Notes

1. Andrew Holland and Xander Vagg, *The Global Security Defense Index on Climate Change: National Security Perspectives on Climate Change from around the World* (Washington, DC: American Security Project, 21 March 2013), http://americansecurityproject.org/ASP%20Reports/Ref%200121%20-%20Global%20Security%20Defense%20Index%20P-Results.pdf.

2. CNA Corporation, *National Security and the Threat of Climate Change* (Alexandria, VA: CNA Corporation, [2007]), https://www.cna.org/cna_files/pdf/national%20security%20and%20the%20threat%20of%20climate%20change.pdf.

3. Ministere de la Defense, "Conférence Climat et Défense: quels enjeux?," 14 October 2015, 3, http://www.defense.gouv.fr/dgris/la-dgris/evenements/conference-climat-et-defense-quels-enjeux-14-octobre-2015.

4. Jane Holloway, Michael Durant Thomas, and Cheryl Durrant, "Strategic Military Geography: Climate Change Adaptation and the Military," in *Handbook of Climate Change Adaptation*, ed. Walter Leal Filho (Berlin: Springer-Verlag, 2015), 506.

5. US Department of Defense, *Quadrennial Defense Review, 2014* (Washington, DC: Department of Defense, 2014), 25, http://www.defense.gov/Portals/1/features/defenseReviews/QDR/2014_Quadrennial_Defense_Review.pdf.

6. US Department of Defense, *2014 Climate Change Adaptation Roadmap* (Washington, DC: Department of Defense, 2014), http://ppec.asme.org/wp-content/uploads/2014/10/CCARprint.pdf.

7. "Defence Infrastructure Organisation Estate and Sustainable Development," Ministry of Defence, 21 June 2013, https://www.gov.uk/guidance/defence-infrastructure-organisation-estate-and-sustainable-development#adaptation-to-the-impacts-of-climate-change-on-the-ministry-of-defence-estate%29.

8. Ibid.

9. "Among the Costs of War: Billions a Year in A.C.?," National Public Radio, 25 June 2011, http://www.npr.org/2011/06/25/137414737/among-the-costs-of-war-20b-in-air-conditioning.

10. Vicki Norberg-Bohm, "Creating Incentives for Environmentally Enhancing Technological Change: Lessons from 30 Years of US Energy Technology Policy," *Technological Forecasting and Social Change* 65, no. 2 (2010): 125–48.

11. Ministry of Defence, *Sustainable Development Strategy: A Sub-strategy of the Strategy for Defence, 2011–2030*, accessed 5 May 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32729/20110527SDStrategyPUBLISHED.pdf.

12. "Our Energy Use," Ministry of Defence, accessed 5 May 2016, https://www.gov.uk/government /organisations/ministry-of-defence/about/our-energy-use.

13. Ministry of Defence, *Sustainable Development Strategy*, 2–3.

14. Ministere de la Defense, "Conférence Climat et Défense," 21.

15. United Nations Environment Programme, *Greening the Blue Helmets: Environment, Natural Resources and UN Peacekeeping Operations* (Nairobi, Kenya: UNEP, May 2012), 16, http://www.un.org/en/peacekeeping /publications/UNEP_greening_blue_helmets.pdf.

16. United Nations Environment Programme, *Special Issue Newsletter: Natural Resources and Peacebuilding* (Nairobi, Kenya: UNEP, April 2014), 17, http://www.un.org/en/peacebuilding/pbso/pdf/PBSO_UNEP _NRM&Peacebuilding_newsletter.pdf.

17. Holloway, Thomas, and Durrant, "Strategic Military Geography," 508.

18. Chad Michael Briggs, "Climate Security, Risk Assessment and Military Planning," *International Affairs* 88, no. 5 (2012): 1055.

19. "President Obama Delivers the Keynote Address at the US Coast Guard Academy Commencement," YouTube video, 2:55:40, 20 May 2015, https://www.youtube.com/watch?t=7328&v=sFgrrsTIRzM.

20. Ibid.

21. Michael Brzoska and Christiane Fröhlich, "Climate Change, Migration and Violent Conflict: Vulnerabilities, Pathways and Adaptation Strategies," *Migration and Development* 5, no. 2 (2016): 190–210, doi: 10.1080/21632324.2015.1022973.

22. Michael Brzoska, "Climate Change and Military Planning," *International Journal of Climate Change Strategies and Management* 7, no. 2 (2015): 172–90.

23. Ministere de la Defense, "Conférence Climat et Défense," 19.

24. Ibid.

25. Anthony Press, Anthony Bergin, and Eliza Garnsey, *Heavy Weather: Climate and the Australian Defence Force*, Special Report, issue 49 (Barton: Australian Strategic Policy Institute, March 2013), 19, https:// www.aspi.org.au/publications/special-report-issue-49-heavy-weather-climate-and-the-australian-defence -force/SR49_heavy_weather.pdf.

26. Mirielle M. Petitjean, "Intelligence Support to Disaster Relief and Humanitarian Assistance," *Intelligencer: Journal of U.S. Intelligence Studies* 19, no. 3 (2013): 57–60.

27. Gary Cecchine et al., *The U.S. Military Response to the 2010 Haiti Earthquake: Considerations for Army Leaders* (Santa Monica, CA: RAND Corporation, 2013), ix, http://www.rand.org/content/dam/rand/pubs /research_reports/RR300/RR304/RAND_RR304.pdf.

28. Gen Douglas M. Fraser and Maj Wendell S. Hertzelle, "Haiti Relief: An International Effort Enabled through Air, Space, and Cyberspace," *Air and Space Power Journal* 24, no. 4 (Winter 2010): 9.

29. "Foreign Military Response Crucial to Ebola Crisis," London School of Hygiene & Tropical Medicine, 26 October 2015, http://www.lshtm.ac.uk/newsevents/news/2015/foreign_military_response_crucial _to_ebola.html.

30. Adam Kamradt-Scott et al., *Saving Lives: The Civil-Military Response to the 2014 Ebola Outbreak in West Africa*, Interim Report (Sydney: University of Sydney, August 2015), 13, http://sydney.edu.au/mbi /PDFs/saving-lives.pdf.

31. United Nations Security Council, S/RES/2177 (2014), Resolution 2177 (2014), 18 September 2014, [1], http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2177(2014).

32. Ministere de la Defense, "Conférence Climat et Défense," 15.

33. Briggs, "Climate Security," 1054.

34. United Nations Security Council, S/RES/1625 (2005), Resolution 1625 (2005), 14 September 2005, 2, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D /CPR%20S%20RES%201625.pdf.

35. Silke Weinlich, *The UN Secretariat's Influence on the Evolution of Peacekeeping* (Basingstoke, Hampshire: Palgrave Macmillan, 2014), 22.

36. Ronald Hatto, "From Peacekeeping to Peacebuilding: The Evolution of the Role of the United Nations in Peace Operations," *International Review of the Red Cross* 95, no. 891 (2013): 495–515, doi: 10.1017/S1816383114000277.

37. Boutros Boutros-Ghali, "Report of the UN Secretary-General: 'Agenda for Peace,'" Council on Foreign Relations, 17 June 1992, http://www.cfr.org/peacekeeping/report-un-secretary-general-agenda-peace/p23439.

38. "Environmental Cooperation for Peacebuilding," United Nations Environment Programme, accessed 5 May 2016, http://www.unep.org/disastersandconflicts/Introduction/ECP/whatisecp/tabid/105949/Default.aspx.

39. United Nations Environment Programme, *Addressing the Role of Natural Resources in Conflict and Peacebuilding: A Summary of Progress from UNEP's Environmental Cooperation for Peacebuilding Programme, 2008–2015* (Nairobi, Kenya: UNEP, October 2015), 30, http://postconflict.unep.ch/publications/ECP/ECP_progress_report_2015.pdf.

40. Ibid., 32.

41. Gérard Prunier, *The Rwanda Crisis: History of a Genocide* (New York: Columbia University Press, 1995).

42. Ibid., 8, 9.

43. Dusko Vejnovic and Velibor Lalic, "Community Policing in a Changing World: A Case Study of Bosnia and Herzegovina," *Police Practice and Research: An International Journal* 6, no. 4 (2005): 363–73, doi: 10.1080/15614260500293994.

44. Gemma Collantes Celador, "Becoming 'European' through Police Reform: A Successful Strategy in Bosnia and Herzegovina?," *Crime, Law and Social Change* 51, no. 2 (2009): 231–42.

45. Mark Malan et al., *Sierra Leone: Building the Road to Recovery*, ISS Monograph Series, no. 80 (Pretoria: Institute for Security Studies, 2003), 170.

46. John Williamson, "The Disarmament, Demobilization and Reintegration of Child Soldiers: Social and Psychological Transformation in Sierra Leone," *Intervention* 4, no. 3 (2006): 185–205.

47. Melissa Leach and Ian Scoones, "Carbon Forestry in West Africa: The Politics of Models, Measures and Verification Processes," *Global Environmental Change* 23, no. 5 (2013): 957–67.

48. Charles T. Call and William Stanley, "Protecting the People: Public Security Choices after Civil Wars," *Global Governance* 7, no. 2 (2001): 151–72.

49. Lise Morjé Howard, *UN Peacekeeping in Civil Wars* (Cambridge, UK: Cambridge University Press, 2008), 80, 156, 164.

50. Victoria Holt and Glyn Taylor with Max Kelly, *Protecting Civilians in the Context of UN Peacekeeping Operations: Successes, Setbacks and Remaining Challenges* (New York: United Nations Department of Peacekeeping Operations and the Office for the Coordination of Humanitarian Affairs, 2009), https://docs.unocha.org/sites/dms/Documents/Protecting%20Civilians%20in%20the%20Context%20of%20UN%20Peacekeeping%20Operations.pdf.

51. Chuck Call and Michael Barnett, "Looking for a Few Good Cops: Peacekeeping, Peacebuilding and CIVPOL," *International Peacekeeping* 6, no. 4 (1999): 43–68, doi: 10.1080/13533319908413798.

52. United Nations, *United Nations Police in Peacekeeping Operations and Special Political Missions* (New York: United Nations, Department of Peacekeeping Operations, Department of Field Support, 1 February 2014), 4, http://www.un.org/en/peacekeeping/sites/police/documents/Policy.pdf.

53. "Security Council Holds First-Ever Debate on Impact of Climate Change on Peace, Security, Hearing over 50 Speakers," press release, United Nations, 17 April 2007, http://www.un.org/press/en/2007/sc9000.doc.htm.

54. "Security Council, in Statement, Says 'Contextual Information' on Possible Security Implications of Climate Change Important When Climate Impacts Drive Conflict," United Nations, 20 July 2011, http://www.un.org/press/en/2011/sc10332.doc.htm; and United Nations General Assembly, *Climate Change and Its Possible Security Implications: Report of the Secretary-General*, A/64/350, 11 September 2009, 2, http://www.refworld.org/docid/4ad5e6380.html.

55. "Remarks by Ambassador Susan E. Rice, U.S. Permanent Representative to the United Nations, at a Security Council Session on the Impact of Climate Change on the Maintenance of International Peace and Security," United States Mission to the United Nations, 20 July 2011, http://usun.state.gov/remarks/5111.

56. Dane Warren, *Climate Change and International Peace and Security: Possible Roles for the U.N. Security Council in Addressing Climate Change* (New York: Sabin Center for Climate Change Law, Columbia Law School, July 2015), 5.

57. Ibid.