ASPJ–Africa and Francophonie 4th Quarter 2017

ASPJ–Afrique et Francophonie 4^{e} Trimestre 2017

ASPJ Africa and Francophonie

4th Quarter 2017 Volume 8, No. 4

Countering Insurgency and the Myth of "The Cause"
Daniel G. Cox, PhD
Alex Ryan, PhD

Irrational Rationality of Terrorism
Robert Nalbandov, PhD

Engaging Non-state Security Providers
Whither the Rule of Law?
Timothy Donais, PhD

China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities
Emilio Iasiello

Operationalizing Protection of Civilians in NATO Operations
Marla B. Keenan
Alexander Beadle

AIR UNIVERSITY
THE INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE

AIM HIGH . . . FLY-FIGHT-WIN

AIR & SPACE POWER JOURNAL

Chief of Staff, US Air Force
Gen David L. Goldfein

Commander, Air Education and Training Command
Lt Gen Darryl Roberson

Commander and President, Air University
Lt Gen Steven L. Kwast

Commander, LeMay Center for Doctrine Development and Education
Maj Gen Michael D. Rothstein

Director, Air University Press
Dr. Ernest Allan Rockwell

Editor
Rémy M. Mauduit

Megan N. Hoehn, *Editorial Assistant*
Nedra O. Looney, *Prepress Production Manager*
Daniel M. Armstrong, *Illustrator*
L. Susan Fair, *Illustrator*

The *Air and Space Power Journal* (ISSN 1931-728X), published quarterly, is the professional journal of the United States Air Force. It is designed to serve as an open forum for the presentation and stimulation of innovative thinking on military doctrine, strategy, force structure, readiness, and other matters of national defense. The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Articles in this edition may be reproduced in whole or in part without permission. If they are reproduced, the *Air & Space Power Journal* requests a courtesy line.

http://www.af.mil

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

http://www.au.af.mil

ASPJ–Africa and Francophonie
600 Chennault Circle
Maxwell AFB AL 36112-6026
USA
Fax: 1 (334) 953-1645
e-mail: aspj.french@us.af.mil

Visit *Air and Space Power Journal* online
at http://www.airuniversity.af.mil/ASPJ/

ASPJ Africa and Francophonie

4th Quarter 2017 Volume 8, No. 4

Editor's Picks

China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities; Countering Insurgency and the Myth of "The Cause;" Engaging Non-state Security Providers: Whither the Rule of Law?; Irrational Rationality of Terrorism; and Operationalizing Protection of Civilians in NATO Operations 2
Rémy M. Mauduit

Articles

Countering Insurgency and the Myth of "The Cause" 5
Daniel G. Cox, PhD
Alex Ryan, PhD

Irrational Rationality of Terrorism. 24
Robert Nalbandov, PhD

Engaging Non-state Security Providers
Whither the Rule of Law? 39
Timothy Donais, PhD

China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities 56
Emilio Iasiello

Operationalizing Protection of Civilians in NATO Operations 78
Marla B. Keenan
Alexander Beadle

Editor's picks

China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities; Countering Insurgency and the Myth of "The Cause;" Engaging Non-state Security Providers: Whither the Rule of Law?; Irrational Rationality of Terrorism; and Operationalizing Protection of Civilians in NATO Operations

It is possible for an insurgency to develop from a single cause, for the insurgents to identify and communicate this unifying cause to the population, and for the insurgents to remain steadfastly focused even as counterinsurgents undermine their organization and redress the cause, posit Dr. Daniel Cox and Dr. Alex Ryan in *Countering Insurgency and the Myth of 'The Cause.'* But often the case is that there is no *single* cause, rather that popular support is mobilized by appealing to multiple motivations, and that by the time counterinsurgents resolve the initial grievance, the insurgency has found alternative justifications to mobilize popular support. Since insurgent leadership is often competent and adaptive, it would be wise to consider the latter scenario against any counterinsurgency strategy. Yet, even when this is acknowledged in the counterinsurgency literature, the theory is remarkably silent how this affects the choice of operational approach. Cox and Ryan address this gap and offer a framework for more accurately mapping, understanding, anticipating, and addressing the multiple causes that draw adherents to insurgency and allow for its perpetuation.

Dr. Robert Nalbandov deals with the ontological problem of applying the rational choice frameworks to the study of terrorism in *Irrational Rationality of Terrorism*. He tests the application of the rational choice to "old" (before the end of the Cold War) and "new" (after the end of the Cold War) iterations of terrorism. He starts with analyzing the fundamentals of rationality and applies it at two levels—the individual (actors) and group (collective)—via two outlooks: tactical (short-term) and strategic (long-term). The main argument of the article is that, while old iterations of terrorism can be explained by the rational choice theory, new iterations of terrorism represent a substantial departure from rationality.

The primacy of the rule of law has long been seen as one of the essential principles of security sector reform (SSR) programming, and part of the larger gospel of SSR is that the accountability of security providers is best guaranteed by embedding security governance within a rule of law framework. In *Engaging Non-state Security Providers: Whither the Rule of Law?*, Dr. Timothy Donais argues that acknowledging the reality of nonstate security provision, however, presents a challenge to thinking about SSR as merely the extension of the rule of law into the security realm—in large part because whatever legitimacy nonstate security providers possess tends to be grounded in *extralegal* foundations. This paper—more conceptual than empirical in its approach—considers the implications of hybrid forms of security governance for thinking about the relationship between SSR and rule of law promotion and argues that the rule of law still provides a useful source of strategic direction for SSR programming.

In *China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities*, Mr. Emilio Iasiello affirms that China is engaged in longstanding cyber espionage against the United States, as well as other nations, to collect sensitive public and private information in support of national objectives laid out in its 12th Five-Year Plan. Foreign governments, citing China's malfeasance, have rebuked these activities—a claim vehemently denied by Beijing. In response, China is leveraging the *Three Warfares*, an integrated three-prong information warfare strategy, to combat these accusations by leveraging media, legal, and psychological components designed to influence the international community. While the United States has threatened the imposition of economic sanctions, Beijing has successfully parried consequential actions by arresting US-identified hackers, thereby demonstrating the regime's commitment toward preserving a stable and peaceful cyberspace. These interrelated *Three Warfares* disciplines have targeted the cognitive processes of the US leadership, as well as the international public's perception of China as a global threat, thereby successfully forestalling the implementation of any effective punitive or economic deterrence strategy, including the imposition of cyber sanctions.

In *Operationalizing Protection of Civilians in NATO Operations*, Ms. Marla Keenan and Mr. Alexander Beadle contend that though NATO and other military forces increasingly recognize protection of civilians as a key objective in their operations, implementation remains challenging. To effectively provide such protection, the military force must understand the threats that exist and match capabilities to counter those threats. The authors strongly believe that military planners need a more formal structure to conceptualize physical protection, and herein outline "The Protection Ladder" as a tool for military planners and leaders to explain the legal obligations and additional operational capabilities necessary for civilian protection. The article offers practical suggestions on how civilian protection can be effectively addressed before, during, and after military operations. NATO should develop its protection capabilities, because future mission success depends upon it.

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

Countering Insurgency and the Myth of "The Cause"

Daniel G. Cox, PhD[*]
Alex Ryan, PhD[**]

There is much already written on the importance of winning "hearts and minds" and how this relates to the insurgent cause.[1] However, most works on the causes of insurgency tends to focus on the spark that ignited the insurgency. That is, the stated list of issues, grievances, or indeed insults, that engaged the hearts and minds of the population sufficiently to motivate them to rebel. Crisis events and initial grievances may serve as a catalyst for the mobilization of an insurgent movement; however, it is often discovered in retrospect that underlying societal tensions fomented rebellion before and after the seemingly critical spark event. In fact, successful insurgents continue to identify and leverage underlying tensions in a society as part of their cause to further the movement and expand participation. In many cases, multiple tensions and propensities fueling the insurgency overlap and intertwine with one another, weaving a complex web that confuses and deceives both academic and military attempts to determine appropriate approaches to defusing the cause of the insurgency.

It is possible for an insurgency to develop from a single cause, for the insurgents to identify and communicate this unifying cause to the population, and for the insurgents to remain steadfastly focused even as counterinsurgents undermine their organization and redress the cause. But often the case that there is no single cause, that popular support is mobilized by appealing to multiple motivations, and

[*]Daniel G. Cox is an Associate Professor of Political Science at the School of Advanced Military Studies and an Adjunct Professor at American Military University. Dr. Cox has published multiple works as well as scholarly articles in several peer-reviewed, academic journals. Dr. Cox is also working on a larger project focusing on the future of war.

[**]Dr. Alex Ryan is a Senior Systems Design Advisor with the Government of Alberta. He co-founded the Alberta CoLab and the Systemic Design Research Network. He is also a co-chair of the Relating Systems Thinking and Design Symposium.

Daniel G. Cox and Alex Ryan, "Countering Insurgency and the Myth of "The Cause"," *Journal of Strategic Security* 8, no. 1 (2015): 43-62. DOI: http://dx.doi.org/10.5038/1944-0472.8.1.1419. Available at: http://scholarcommons.usf.edu/jss/vol8/iss1/4.

that by the time counterinsurgents resolve the initial grievance, the insurgency has found alternative justifications to mobilize popular support. Since insurgent leadership is often competent and adaptive, it would be wise to consider the latter scenario against any counterinsurgency strategy. Yet, even when this is acknowledged in the counterinsurgency literature, the theory is remarkably silent how this affects the choice of operational approach. We must venture outside of the standard counterinsurgency (COIN) literature to address this gap.

The structure of this article is as follows. The next section briefly reviews the way classic COIN theories deal with underlying tensions and the insurgent cause. This is followed by two case studies in the Philippines and Indonesia, which illustrate how propensities and tensions within a society give rise to and sustain the insurgents' cause. Next, the authors introduce a framework for considering insurgencies with more than one potential cause. This presents a number of practical implications for COIN strategy, which are developed in the last section.

The Cause in Counterinsurgency Theory

Roger Trinquier's early recognition of the link between underlying tensions in society and insurgent movement formation is a good place to begin this discussion. Trinquier notes:

> Warfare is now an interlocking system of actions—political, economic, psychological, military—that aims at the *overthrow of the established authority in a country and its replacement by another regime.* To achieve this end, the aggressor tries to exploit the international tensions of the country attacked—ideological, social, religious, economic—any conflict liable to have a profound influence on the population to be conquered [italics in original].[2]

Trinquier identifies four broad categories of tension in the above quote: ideological, social, religious and economic, which seem to encompass most of the specific complaints that could emanate from a group in society and be used by an exploitative insurgent or group of insurgents to develop a cause which can be used to rally support around. Trinquier also emphasizes that the tensions that can turn into the foundation of an insurgent cause seemed limitless even in 1964. He observes that, "from a localized conflict of secondary origin and importance, they will always attempt sooner or later to bring about a generalized conflict."[3]

It is ironic that while Trinquier observes underlying tensions as being fundamental to the cause and insurgency formation and sustainment, he spends the rest of his book explaining how population and resource control through accurate censuses, intelligence, and restricting and monitoring movement, is the key to victory. His original observations regarding tensions seem lost and it is almost as if he has taken for granted that once an insurgency begins, it must be dealt with using almost the same COIN methods that the insurgent is employing: clamping down on the population instead of addressing those issues that are fueling the movement.

Galula places more emphasis on the necessity of the cause and notes that, "problems of all natures are exploitable for an insurgency."[4] But he does not discuss these problems in terms of tensions or even local grievances, instead focusing on what makes a good and sustainable cause. While Trinquier explains the role of tensions in cause formation well, Galula does a far better job of providing avenues for attacking the underlying tensions and thus undermining the insurgent's cause. Galula argues that even after the insurgency has initiated armed violence, a good COIN strategy would be to research insurgent demands and comprise a list that the counterinsurgent will immediately use to identify easily addressed complaints. If successful, the entire insurgency can be undermined by addressing some of the core complaints or tensions that the insurgent had previously used to develop the insurgent cause.[5]

Propensities and Tensions Feeding Insurgent Causes

Appreciating the historical and cultural context is particularly important to understanding the dynamics of insurgencies. The history and culture of a nation-state, identity group, or region is an important source of underlying tensions. The collective memories of actors, kept alive through narrative accounts of histories often extending back hundreds or thousands of years, are relevant because they guide and constrain future actions.

The present study refers to the influence of past events, ideas, and emotions on future events as the propensity of a situation. This is not a deterministic relationship between past and future states, but rather a conditioning of future possibilities on the past. For example, a history of exploitative engagements with Western nation-states and past colonizers could place a counterinsurgent in the unenviable position of actually having to "fight" history, or at least historical perception, just to be accepted as a legitimate actor by the local population. This society may have a propensity for xenophobia and defiance against external intervention.

There are multiple insurgent groups that have operated or are currently operating in the Philippines, including Abu Sayyaf Group (ASG), Moro National Liberation Front (MNLF), and the Moro Islamic Liberation Front (MILF). These groups have exhibited very little operational synergy. In fact, ASG and MILF are splinter groups from MNLF. However, they and their civilian supporters share one key propensity. They view the national government and any foreign military interveners on behalf of the national government as nothing more than an extension of unfair and brutal repression of Muslims, which began with Spanish colonization.

Case of the Philippines

Islam was introduced to the Philippines in the thirteenth century. Originally, it was isolated to the Sulu islands but eventually spread to encompass not only the Sulu islands but, almost all of the southern island of Mindanao. Spanish conquistadors arrived shortly after the spread of Islam in 1565 and a brutal colonization effort was waged for three hundred and thirty four years.[6] Eventually, the Spanish relinquished control of the Philippines to the United States in 1898, but this almost immediately resulted in hostilities between the United States and the Philippines and ultimately resulted in the American-Philippine War (1899-1902). The bloody war that ensued produced over seven thousand U.S. casualties and a far greater magnitude on the Filipino side. The war cost the United States $400 million to prosecute.[7] The goal of the United States was to ultimately produce a self-governing Philippines.[8] Even though the Philippine Independence Act of 1934 was crafted guaranteeing a free and sovereign state, the damage done during the war—coupled with the Spanish colonial experience—created a deep-seated mistrust of foreign military intervention, especially among Muslims in the south.[9]

The animosity from this historical legacy and the resulting distrust of outsiders is just one of many aspects that must be taken into account when intervening in the Muslim-dominated regions of the Philippines. Considering this obstacle, the successful trajectory of the U. S. Special Forces continuing Joint Special Operations Task Force-Philippines (JSOTF-P) operation is particularly noteworthy. The use of the indirect approach by U. S. Special Forces manifested in operating by, with, and through the Filipino military may have allowed the U. S. Special Forces to mitigate the negative propensity described above.

Unfortunately, propensities are not the only critical part of the operating environment that a counterinsurgent has to indentify and contend with. Underlying tensions are also an important aspect feeding into the insurgent cause. Tensions exist whenever two or more opposing forces coincide. For the case of insurgency, we are particularly interested in tensions arising from value conflict, whether this is within or between actors. Because these tensions can be layered, this creates a problem of transparency. This, in turn, may create a causal link problem whereby the counterinsurgent addresses the most recent tension being exploited by the insurgent without addressing root tensions or causes, which initially or more fundamentally fed the insurgent cause. Conversely, new tensions may have replaced old ones, creating a situation whereby the counterinsurgent is wasting time and resources addressing the original tension(s) that were formative to the movement but no longer active.

Case of Indonesia

The Banda Aceh region of Indonesia located on the northern tip of the island of Sumatra provides an example of layered tensions that can fuel an insurgency. Indonesia is a patchwork of disparate peoples, many of whom have only the historical experience of repressive Dutch colonialism in common. Both Sukarno's and Suharto's dictatorial rule, while admittedly very brutal, helped to forge a national identity for Indonesia. But even this was fragile, and poor economic and human rights treatment of the people of East Timor eventually led to the small southern island breaking away from the Indonesian nation-state. Further, both the Papuans of West Papua and the Acehnese of northern Sumatra have expressed their desire for independence.

The layering of tensions fueling the rebellion against the Indonesian government is most evident in the Acehnese case so it will be briefly described here. The people of the province of Aceh have suffered a great deal from the founding of the nation through the rule of President Megawatti. Under the rule of President Suharto, Indonesia was witness to a great deal of persecution of out-groups. Developing his dictatorial vision of the "New Order," Suharto enforced authoritarian rule to pursue economic development. He initially targeted communists, culminating with the outlawing of all communist parties.[10] After dealing with the communists, Suharto turned his attentions to Muslim political activists, persecuting key leaders and movements.[11]

Understandably, a resistance movement formed known as the Free Aceh Movement, Gerakan Aceh Merdeka (GAM), which soon drew violent crackdowns from the Indonesian government. This movement has been labeled as a terrorist organization by the central government but there is little proof that GAM ever perpetrated an attack against civilian targets. The present authors feel GAM would be better labeled an insurgent or secessionist movement although most of the actions taken by members of GAM fell under the domain of peaceful protest. Despite these facts, GAM was a threat to Indonesian control of the province of Aceh and several notable violent clashes did occur between members of GAM and the Indonesian military.

The tsunami of 2005, which killed over 160,000 people, changed the landscape and created an opportunity for the Indonesian government and America to step in and provide emergency aid and longer-term aid to rebuild the catastrophe ravaged province. Susilo Yudhayono had only recently replaced Megawatti as

President but he decided to extend a hand to the people of Aceh offering profit sharing from the massive natural gas reserves off the coast of Aceh as well as greater participation in Indonesian politics.[12] Stability soon returned to the region and GAM entered a period of inactivity. This would have been the end of the story except that a new background tension had already developed fueled by the same government mistreatment that the people of Aceh had suffered at the hands of the national government.

The propensity to distrust central government rule engendered through an unbroken succession of Presidents willing to use heavy-handed military tactics against the Acehnese from Sukarno to Megawatti is now being enmeshed with a tension, engendered by regional terror group Jemaah Islamiyah (JI), between religious fundamentalism and secularism. Therefore, despite massive aid to the province following the tsunami of 2005 and despite recent political and local rule concessions granted by the Indonesian government to the Aceh province, a strong fundamental Islamic movement is forming. It should be noted this is a novel development in Indonesian history.[13] In 2003, Aceh's first sharia court opened. It was initially promised by local religious leaders that implementation of sharia law would be "moderate" and that human rights would not be abused. However, punishment for failing to attend Friday prayer, for example, could be public caning.[14] Any pretentions at moderation are quickly passing. In Fall 2009, new laws passed which stated "married people convicted of adultery can be sentenced to death by stoning. Unmarried people can be sentenced to 100 lashes with a cane."[15]

Similarly, a specialized police unit, Wilayatul Hisbah, is now patrolling the streets of Aceh looking to disrupt or arrest "unmarried couples, Muslim women without headscarves or those wearing tight clothes, and people drinking alcohol or gambling," which is apparently aimed at combating Western influence, especially influence that seeped into the region when Western nations provided post-tsunami aid.[16] Even though some Acehnese citizens have expressed discontent with the increasingly harsh religious laws, most are afraid to voice their concerns for fear of being branded unreligious.[17]

Overlaying this fundamentalist trend is increasing violence surrounding elections in the province and an increasingly active and violent JI. While a period of quiescence has ensued after the 2005 peace agreement, if violence aimed at the Indonesian national government ensues again, a new tension—religious fundamentalism vs. political secularism firmly layered over old economic grievances and a history of poor human rights treatment—will create an even more complex insurgency to deal with than was ever presented by GAM.

In summary, even if one could identify "the cause" for an insurgency, it must still emerge from a complex web of dynamic tensions and propensities. As the underlying tensions evolve, so too can the cause. Consequently, a singular, static definition of the insurgent cause is not a reliable foundation for planning COIN operations. While this is already largely recognized in COIN doctrine and theory, the logical implications for COIN strategy have not been fully resolved. A multi-causal account of insurgency requires new conceptual tools not available within traditional COIN theory.

A Conceptual Framework for Multi-causal Insurgency

This section develops a multi-causal framework for understanding insurgency. First, a distinction is necessary between causation and insurgent causes. Causation is the inference of relationships of necessity and sufficiency between a cause and its effects. Research into the causes of war seeks to uncover this kind of causal relationship. In the previous discussion, the complex web of dynamic tensions and propensities links causes and effects.

In contrast, according to U.S. Field Manual (FM) 3-24, "A cause is a principle or movement militantly defended or supported."[18] Galula explains how a cause is linked with underlying tensions:

> What is a political problem? It is 'an unsolved contradiction', according to Mao Tse-tung. If one accepts this definition, then a political cause is the championing of one side of the contradiction.[19]

Insurgent causes are not material causes that produce causal effects; rather insurgent causes provide justification for resorting to violent action. Although the two concepts are related, they are quite distinct and should not be conflated. Causation is generally relevant to the level of tactical action, whereas insurgent causes influence the insurgency at the strategic level. Both causation and insurgent causes will be relevant to our discussion below.

Until recently, most scientific explanations of causation focused on single cause-effect relationships. For example, the *Guide for Understanding and Implementing Defense Experimentation: GUIDEx*, a report produced in collaboration between defense scientists representing Australia, Canada, the United Kingdom, and the United States, asserts:

> Any national or coalition capability problem may be stated as: Does A cause B? An experimental capability or concept—a new way of doing business—is examined in experimentation to determine if the proposed capability A causes the anticipated military effect B. The experiment hypothesis states the causal relationship between the proposed solution and the problem.[20]

This accurately expresses the classical scientific view of experimentation. The GUIDEx goes on to say that an important criteria of a good experiment is the ability to isolate the reason for change in the effect B.[21] In this paradigm, the goal of experimentation is to answer the question of causation between one independent variable and one dependent variable. The method of experimentation is to create a closed system to eliminate alternative sources of variation that could confound the experimental result. In this paradigm, accumulated knowledge from multiple experiments permits reasoning about causal chains: A causes B, which causes C, which causes D.

Although scientists may occasionally approximate the ideal conditions of a closed system for long enough to isolate a single independent variable, this degree of control is of course impossible in any human society. The societies in which insurgencies foment are open systems, characterized by perpetual novelty and an uncountable number of independent variables. Here, causality is networked, and cannot be reduced to single cause-effect relationships, or even to linear causal chains.

Complex systems science provides an alternative perspective capable of making sense of networked causality. Distributed networks of autonomous agents that make local decisions based on local information characterize complex adaptive systems. From these individual local choices, global patterns emerge and feed back to affect the subsequent decisions of the autonomous agents. As a result of these iterative feedback cycles, causation is complex, networked, and circular. Perturbation of A may ripple out to affect B, C, and D, which in turn affects A. Thus, not only do causes have effects but, those effects may actually have caused the cause!

If this all sounds unnecessarily convoluted, it is worthwhile considering the very real effects these feedback loops can generate. A classic example is the self-fulfilling prophecy of a bank run. A rumor that a bank is in financial difficulty—even when it is not—may cause cautious investors to withdraw their money. Seeing long queues of customers withdrawing their savings causes more customers to withdraw their savings, and the problem snowballs. Before the end of the day, the bank has exhausted its liquid reserves, and actually is insolvent. Perceptions and rumors can have similar and no less dramatic effects during revolutions and counter insurgencies. Galula cites the effective use of the slogan "Land to the Tiller" by the Chinese Communists to promote the false idea that land ownership in China was concentrated in the hands of a small minority.[22]

Complex Systems and Intervention Options

Complex systems exhibit self-organization, emergence, hysteresis, latent pathways, and adaptation. Understanding each of these concepts provides important insights for COIN theory, and opens up new intervention options for counterinsurgents.

Self-organization

Self-organization is the spontaneous increase in order over time in an open system. It is spontaneous in the sense that it is not externally imposed, but accrues through interactions between parts of the system as energy flows through it. A widely studied model of self-organization demonstrates a spontaneous increase in organization when agents set their color by following two rules. The first rule, short-range activation, sets the color preference to the most common color of the agent's closest neighbors. The second rule, long-range inhibition, sets the color preference to be opposite of the most common color of the agent's more distant neighbors. Other parameters of the model include the radius for the nearest neighbors, the radius for the distant neighbors, and the weighting given to short range activation versus long range inhibition. The outcome of this model is shown in Figure 1. Within five time steps, an initially random mix of black and white agents has self-organized into a pattern of black and white stripes. With different initial conditions, the model will produce black and white stripes different in detail, but with the same qualitative pattern. With different parameter settings, the same rule set can produce uniformly black or white agents, black spots on a white background, or vice versa. This very simple model has been used to explain growth and differentiation of the structure of an organism, pattern formation in animal fur, and the clustering of industries in regional economics.[23]

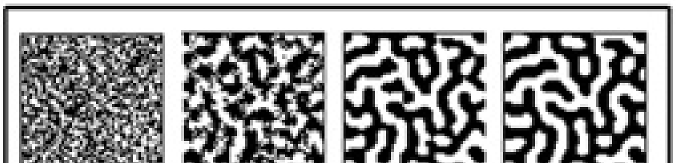

Figure 1: Pattern Formation as an Example of Self-Organization and Emergence

In the COIN literature, it is common to divide the population into three states: actively supporting the Government, the neutral majority, and actively supporting the insurgency. Accepting this simplification for the present discussion, the dynamics of self-organization help to explain why one village can be pro-Government, while a nearby village with identical social conditions supports the insurgency. Because an actor's choice of state is conditioned by the states of others in the actor's social network, a population that is compelled to choose between insurgents and counterinsurgents will tend to cluster into spatially organized patterns over time.

The first implication of self-organization is that the spatial distribution of pro-Government and pro-insurgent populations is more important than the total proportion of the population in each state. Measures of effectiveness that aggregate national statistical data can be misleading. A color-coded map that shows patterns of allegiance over time provides a much richer assessment tool. In COIN, the local situation can be very different from the neighboring local situation and from the regional situation. Therefore, decision-makers at lower levels need greater autonomy to tailor plans to their local context. Of course, the importance of bottom-up intelligence flows and devolving decisions to the lowest levels are already standard tenets of COIN doctrine.[24] The jointly published U.S. Army and U.S. Marine Corps doctrine Counterinsurgency describes COIN as "a shifting 'mosaic war' that is difficult for counterinsurgents to envision as a coherent whole."[25] What is new here is that self-organization provides a theoretical explanation for the "mosaic war" observed in practice, a justification for decentralized execution of COIN operations, and a prescription for assessment of progress.

The second implication of self-organization is that indirect approaches lead to more radical transformations in the observed pattern than direct intervention. The patterns formed are attractors in a dynamical system, and tend to be robust to local perturbation. For the majority of agents in Figure 1, changing their color from black to white has no permanent effect on the system. The unchanged state of their neighbors simply means the agent will flip back in the next time step. Direct action will only work if a critical number of agents are simultaneously flipped. Even then, as long as the underlying calculus of the agents remains unchanged, direct action will likely only redistribute the location of black and white stripes, and have no long-term effect on their relative proportion. In contrast, a relatively small shift in the weighting between the short-range activation and long-range inhibition rules can qualitatively change the observed patterns. The change sweeps through the system using exactly the same self-organizing dynamics that perpetuated the original pattern. In COIN, this means that in general, taking indirect action to alter the calculus of the population in choosing whether to support the insurgents or the Government is likely to be more effective for transformation than coercion through population control measures.

Emergence

The patterns produced by self-organizing systems are emergent. Emergence means the whole is different from the sum of its parts.[26] In science, there is an emergence hierarchy between physics, chemistry, biology, and psychology. The laws of chemistry are constrained by, but additional to, the laws of physics. Biology is constrained by the laws of chemistry, and chemicals are the building blocks of cells, but chemistry also introduces new theories to explain life. Psychology is constrained by biology, but again new theories operate at the level of mind. At each level, theory is constrained by lower levels, but it also has some autonomy from the level below. New concepts and new rules are needed to explain regularities at the higher level. In Figure 1, one can meaningfully talk about stripes and spots in relation to the whole. Yet, at the level of individual agents, the rule set operates only on local information about the color of close and distant neighbors. Stripes and spots are emergent properties that are meaningless at the individual level. Patterns that emerge from one level provide the building blocks for systems at the next level up.

In the same way, there is an emergence hierarchy in counterinsurgency warfare. The operational level of warfare is not simply the aggregation of tactical engagements. The strategic level that connects the military instrument with policy is qualitatively different than the operational level, which plans and executes the campaign within the theatre of operations. Different concepts are required for different levels of war. For example, Stathis Kalyvas finds in his detailed study of violence in civil war, especially in the Greek Civil War, that people, far from being unified to act violently because of fear, ideology, or prewar political social polarization, acted violently selectively for very sub-regional, even local reasons.[27] Kalyvas is not arguing that all violence is local for political and insurgent leaders can certainly move people and groups to violence. Instead, he is attempting to differentiate between the macro and micro motives that move people to violence in all conflicts. As Kalyvas argues,

> indiscriminate violence is an informational shortcut that may backfire on those who use it; selective violence is jointly produced by political actors seeking information and individuals trying to avoid the worst—but also grabbing what opportunities the predicament affords them.[28]

Kalyvas notes that civil wars are distinct from interstate wars mainly through the level of intimacy each exhibits. Interstate wars are affairs between strangers and thus lack intimacy but civil wars, and we would argue insurgencies as well, are wars against countrymen, neighbors, and even relatives.[29] Neighbors, relatives, and friends would regularly denounce each other to legitimate and illegitimate authorities for myriad reasons including jealousy and personal grievance. It was a short step from denunciation to violence, for neighbors, relatives, and friends, if the opportunity afforded it.[30] Some people were genuinely moved by their leaders' political motives but many others are found in civil war and insurgency to be motivated by petty and extremely personal agendas.

The implication of Kalyvas' study and our current work is that it is misguided to establish an operational campaign aimed at the cause or the center of gravity. As Kalyvas notes, many scholars and practitioners find the cause of violence to be impenetrable so they hand-wave "explanations for violence emphasizing collective emotions, ideologies, and cultures that have low explanatory power."[31] Therefore, the best campaign plan might be to allow brigade and battalion commanders a great deal of latitude in dealing with the local motives for violence in a counterinsurgency since motives might be macro, micro, or a mix of the two.

Hysteresis

The third concept from complex systems science, hysteresis, is a non-linear behavior encountered in a wide variety of processes ranging from ferroelectricity to biology, where the input-output dynamic relations between variables involve memory effects.[32] Hysteresis implies path dependence. When a system returns to a previous state, it may behave differently. Moreover, different paths to the same state can result in different behavior. Consequently, in systems with hysteresis, it is insufficient to know only the current state. The history of the system is essential for making sense of future possible patterns of behavior.

Path dependence and the importance of history are hardly new to the counterinsurgent. The significance of hysteresis is in targeting insurgent causes. Once a Government loses legitimacy, addressing stated grievances would not automatically win back popular support. For example, in Egypt, President Mubarak's concession in response to mass protests may have actually emboldened the protesters to raise additional demands and led to wider support. A more sophisticated approach is required to counter insurgent causes.

Instead of reacting to the insurgent causes directly, counterinsurgents need to understand how causes relate to dominant narratives within a society. Narratives are not simply a disinterested chronology of events. The choice of perspective from which the story is told, which actors are given a voice and which are ignored, which events are emphasized and which are omitted, as well as the bounding of the narrative in time and geography all affect the implied moral of the story. The sequencing of events, feelings, and actions can be used to suggest relationships between effects and their causes. Insurgent causes that can be connected with existing narratives are more likely to achieve resonance within a society, which can greatly expand the base of support.

Once insurgent causes become associated with a narrative, directly countering the narrative may inadvertently strengthen it. George Lakoff uses a simple example to illustrate this point. The effect of the instruction "Don't think of an elephant!" is invariably the opposite of its intent. Elinor Ochs and Lisa Capps make the point that

> counternarratives do not necessarily involve overt reference to a prevailing narrative world view. It is the voicing of a disjunctive reality itself that constitutes the counterpoint. Indeed, the posing of an alternative account may be more effective in dismantling the status quo perspective than overt critiques. In making reference to them, critiques perpetuate the salience of the dominant discourses they otherwise aim to uproot.[33]

Effectively countering insurgent causes requires the fostering of new identities and a narrative that voices a "disjunctive reality." A good example of this is the change in usage of "United States" prior to the American Civil War as a plural noun, to a singular noun afterwards, representing a transformation from "Union" to nation.

Lincoln's wartime speeches betokened this transition. In his first inaugural address, he used the word "Union" twenty times and the word "nation" not once... In his letter to Horace Greeley of August 22, 1862, on the relationship of slavery to the war, Lincoln spoke of the Union eight times and of the nation not at all. Little more than a year later, in his address at Gettysburg, the president did not refer to the "Union" at all but used the word "nation" five times to invoke a new birth of freedom and nationalism for the United States.[34] And in his second inaugural address, looking back over the events of the past four years, Lincoln spoke of one side seeking to dissolve the Union in 1861 and the other accepting the challenge of war to preserve the nation.[35]

Lincoln used language to help forge new identities and shape narratives as America emerged from civil war. A narrative emphasizing nationalism reframed political discourse away from the divisive Union and Confederate terminology.

Latent pathways

Complex systems are highly networked. This gives rise to the fourth concept from complex systems science: energy, matter, and information flows along multiple pathways. Observing the current pattern of behavior only provides information about active pathways; latent pathways may not be visible. Consequently, complex systems generally exhibit graceful degradation. When one pathway is blocked, latent pathways are activated to preserve system functionality. The so-called balloon effect is a good example of multiple pathways in a complex system. To counter the Medellin cartel's drug smuggling operations between Columbia and the United States, the South Florida Drug Task Force conducted a successful operation that dramatically reduced the volume of drugs entering Florida via the Caribbean. However, this did not stop the flow of drugs into the United States. In response, Columbian cartels established relationships with Mexican marijuana cartels to smuggle narcotics across the 2000 mile shared border with the United States. The current violence of the Mexican drug war is an indirect result of successfully closing down one pathway within a complex system.

The concept of multiple pathways is related to insurgent causes. One should expect that effectively addressing one cause would activate new pathways for mobilizing the insurgency. This reinforces the dangers of focusing on a single insurgent cause. Even though latent pathways in a complex system may not be obvious from observing the current pattern of behavior, it is possible to anticipate alternative pathways before they are activated. This is where an understanding of the underlying tensions and propensity within the society is critical, because it illuminates contradictions that the insurgents may seek to exploit. Identifying potential out-groups, such as the Shiite population in Bahrain, also allows the counterinsurgent to anticipate the kind of grievances insurgents may use to mobilize these out-groups, and then take steps to mitigate these latent pathways before they are activated.

Adaptation

The final complex systems concept considered here is adaptation. COIN theorists often remark upon the adaptive nature of insurgents. FM 3-24 claims that competent insurgents are adaptive.[36] Yet, paradoxically, it is the relative weakness of insurgent forces that provides them an edge in adaptability. Complex systems scientists have drawn on Charles Darwin's theory of evolution to show why insurgents adapt faster and more effectively.[37] Adaptation requires the presence of variation, selection, and replication. In an asymmetric conflict, the weaker side usually contains more diversity, are subject to a stronger selection pressure than the pressure they exert on the strong side, and are exposed to combat for longer, which replicates combat experience.[38] This theory is supported quantitatively with data from both Iraq and Afghanistan, which shows that the average time interval between fatal improvised explosive devise attacks increases logarithmically over the duration of the war.[39] To paraphrase Megginson's paraphrasing of Darwin, it is not the strongest insurgencies that survive, nor the most intelligent, but rather the most adaptable to change.

Given the central importance of adaptation in COIN, counterinsurgents need to both improve their own adaptability and counter the adaptability of the insurgent. This requires increased variation in our own forces, stronger selection pressure, and faster replication of successful innovations. Counter-adaptation requires weakening or distorting the evolutionary pressure applied to insurgents. Lieutenant Colonel Michael Ryan, Australian Army, deliberately used counter-adaptation against the Taliban as the commander of the 1st Reconstruction Task Force in Oruzgan Province, Afghanistan.

Recent advances in evolutionary theory provide new insights into how to leverage the power of adaptation. The evolution of evolvability—second order adaptation—applies evolution to the process of evolution itself. For example, the way that variation is generated is far from random, because it has adapted to produce genotypic variation in areas that are correlated with the greatest environmental flux, while error-correcting codes protect regions associated with critical functionality from too much variation. Second order adaptation enables counterinsurgents to accelerate their rate of adaptation. As a simple example, the use of after-action reviews (AAR) helps units to learn and adapt. Adapting how AARs are conducted to improve their effectiveness is a second-order adaptation.

Evolutionary biologists are now also accepting that selective pressure applies not just at the level of the gene, but also to organisms and even groups of organisms. While selection pressures at the lowest level of selection are the most rapid and strongest in magnitude, the subtle effects of group selection may actually dominate over longer time scales. A multilevel view of selection points to a potential key advantage for counterinsurgents. Even if insurgents have an advantage in tactical adaptation because of their highly variable and decentralized structure, counterinsurgents can still be more adaptive at the operational and strategic levels, because they are better integrated. The slower, but more strategic adaptations of the counterinsurgent may steer insurgents into a corner where faster tactical adaptation becomes largely irrelevant. However, this requires counterinsurgents to deliberately work to improve their higher-level adaptive mechanisms.

Conclusion: Implications for COIN Approaches

Given what has been argued thus far, a premium is placed on developing historical and cultural intelligence on the leader and member mindset. What has propelled these individuals to transmutate from peaceful political grievance to violent rebellion? This is just one example of a cogent question that must be answered before the cause can be fully understood and dealt with. Such cultural and historical intelligence necessitates that deep knowledge be developed on the insurgent identity group(s) but that is a positive development as it narrows the scope of study when addressing the insurgent cause. For example, in terms of operations and tactics, it is certainly important to know that Iraqi citizens harbor a deep distaste for dogs. However, this information is of little use in developing a plan to combat the insurgent cause, excepting, of course, that employment of culturally insensitive tactics only adds fuel to the insurgent cause.

What needs to be discerned are the historical, political, and cultural antecedents to insurgency. One needs to understand the historical propensities that will have to be considered when developing a campaign to combat the insurgency. But one also needs to know the individual tensions in society, like discrimination against certain minorities, historical economic exploitation of a region, religious discrimination, etc. that are not only currently being used by the insurgents to develop their cause and broaden their appeal, but also tensions that could be exploited in the future either to expand the insurgency or can be shifted to it if the counterinsurgent is successful in combating one or more of the original tensions that fueled the insurgent cause. The counterinsurgent would take all of this into consideration developing a more sophisticated Galulesque list of not only insurgent demands but, underlying tensions and propensities which are feeding these demands.

Galula suggests immediately addressing the demands that the legitimate national government can and ignoring the rest.[40] The present authors do not suggest this course of action. Before meeting even a single demand or addressing a single underlying tension in society one must attempt to think through how injecting energy into the system will affect the overall system. For example, does dealing with the underlying poverty in a society push the insurgent to a more religious tension from which to fuel the insurgency? Are there other tensions the insurgents are not using which could be co-opted after poverty is addressed? When one views just the cause through the lens of complexity, it becomes clear that engaging in counterinsurgency is a very messy endeavor.

Also, it should become clear from this analysis that COIN operations will have to be very fluid and undergo a process of constant revision as one notes changes in the environmental frame. Such an approach should also help one to successfully categorize what type of insurgency is being presented. Bard O'Neill makes a valiant attempt at disaggregating types of insurgency noting that each type demands different COIN approaches to address it.[41] This implies that certain strategies might work with some insurgencies while they inadvertently fuel others making identification of the tensions and cause even more important.

The current situation in Pakistan serves as an illustrative example. The Pakistani government has always had great trouble penetrating and controlling the

Baluchistani area and Northwest Frontier Porvince (NWFP). This problem has become particularly acute in the post-Musharef era and the Pakistani Taliban have experienced success exploiting this historical lack of control coupled with the chaos created by the fall of Musharef. The government initially attempted to offer conciliations to the Pakistani Taliban such as more local autonomy and stricter religious standards in schooling and local law enforcement. But this approach soon backfired as the Taliban rather than entering into a period of calm inactivity actually became emboldened and challenged the rule of the national government more forcefully. A messy and violent counterinsurgency campaign ensued and the outcome regarding whom will eventually rule Pakistan is still in doubt.

Noting all of the above, conciliations given to insurgents has been successfully employed as a counterinsurgent strategy in past insurgencies, but according to the 2010 RAND study *How Insurgencies End* this is rare, occurring in less than a third of modern insurgencies. Notable twentieth century examples include El Salvador, Guatemala, South Africa, and Northern Ireland.[42] The key is in understanding the system, propensities, and tensions that feed and frame the cause before attacking it.

In the final analysis, if one takes Kalyvas's thesis that all violence is local at face value, and one recognizes the complexity of social interactions, then one must also admit that causes will be highly personalized. One person might join the insurgency out of a real hatred for the central government. Another might join for social reasons. Still others might be drawn for religious reasons or even by the allure of potential criminality. Not only will different people and different groups join for different reasons but the main cause will likely shift over time.

This article is aimed at beginning the conversation and shifting the mindset of counterinsurgency researchers. Without a more sophisticated approach toward understanding the causes of insurgency, countering them will be impossible.

Notes

[1] David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Praeger, 1964); Jeffrey Record, *Beating Goliath: Why Insurgencies Win* (Dulles, VA: Potomac Books, 2007); Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping* (Saint Petersburg, FL: Hailer, 1973); Bard O'Neill, *Insurgency and Terrorism: From Revolution to Apocalypse*, 2nd ed. (Washington, D.C.: Potomac Books, 2005); Anthony James, *Resisting Rebellion: The History and Politics of Counterinsurgency* (Lexington: University of Kentucky Press, 2004).

[2] Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (Fort Leavenworth: Combat Studies Institute, 1964): 20, 22.

[3] Ibid., 6.

[4] Galula, *Counterinsurgency Warfare*, 22.

5. Ibid., 103.

6. Thomas G. Wilson, Jr., "Extending the Autonomous Region in Muslim Mindanao to the Moro Islamic Liberation Front: A Catalyst for Peace," *U.S. Army School of Advanced Military Studies MMAS Monograph series*, 2009, 13-14.

7. Andrew J. Birtle, *U. S. Army Counterinsurgency and Contingency Operations Doctrine 1860-1941* (Washington, D.C.: U. S. Army Center of Military History, 2004), 108.

8. Ibid., 119.

9. Also known as the Tydings-Mcduffie Act.

10. Ulf Sundhaussen, "Indonesia: Past and Present Encounters with Democracy," in *Democracy in Developing Nations, Volume Three: Asia*, Larry Diamond, Juan Linz, and Seymour Martin Lipset, eds., (London, England: Adamantine Press Limited, 1989), 440.

11. William R. Liddle, "The Islamic Turn in Indonesia," *The Journal of Asian Studies* 55, no. 3 (1996): 614.

12. Michael Vatikiotis, "Southeast Asia in 2005: Strength in the Face of Adversity," in *Southeast Asian Affairs,* Dajit Singh and Lorraine Carlos Salazar, eds. (Singapore: Institute of Southeast Asian Studies, 2006), 6.

13. Michael Vatikiotis, *Indonesian Politics Under Suharto: The Rise and Fall of the New Order*, 3rd ed., (New York: Routledge, 1993), 119.

14. "Aceh's Sharia Court," *BBC News Online*, 4 March 2003, http://news.bbc.co.uk/go/em/fr/-/2/hi/asia-pacific/2816785.stm.

15. "Aceh Passes Adultery Stoning Law," *BBC News Online*, 14 September 2009, http://news.bbc.co.uk/go/em/fr/-/2/hi/asia-pacific/8254631.stm.

16. "Islamic Police Tighten Grip on Indonesia's Aceh," *The Malaysian Insider*, 14 January 2010, http://themalaysianinsider.com/index.php/world/49530-islamicpolice-tighten-grip-on-indonesias-aceh.

17. Katie Hamann, "Aceh's Sharia Law Still Controversial in Indonesia," *VOA News*, 29 December 2009, http://www.voanews.com/english/news/religion/Acehs-Sharia-Law-Still-Controversial-in-Indonesia-80257482.html.

18. Department of the Army, *Field Manual 3-24: Counterinsurgency* (Washington, D.C.: HQDA, 15 December 2006), 1-10.

19. Galula, *Counterinsurgency Warfare*, 10.

20. The Technical Cooperation Program, Guide for Understanding and Implementing Defense Experimentation (Ottawa, Canada: Canadian Forces Experimentation Centre, February 2006), http://www.acq.osd.mil/ttcp/reference/docs/GUIDExBookFeb2006.pdf.

21. Ibid., 13.

22. Galula, *Counterinsurgency Warfare*, 17.

23. Alan M. Turing, "The Chemical Basis of Morphogenesis," *Philosophical Transactions of the Royal Society of London, Series B, Biological Sciences* 237, no. 641 (1952), 37-72; BN Nagorcka and JR Mooney, "From stripes to spots: prepatterns which can be produced in the skin by a reaction-diffusion system," *IMA Journal of Mathematics Applied in Medicine and Biology* 9, no. 4 (1992): 249-67; Paul Krugman, "A Dynamic Spatial Model,"(working paper No. 4219, National Bureau Of Economic Research, Cambridge, MA, November 1992).

24. Department of the Army, *Field Manual 3-24*, *1-26* and *3-31*.

25. Ibid., 1-8.

26. P.W. Anderson, "More is Different," *Science* 177, no. 4047 (4 August 1972): 393-396.

27. Stathis N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge: Cambridge University Press, 2006), 328.

28. Ibid., 388.

29. Ibid., 330-33.

30. Ibid., 333-34.

31. Ibid., 388.

32. Fayçal Ikhouane and José Rodellar, *Systems With Hysteresis: Analysis, Identification and Control Using the Bouc-Wen Model* (Chichester, West Sussex: Wiley-Interscience, 2007), xi.

33. Elinor Ochs and Lisa Capps, "Narrating the Self," *Annual Review of Anthropology* 25 (1996), 37.

34. Abraham Lincoln to Horace Greeley, letter, 22 August 1862, http://www.abrahamlincolnonline.org/lincoln/speeches/greeley.htm.

35. Abraham Lincoln, Second Inaugural Address, 4 March 1865, http://www.abrahamlincolnonline.org/lincoln/speeches/inaug2.htm.

36. Department of the Army, *Field Manual 3-24*, 1-28.

37. Dominic Johnson, "Darwinian Selection in Asymmetric Warfare: The Natural Advantage of Insurgents and Terrorists," *Journal of the Washington Academy of Sciences* 95 (2009), 89-112.

38. Ibid., 89.

39. Neil Johnson et al, "Dynamic Red Queen explains patterns in fatal insurgent attacks," *arXiv* (January 2011), 1101.0987.

40. Galula, *Counterinsurgency Warfare*, 103.

41. Bard, *Insurgency and Terrorism*, Chapter 3.

42. Ben Connable and Martin C. Libicki, *How Insurgencies End* (Santa Monica, CA: RAND, 2010), 18-19.

Irrational Rationality of Terrorism

Robert Nalbandov, PhD*

The recent increase in research on terrorism put scholars and counterterrorism practitioners in a quandary with no single overwhelming definition of terrorism.[1] The reason for such ontological diversity is the wish to put terrorism into the cognitive frameworks of rationality. According to a RAND study, "the main argument favoring a rational-choice model is that, if terrorists and terror organizations behave rationally, knowledge of their beliefs and preferences should help us understand and predict their behavior."[2] The more rational, or predictable, the terrorists' behavior is the easier it would be to find their true motivators and to deal with terrorism.

There have been several attempts to compartmentalize terrorism within the rational frameworks: Caplan looked into actor-specific rationalities; Crenshaw explored the rationality of the causes of terrorism; Kydd & Walter and Pape brought the rationality into the strategic actions of the terrorists; Oberschall focused on the collective action theory, while Libicki researched the rational thinking behind the terrorist's motivations.[3] With all those multiple approaches to studies of terrorism there is a remarkable lack of the coherent and parsimonious theory of rationality that would bring it different forms under a uniform theoretical framework.

The present article fills this gap by testing the application of the rational choice to the "old" (before the end of the Cold War) and the "new" (after the end of the Cold War) concepts of terrorism. While the distinction follows the timeframe consideration it is far more fundamental.

The phenomenon of "new" terrorists is not necessarily limited to suicide terrorists who had been in existence long before the Cold War ended—the Japanese kamikaze fighters during WWII, the Jewish resistance operatives in the wake of the State of Israel, the Tamils who modernized the suicide terror in the 20th

*Dr. Robert Nalbandov is an Assistant Professor at the Department of Political Science, Utah State University. He received his PhD in Political Science from the Central European University, Budapest, in 2008. He is the author of numerous works on international security and conflict resolution.

Robert Nalbandov, "Irrational Rationality of Terrorism." *Journal of Strategic Security* 6, no. 4 (2013): 92-102, DOI: http://dx.doi.org/10.5038/1944-0472.6.4.5. Available at: http://scholarcommons.usf.edu/jss/vol6/iss4/5.

century and many more. The most recent self-radicalized "new" terrorists, the Boston bombers Tsarnayev brothers, had no intention to die with the intended victims of their terrorist attacks. The difference between "old" and "new" terrorism permeates the multi-layered categories: their goals and objectives; the targets they have and the victims they aim to destroy; the rationales behind their radicalization; the areas where they operate and the constituencies supporting them.

The article starts with analysis of the fundamentals of the rational choice theory and applies it at two levels: the individual (actors) and group (collective) via two outlooks: tactical (short-term) and strategic (long-term). The main argument of the article is that while the "old" terrorism can be explained by the rational choice theory, its "new" version represents a substantial departure from rationality. The article ends with the premise that one-fit-all solution to terrorism cannot be found and offers some alternatives to current counter-terrorist efforts.

Rational Conundrum of Terrorism

As a theory of human behavior, rational choice focuses on both individual and groups as actors in two forms, "narrow" and "broad." According to van Um, "The narrow version allows only for action that enhances the personal utility so that individuals act purely selfishly, while a broader version also allows for altruistic goals to be pursued."[4] On the individual level, rational choice "…assumes that the individual is the most appropriate judge of what is best for him or her… The individual has the freedom, as well as the responsibility, to shape his or her own life."[5] On the group level, rational choice emphasizes "…loyalty to groups, with the consequent tendency to evaluate actions in terms of their consequences for the group and without consideration of their consequences for people outside the group…"[6] At both levels, rational choice postulates that all actors are utility maximizers and consistently pursue goals based on the consciously chosen stable preferences.[7] The actors are guided by the logic of expected consequences: they possess credible information about the options available to them and chose the best ones based on their expected utility calculation.[8]

The problem with applying the rational choice framework to the phenomenon of terrorism is threefold. First, a single holistic approach is used to determine the existence or absence of rationality, which disregards other variables beyond the objectively existing cognitive patterns. Rationality is applied in absolute terms and the actors are considered static figures always ending up choosing between the actions with the highest post-action expected utility values.[9] In reality, rational behavior for one actor with set value systems may be irrational for other actors under the same circumstances due to their conflicting value systems. It is a universally accepted assumption that "actors know what they want and can order their wants transitively."[10] The predicament of this approach is that a more rational outcome with increased utility value may occur on its own, or as a result of multiple interceptions of choices that may not always be rational. Rational actors may choose irrational options that may eventually maximize their expected utility and vice versa.

This theoretical quandary is best seen in altruistic suicide. The end state of actions is rational if it fits within the specific cognitive frameworks: to die for the common good may be a noble fit. However, as Mises noted, "No man is qualified to declare what would make another man happier or less discontented,"[11] which means that the core of rationality is essentially subjective. On the individual level, an example of the suicide for the public good is a soldier who daily fights the enemy on the battlefield to ultimately survive, but suddenly decides to consciously commit a heroic but suicidal feat to save her fellow soldiers. Here rational terrorism would predict high upsurge in the numbers of soldiers willing to commit suicide because of the set preferences to save the lives of others by sacrificing one's own. This, however, is not happening and the rationale behind the premeditated suicide remains within the cognitive frameworks of an individual, and her unique personal preferences.

Another problem of the holistic rational approach to terrorism comes from the multiple layers of cognitive behavioral patterns. In the ideal world, the actors should clearly see and easily calculate the post-action expected utility of each option. However, as Monroe and Maher suggested, "…real people don't always operate this way, nor should they. We know that each of us has limited…capacity to perceive, recall, interpret, and calculate…"[12] Rationality is confined by human imperfections, by their inherent inability to "perform the calculations necessary even for a reduced set of options in a decision-making situation," and, ultimately, by the absolute and objective flaws imposed by the "cognitive limitations of their minds."[13]

A possible explanation for the irrational behavior of the actors is the factor of identity, which varies in different actors. Specific identity constructs force them to choose different options not based on the objective utility calculations but on their subjectively constructed assessment of the objective reality. The identity-based "logic of appropriateness" limits the power of rational reasoning of the actors, forces them "to derive actions from given identities" and act "according to the institutionalized practices of a collectivity, based on mutual, and often tacit, understandings of what is true, reasonable, natural, right, and good."[14] Unfortunately, no data is available on the multiplicity of layers of cognitive behavioral patterns that would explain heroism of the soldier from the previous example. The decision to act heroically may be based on her desire to bring victory to her own group out of her specific identity or following the Christian doctrine on self-sacrifice for the sake of the common good. On the contrary, a soldier with a different identity—for instance, a deep believer in another Christian doctrine on suicide being a sinful act (depending on individual interpretations of the scriptures)— may wish to abstain from taking such a step.

Finally, the "weak" rationality fails when the actors are confronted by time-relative constraints. Rationality may or may not be present in immediate decision making: what may be rational in an instant may turn irrational, and vice versa if the actors take time for rational re-thinking of their actions. An immediately rational action may lose its rationality under the influence of additional variables extrinsic to the rational choice frameworks. An option that previously had the lowest expected utility and was anticipated to remain as such may increase its utility depending on external factors. Similarly, a step that seemed immediately irrational may acquire rational basis provided there is enough time for re-thinking. The soldier from the previous example may change her mind and abstain from the heroic suicidal feat if she has enough time to carefully (i.e. rationally) weigh all the pros and cons of it instead of engaging in an impulsive immediate action. Likewise, if her extemporaneous reaction was to hold back from sacrificing her life, she may, at some point in the future or under similar circumstances, choose to die heroically and save others. In all the instances above the preferences are not set: they are multiple and volatile depending on individual cases.

Individual Level Rationality

When applying rational choice theory to the actions of the individual terrorists, a distinction should be made between the non-suicide and the suicide forms of terror. The non-suicide, or "survivalist" terrorism, was mostly characteristic of "old" terror, existing prior to the end of the Cold War, such as the Basque Eucadi ta Askatasuna (ETA), Real Irish Republican Army (RIRA), the Armenian Secret Army for the Liberation of Armenia (ASALA), the Kurdistan Workers' Party (PKK), the Farabundo Marti Liberation Front (FLMN), the Liberation Tigers of Tamil Eelam (LTTE), the Russian "Narodovolci" (short for the "Narodnaya Volya"), and the "Esers" (short for "Party of Socialists–Revolutionaries"). Most of the "old" terrorists were rational actors who wished to live through their struggle to see the results of their actions and to share their benefits with the whole group they represented. The notion of self-sacrifice for the greater common good was absent in the selfish rationality of the "old" terrorists. In addition to having survivalist reasons, the "old" terrorist directed their goals toward attaining tangible benefits: at minimum wider autonomy for their kin or sovereignty and independence, at maximum. These goals were limited in scope, geographic coverage, and usually concerned terrorists themselves.

The goals of the "new" terrorists, who appeared after the collapse of the bipolar system in early 1990s, are transnational in reach and limited in their long-lasting effects. On the individual level, the terrorist who sacrifices her life "hope[s] to achieve infinite bliss in heaven."[15] At first glance, she can, indeed, be considered as "an agent who accepts certain death in order to kill with high probability."[16] Similar to traditional terrorists, she would make relative cost calculations, which, in Sandler's words, "…must demonstrate that the utility associated with the suicidal mission is at least as large as the utility of the status quo."[17] This can be possible, as Caplan rightly noted, "…if you genuinely believe that death in a jihad brings infinite reward," which makes "new" terrorism seem rational.[18]

Rational approach in decision making assumes the post-action utility to be higher, or, at least, not lower than the pre-action one. The key here is that both these utilities should be easy to calculate in tangible terms. The thought of exchanging individual lives for a greater common good is quite problematic to accept since sacrificing one's life for the unknown and, thus, the unquantifiable outcome, is far from being rational. Even if the person believes that her post-action utility from the suicide attack would be higher than her pre-action one she still cannot calculate the true value of the former. On the tactical level, the terrorists committing suicide attacks remain *in absentia* of the results of their actions. They die without comparing (in rational terms) their post-action utility with pre-action one. After all, no one had ever returned from the "other world" with the message that life after death is better or worse than life itself. In sum, there is no way to credibly quantify the individual utility in life and death: the suicide bombers might "go straight to paradise and enjoy the company of seventy-two virgins" or they might end up in hell (assuming that former is unarguably "better" than latter).[19]

Separate consideration should be given to the religion-based rationality. To start with, religion acts as an important motivator for human actions. Those who consider themselves true believers have the value-systems different from those who view themselves as atheists. This leads to different cognitive frameworks of reference: what is rational for a believer (i.e. justifiable from the point of view of post-action utility) can be as irrational for a disbeliever. Many religions have the rational-choice frameworks imbedded in their belief systems. The notions of "heaven" versus "hell" are more or less present in most of the religions and the paths to either one depend on how their followers had spent their lives. Compliance with the dogmas leads to better existence after life and vice versa–a sinful person would face worse future after death. The choice of the afterlife is rational as much as the person "chooses" to live in sin or in righteousness according to different religious institutional standards.

This fact, however, does not make religion either the independent or the intervening variable here. By their very virtues many religions are "outward" discriminatory and "inward" nondiscriminatory. This means that single religions discriminate between those of followers and those of other faiths; discriminate between what is considered "good" or "evil" but do not discriminate between all own believers or all own non-believers. Religious preferences are set equally for all own actors: all "righteous" people will face the afterlife corresponding to their earthly deeds and so will all the "sinners". The same reasoning is applied to own followers and those of other religions.

The problem of accepting religion as a factor-variable here is that the resulting rational choice framework would predict that all actors-believers would normally strive to achieve the same outcome: "Heaven" for Christians, "Nirvana" for Buddhist, "Shamayim" for the Hebrews or "Jennah" for Muslims. If the religion is assumed to be the predominant driving force among the "new" terrorists, another assumption should be equally true: that all believers would commit mass acts of suicidal or non-suicidal violence in their beliefs to take the lives of all other non-believers. If this is the case, then Mises's argument on the impossibility to prescribe universal happiness fails. When all actors supposedly have equally set preferences within the frameworks of their respective religions, this would predefine their modus operandi: killing heretics/infidels should be omnipresent across all religious actors. However, this view fails the test of scientific robustness and generalizability.[20] Suicidal acts are still quite rare and not all the true believers in paradise randomly attack the followers of other religions: events like the St. Bartholomew's Day Massacre are still outliers.

Economics of New Terrorism

From a purely economic standpoint, there is conflicting evidence of lethal efficiency of "new" terrorism. In absolute terms, suicide terrorism proves to be more efficient than its survivalist version: according to Caplan, "[a]n average suicide attack claims anywhere from four to over thirteen times as many victims as a non-suicide attack."[21] Pape, too, found that, although rare, suicide attacks account for almost half of the total human casualties for the same period.[22] However, the costs imposed on the target governments by all terrorists are exponentially lower than those of the conventional warfare. Mueller & Stewart's study corroborate this claim, "…annual terrorism fatality risks… are less than one in one million and therefore generally lie within the range regulators deem safe or acceptable, requiring no further regulations, particularly those likely to be expensive."[23] Charkavorti also points out that "…terrorism alone does not anywhere match the range of destruction caused by regular war, guerilla war and communal riots."[24] Finally, as the findings of Asthappan's statistical analysis show, from 1981 to 2006 "…suicide bombers are killing fewer people even though more incidents are occurring."[25]

In relative terms, however, the violent deaths of the so-called "hard targets"—high-level government officials—would have significantly higher policy-altering strategic impacts on the domestic and/or international environments than the deaths of ordinary citizens.[26] Yet even here rationality is relative: the assassination of the Archduke Franz Ferdinand of Austria in 1914 by Gavrilo Princip, a member of the Serbian terrorist organization "Black Hand," led to more significant political shifts than the killing of the Indian Prime Minister Rajiv Gandhi in 1991 by the LTTE, which caused no noteworthy international or regional political deviations.

Strategic Rationality

On the strategic level, i.e. long-term effects of the terrorist actions, individual terrorism may acquire some rationality traits. Strategic rationality postulates pursuing long-term goals by the actors. Here the distinction should be made into the actual perpetrators of terrorist attacks and the masterminds behind them. As Etzioni claims, "It may indeed be rational (in the sense of serving the goal) for the terrorist organizations and their leaders to send some of their recruits to die in acts of suicide; but that does not make it rational from the viewpoint of the individual recruits."[27]

Thus, the death of a suicide bomber as a result of her attack—whether premeditated or accidental—is not a sole variable in defining the overall rationality of the act. The factor of third party–organizers of terrorist attacks and not their immediate perpetrators–should be also taken into account.

Whether suicidal or survivalist, terrorist attacks usually tend to spare the lives of their organizers and risk only those of the actual perpetrators. The leaders of various terrorist groups and factions, according to Cowen, "…may have differing motivations than the lower-level troops. Often they organize attacks but do not conduct them personally."[28] From that standpoint the threat of being damaged as a result of any terrorist attacks for the individual group leaders is minimal. According to Pape, "even if many suicide attackers are irrational or fanatical, the leadership groups that recruit and direct them are not."[29] Finally, Neumayer and Plumper claimed that "the leaders of terrorist groups are predominantly rational and act strategically to reach their goal of gaining political influence on the political system of their home country."[30]

Group Level Rationality

Terrorism is mostly a collective endeavor with rare exceptions, such as the 2013 Boston marathon bombers. The individual terrorism is still an "aggregation of individual decisions and the behavior of a group can be explained with recourse to individual behavior."[31] Terrorist loners can claim their identity affiliations with the known terrorist organizations but this does not make them more than mere criminals in pursuit of their personal agendas. This, of course, does not mean that self-radicalization cannot happen on the individual level. The case of the Tsarnayev brothers is a perfect example of the terrorist identity based on the "imagined communities."[32] These terrorists had little or no contacts with the umbrella organizations and even attacked the country that had done nothing wrong to their ethnic external homeland in Chechnya.

This brings in the following point: radicalization and political motivations are two distinct instances of terror. For violence to be truly politically motivated it should have some sort of an institutionalized approval by specific groups. Otherwise the counter-terrorist efforts will stumble upon the problem of non-falsifiability. If every lone wolf chooses the identity that forces her to undertake premeditated acts of violence, then there is no political motivation as a separately existing phenomenon. As in the Tsarnayev brothers case, the discourse on their political motivations is futile: not only does it not yield any valuable insights into the reasons for the terrorists attacks it also distracts the counter-terrorism efforts by taking them in the wrong direction of organizational versus individual terror.

At the group level from the point of view of rational choice, the objective is to increase the aggregate expected utility for the whole group. The difference is in the degree of rationality in achieving goals by the "old" and "new" concepts of terrorism. Most of the "old" terrorist organizations represented and recruited from ethnically or ideologically limited circles of supporters and strived to achieve the benefits for these groups only. This was largely due to the specificity of their strategic objectives. Since most of them were advocating for social justice for their respective groups, their supporters would, naturally, come from these very communities.

The embodiment of traditional terrorism, ETA was almost entirely composed of the Basque nationals acting in Spain. Similarly, the RIRA recruits were Irish only: "unpropertied unmarried, young men of middle classes, increasingly disproportionately dominated by urban, skilled and socially mobile activists" throughout the world.[33] ASALA also used to replenish its ranks among young

Armenians, and so did the PKK: according to Kalyvas, "…it would be hard to find ethnicTurks fighting on the side of the PKK."[34] The "Narodnaya Volya" and the "Esers," too, were composed of ethnic Russians and operated within the Russian empire only.

From a tactical standpoint, the purpose of the "old" terrorism was to impose insurmountable human and economic costs on the opponent side to force the latter to undertake the sought policy change.[35] These goals, according to Pape, were pursued by "inflict[ing] enough pain on the opposing society to overwhelm their interest in resisting the terrorists demands and, so, to cause either the government to concede or the population to revolt against the government…"[36] With this, the "old" terrorism had limited goals to achieve: "to coerce a target government to change policy, to mobilize additional recruits and financial support, or both" or "…to provoke the target into a disproportionate response, radicalize moderates, and build support for its ambitious goals over the long term."[37] For instance, ASALA was pressing on Turkey to acknowledge the Armenian Genocide and eventually wanted "…to establish an independent and fully sovereign Armenian state comprising of the Armenian Soviet Republic and Turkish Armenia" without complete destruction of the Turkish Republic per se.[38] The RIRA and ETA advocated for the sovereignty of their respective ethnic groups–the Irish and the Basques–from the UK and Spain, correspondingly, without complete annihilation of their enemies' statehood or the supranational governance of the European Union. The same limited locate can be seen in PKK's actions: to gain increasing political rights for their group representatives and "to form an independent state of Kurdistan."[39] Such goals were, in principle, rationally achievable and showed the "behavior that benefit[ed] not only an individual but also a group the individual feels loyal to may also be considered as rational."[40]

On a strategic level, the limited objectives of the "old" terrorist organization made them act very selectively mostly aiming at "hard targets." By doing so, the terrorists were sending a clearly rational message to their successors: we will kill you if you continue to resist. Over 60 percent of ETA's victims were the members of the Spanish police, the military, and the politicians whereas the civilians were mainly the collateral or the "[i]nformers, drug dealers, entrepreneurs who do not succumb to the financial extortion, people with extreme right-wing ideology, or people involved in the "dirty war" against ETA."[41] ASALA was also notorious for targeting exclusively Turkish policymakers and mainly diplomats.[42] RIRA had developed the similar pattern in their attacks.[43] The FLMN also mostly targeted the governments' military and installations.[44] The LTTE's preferred hits were the military, police, government officials, and the private citizens associated with and supporting the policies of the Sri Lankan Government.[45] The "Narodovolci" and the "Esers" focused exclusively on "governor-generals, mayors, commanders of military regiments, heads of prisons, gendarmes, high-level policemen, bailiffs, constables, judges and prosecutors,…members of the State Duma and even the royal family."[46]

The "new" terrorism became a truly global enterprise: as the avant-garde of the new terrorism, al-Qaeda recruits Muslims and coverts all over the world. It does not have a "single, uniform recruitment process for a group; rather, there are as many recruitment processes as there are distinct regions and nodes in which the group operates."[47] Appearance of "new" terrorism also altered the overall strategy of politically motivated violence, which made it even more dangerous than ever. This change occurred as a result of moving away from the politically motivated attacks to staged shows of unexpected blanket violence on the organizational and individual levels. "New" terrorism has lost the privilege of the "exclusive club membership" and has turned into "franchised" tactics readily available to organized and individual actors: anyone with any background living anywhere can be self-radicalized and commit terrorist attacks on behalf of any organization and any cause.

Tactical Rationality

Tactically, the "new" terrorists are not engaged in the war of attrition but the war for full but less perceivable zero-sum victory. They wish not just to change the system where they live or to place their own policy entrepreneurs in charge: they want to destroy it completely and to create a new world order, the global Caliphate under Sharia law. Numerous Chechen terrorist organizations operating in Russia replicate this idea on a smaller, regional scale in the form of the Caucasian "Imarat," a Chechen word for an all-Muslim political entity in the Caucasus.[48]

The problem with such a strategy from the rational choice perspective is revealed on the level of strategic objectives. The "new" terrorists have no points of reference to credibly evaluate the expected utility of the proposed end state of their struggle. Al-Qaeda's proposed global Caliphate is related to its various historically existing forms, including the Rashidun, Umayyad, Abbasid and the Ottoman empires. However, even those "mini-caliphates" suffered from a steady desire of their people to move away from pure Islam and Sharia law to secularism. According to Arnason and Stauth, "[t]he history of Islamic states appears as a long-drawn-out retreat from full exercise of religious authority. The early caliphate…was replaced by a monarchy, which… tended to replace the direct authority of religion with 'group feeling and the sword'…"[49] In case of both al-Qaeda and the Chechen terrorist organizations, strategic rationality rests on their ephemeral promise to the followers without any rational framework of reference that they would be better off in the Global Caliphate than without it.

From the point of view of tactical rationality the "new" terrorism can be quite rational due to its specific targeting pattern: indiscriminate violence against civilians. Due to the fact that all terrorism, but mostly so its new version is essentially a show in need of its audience, according to Stohl, the latter's "… victims and all that destruction were not as important to the perpetrators as the audience around the world that viewed that destruction."[50] Crenshaw also supports this change in wider targeting of "new" terrorists groups by saying, "The victims or objects of terrorist attack have little intrinsic value to the terrorist group but represent a larger human audience whose reaction the terrorists seek."[51] The change in asymmetric tactics happening all over the world is backed up by the statistical data. A 2008 RAND study identified 3,827 civilian deaths and over 8,000 injuries with only 110 military deaths and 221 injuries in al-Qaeda attacks between 1994 and 2007.[52]

Instead of sending the personalized message to their targets, by attacking unknown and mostly civilian actors, the "new" terrorists indirectly aim at the "hard targets" to instigate the political change. This is a significant departure from the targeting modus operandi of the "old" terrorists for whom both victims and targets were the same. The "new" terrorists' demands are delivered indirectly by the survivors of the attacks. In these cases and especially when the terrorist acts threaten to spoil the re-election prospects, some governments tend to succumb to terrorists' demands. There is nothing that the democratically elected governments hate to see more than the deaths of their innocent constituencies. To a point, such tactics can, indeed, help terrorists to succeed. More recent examples of the tactical rationality include the withdrawal from Iraq of the Philippines troops shortly after their truck driver was kidnapped by the extremists and removal of the Spanish troops as a result of the pre-election promise of then Prime Minister Zapatero after the 2004 Madrid Bombings, shortly followed by Honduras and the Dominican Republic.[53] This, however, did not have a desired effect on the overall long-term counter-terrorist mission of the coalition forces in Iraq.

Conclusion

The difference in applying the rational choice framework to the study of motivators and behavior of the "old" and "new" terrorists is substantial. The rationality-based approach presupposes the counter-terrorism efforts based on the rationality of the government actors fighting with terror.

Such an approach would be successful in cases of the "old" terrorists who had clearly presented and tangible goals. This made their behavior more or less predictable and easy to target due to the clearly identifiable sources of threat. On the contrary, the "new" terrorists are unpredictable in their global reach, mutating forms and vague objectives. The same counter-terrorist operations that applied in cases of the "old" terrorists—small-scale operations, such as in Ireland and the Land of Basks, or larger military interventions, as in case of Afghanistan—are likely to fail here.

The "Global War On Terror" coined by President Bush after the September 11 attacks is a very dangerous term from the point of view of absence of an exit strategy. The "new" terrorists are not fighting for any specific or tangible goals. Their aim is to fight for the sake of fighting. This is the inherent difference of "new" terrorism from its predecessor and its grave danger: absence of clearly defined and attainable end states for the terrorists themselves. Global or even regional caliphates and the universal Sharia rule are utopia primarily for the terrorists themselves as well as the counter-terrorist circles.

Absence of rationality makes the "new" terrorism nothing but a fear show with the sole purpose of sustaining further shows with the increasing number of audiences around them. Success of terrorist attacks should be measured not in terms of its victims–as shown above; from purely rational perspective the lethality rate of terrorism is very low if compared with other threats. The United States' troops may withdraw from Afghanistan but this would in no way mean defeat or victory for terrorists. The only way a show would end is when the audience would stop buying tickets. The philosophical school of empiricism postulates that the world exists as long as we acknowledge its existence.[54] The world is, essentially, a combination of the matters that came into being because of the actors' desire to recognize them. Similarly, the "new" terrorism would remain a threat until the counter-terrorism cycles continue to perceive it as such. Once the audience stops paying attention to multiple tapes of caved terrorists broadcast by global television networks, to the ephemeral jihads sporadically launched in different areas of the globe by numerous terrorist cells and affiliates against different nations, and starts treating it as an ordinary crime requiring relevant punishment, the pandemics of terrorism will gradually evade.

Notes

[1] Schmid counted up to 190 definitions of terrorism between the 1930s and 1980s; Alex P. Schmid, and A.J. Jongman, *Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature* (New Brunswick, NJ: Transaction, 1983).

[2] Paul K. Davis and Kim Cragin, eds., "Social Science for Counterterrorism. Putting the Pieces Together," *RAND Corporation Monograph Series*, 2009, 170, http://www.rand.org/pubs/monographs/2009/RAND_MG849.pdf.

[3] Bryan Caplan, "Terrorism: The Relevance of the Rational Choice Model," *The Political Economy of Terrorism* 128, no. 1/2 (2006): 91-107; Martha Crenshaw, "The Causes of Terrorism," *Comparative Politics* 13, no. 4 (1981): 379-399; Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (2006): 49-80; Robert A. Pape, "The Strategic Logic of Suicide Terrorism," *American Political Science Review* 97, no. 3 (2003): 1-19; Anthony Oberschall, "Explaining Terrorism: The Contribution of Collective Action Theory," *Sociological Theory* 22, no. 4 (2006): 26-37; Martin C. Libicki, Peter Chalk and Melanie Sisson, "Exploring Terrorist Targeting Preferences," *RAND Corporation Monograph Series*, 2007, http://www.rand.org/pubs/monographs/2007/RAND_MG483.pdf.

[4] Eric van Um, "Discussing Concepts of Terrorist Rationality: Implications for Counter-Terrorism Policy," (working paper 22, Economics of Security, 2009), 9.

[5] William H. Riker, "The Political Psychology of Rational Choice Theory," *Political Psychology* 16, no.1 (1995): 37.

[6] Herbert A. Simon, "Rationality in Political Behavior," *Political Psychology* 16, no. 1 (1995): 58.

[7] Bryan D. Jones, "Bounded Rationality," *Annual Review of Political Science* 2 (1999): 297–321; Kristen R. Monroe and Kristen H. Maher, "Psychology and Rational Actor Theory," *Political Psychology* 16, no. 1 (1995): 2.

[8] For additional accounts of the discourse on the logics of appropriateness and expected consequentiality see the following works: James G. March and Johan P. Olsen, *Ambiguity and Choice in Organizations* (Bergen, Norway: Universitetsforlaget, 1976); James G. March and Johan P. Olsen, *Rediscovering Institutions* (New York: Free Press, 1989); James G. March and Johan P. Olsen, *Democratic Governance* (New York: Free Press, 1995); James G. March and Johan P. Olsen, "The Institutional Dynamics of International Political Order," *International Organization* 52, no. 4 (1998): 943–969.

[9] John R. Oneal, "The Rationality of Decision Making During International Crises," *Polity* 20, no. 4 (1988): 601.

[10] William H. Riker, "The Political Psychology of Rational Choice Theory," 24.

[11] Ludwig von Mises, *Human Action* (Chicago: Contemporary Books, Inc., 1966), 19.

[12] Monroe and Maher, "Psychology and Rational Actor Theory," 1-21.

[13] Bryan D. Jones, "Bounded Rationality," 306; Herbert A. Simon, "Human Nature in Politics: The Dialogue of Psychology with Political Science," *The American Political Science Review* 79, no. 2 (1985): 293-304. doi:10.2307/1956650.

[14] Kjell Goldmann, "Appropriateness and Consequences: The Logic of Neo-Institutionalism," *Governance: An International Journal of Policy, Administration, and Institutions* 18, no. 1 (2005): 44; James G. March and Johan P. Olsen, "The Logic of Appropriateness," in *The Oxford Handbook of Public Policy*, ed. Robert E. Goodin et al. (Oxford: Oxford University Press, 2008), 4.

[15] Tyler Cowen, "Terrorism as Theater: Analysis and Policy Implications," *Public Choice* 128, no. 1/2 (2006): 238.

[16] Mark Harrison, "An Economist Looks at Suicide Terrorism," *World Economics* 7, no. 4 (2006): 1.

[17] Todd Sandler, "Collective Action and Transnational Terrorism," *World Economy* 26, no. 6 (2003): 785.

[18] Caplan, "Terrorism: The Relevance of the Rational Choice Model," 98.

[19] Ibid., 97.

[20] Lena Soler et al., ed., *Characterizing the Robustness of Science: After the Practice Turn in Philosophy of Science* (New York: Springer, 2012).

[21] Caplan, "Terrorism: The Relevance of the Rational Choice Model," 94.

[22] Pape, "The Strategic Logic of Suicide Terrorism," 1-19.

[23] John Mueller and Mark G. Stewart, "Hardly Existential: Thinking Rationally About Terrorism," *Foreign Policy,* (2 April 2010), http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardlyexistential

24. Robi Chakravorti, "Terrorism: Past, Present and Future," *Economic and Political Weekly* 29, 36 (1994): 2343.

25. Jibey Asthappan, "The Effectiveness of Suicide Terrorism," *Journal of the Washington Institute of China Studies* 5, no. 1 (2010): 22.

26. Eli Berman, and David D. Laitin, "Hard Targets: Theory and Evidence on Suicide Attacks," (December 2006), http://econ.ucsd.edu/~elib/Hardtargets.pdf.

27. Amitai Etzioni, "Rational Actors: Neither Mad nor M.A.D.: The Meanings of Rationality, Rogue States and Terrorists," *Defense & Security Analysis* 26, no. 4 (2010): 434.

28. Cowen, "Terrorism as Theater: Analysis and Policy Implications," 237.

29. Pape, "The Strategic Logic of Suicide Terrorism," 2.

30. Eric Neumayer and Thomas Plumper, "International Terrorism and the Clash of Civilizations," *British Journal of Political Science* 39, no. 4 (2009): 712.

31. Um, "Discussing Concepts of Terrorist Rationality: Implications for Counter-Terrorism Policy," 10.

32. Benedict Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (London: Verso, 2006).

33. Peter Hart, "The Social Structure of the Irish Republican Army, 1916-1923," *The Historical Journal* 42 (2009): 207;

34. Stathis N. Kalyvas, "Ethnic Defection in Civil War," *Comparative Political Studies* 41, no. 8 (2008): 1043-1068.

35. Andrew Mack, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict," *World Politics* 27, no. 2 (1975): 175-200.

36. Pape, "The Strategic Logic of Suicide Terrorism," 4.

37. Libicki, Chalk and Sisson, "Exploring Terrorist Targeting Preferences,"; David A. Lake, "Rational Extremism: Understanding Terrorism in the Twenty-first Century," *Dialog-IO* (2002): 26.

38. Paul Wilkinson, "Armenian Terrorism," *The World Today* 39, no. 9 (1983): 346.

39. Hatem Mukhlis, "Voting Yes to Chaos," *The New York Times*, 18 October 2005, 27.

40. Um, "Discussing Concepts of Terrorist Rationality," 9.

41. Ignacio Sánchez-Cuenca, "The Persistence of Nationalist Terrorism: The Case of ETA," in *Violent Non-State Actors in Contemporary World Politics*, Kledja Mulaj, ed. (New York: Columbia University Press, 2010): 24.

42. "Turkish Diplomats Killed by Armenian Terrorists," Assembly of Turkish-American Associations, 2011, http://www.ataa.org/reference/diplomats.html.

43. "Targets of the Irish Republican Army," Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, accessed 27 September 2017, http://www.start.umd.edu/gtd/search/Results.aspx?chart=target&search=Irish republican army&count=100.

44. "Targets of the Farabundo Marti National Liberation Front," Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, accessed 27 September 2017, http://www.start.umd.edu/gtd/search/Results.aspx?charttype=pie&chart=target&search=FML.

45. "Targets of the Tamil Tigers," Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, accessed 27 September 2017, http://www.start.umd.edu/gtd/search/Results.aspx?charttype=pie&chart=target&search=Tamil%20Tigers.

46. "History. Terrorism in Russia," K.G. Razumovsky Moscow State University of Technology and Management, http://mgutm.ru/stopteror/histori.php.

47. Scott Gerwehr and Sara Daly, "Al-Qaida: Terrorist Selection and Recruitment," in *McGraw-Hill Homeland Security Handbook*, David Kamien, ed., (New York: McGraw-Hill Companies: 2006), 75.

48. The following are among the most notorious Chechen terrorist groups: the Supreme Military Majlisul Shura of the United Mujahidin Forces of the Caucasus; the Congress of the Peoples of Ichkeria and Dagestan; the Caucasus Front of the Military Forces of Chechen Republic Ichkeria.

49. Johann P. Arnason and Georg Stauth, "Civilization and State Formation in the Islamic Context: Re-Reading Ibn Khaldun," *Thesis Eleven* 76, no. 1 (2004): 39.

50. Michael Stohl, "Old Myths, New Fantasies and the Enduring Realities of Terrorism," *Critical Studies on Terrorism* 1, no. 1 (2008): 13.

51. Crenshaw, "The Causes of Terrorism," 379.

52. Seth G. Jones and Martin C. Libicki, "How Terrorist Groups End. Lessons for Countering Al Qa'ida," *RAND Corporation Monograph Series*, 2008, http://www.rand.org/pubs/monographs/2008/RAND_MG741-1.pdf.

53. James Glanz, "Hostage Is Freed after Philippine Troops Are Withdrawn from Iraq,*" New York Times*, 21 July 2004, http://www.nytimes.com/2004/07/21/world/hostage-is-freed-after-philippinetroops-are-withdrawn-from-iraq.html.

54. Locke, John, *An Essay Concerning Human Understanding* (Nabu Press, 2010).

Engaging Non-State Security Providers

Whither the Rule of Law?

Timothy Donais, PhD*

The rule of law has long been a core pillar of security sector reform (SSR) programming. To the extent that SSR seeks to ensure that security forces are not only effective but also accountable to both the state and its citizens, the proposition that accountability is best guaranteed by embedding security governance within a rule of law framework has, with a few notable exceptions, gone relatively uncontested despite SSR's uneven track record. In the context of post-conflict transitions in particular, the standard SSR narrative has been that the (re)-consolidation of coercive power within the hands of the state (in a Weberian sense) is both justified and legitimized by the parallel establishment of legal and institutional frameworks that serve to constrain and limit the uses and abuses of this power. Just as SSR lies at the core of the contemporary statebuilding agenda, part and parcel of a larger effort to create capable, accountable and responsive states, the rule of law, as a set of principles and practices aimed at bringing political and socio-economic relations within a predictable, transparent framework of enforceable rules, remains central to the contemporary SSR agenda.[1]

That this narrative remains compelling both in terms of its internal logic and in terms of how most SSR practitioners differentiate between successful and unsuccessful security sectors goes a long way towards explaining the unease with which the growing emphasis on non-state security provision has been received

*Professor Timothy Donais joined Laurier in 2008, after having taught for four years in the political science department at the University of Windsor. His research focuses on post-conflict peacebuilding, and he is currently engaged in a multi-year research project, funded by the Social Science and Humanities Research Council of Canada, examining issues of 'local ownership' in peacebuilding processes. Dr. Donais is the author of *The Political Economy of Peacebuilding in Post-Dayton Bosnia* (Routledge, 2005) and, more recently, the editor of *Local Ownership and Security Sector Reform* (Lit Verlag, 2008).

Timothy Donais, "Engaging Non-State Security Providers: Whither the Rule of Law?," *Stability: International Journal of Security and Development*, 6, no. 1 (2017), DOI: http://doi.org/10.5334/sta.553.

within the wider SSR community. Non-state security providers, in this context, include those actors—from militias to neighborhood watch groups to traditional chiefs—who command coercive power, and provide a measure of security and protection to particular communities and/or across specific territories, outside of the context of formal state security provision. Hybrid forms of security provision, in which state and non-state security providers co-exist and overlap, are increasingly acknowledged as the reality in many fragile and conflict-affected states. Typically, however, such security 'orders' are decidedly *disorderly*, inherently unstable, and sometimes violent, presenting myriad points of friction where the claimed and contested jurisdictions of various security providers overlap. While they may be acknowledged, such hybrid security arrangements have rarely been considered viable alternatives to conventional SSR approaches. At best, they have tended to be viewed as ephemeral features of the transitional landscape, to be tolerated until such point as the state can take up its rightful monopoly over the legitimate use of force.

While SSR is not easily disembedded from these state-centric presumptions, evidence is slowly accumulating that hybrid forms of security governance may be more durable, more effective, and less easily-displaced than previously thought. While it may be premature to declare, as Bruce Baker has, that 'the future is non-state,' the case for embracing hybridity in SSR programming is gaining strength.[2] It also rests on decidedly pragmatic grounds. As Kate Meagher has observed, the willingness to re-consider the viability of hybridity as a model of security governance has much to do with the search for less elaborate and less costly forms of governance, and with a growing recognition that existing systems of security governance should be judged for what they are, rather than what outsiders would like them to be.[3] Consistent with broader critiques of liberal peacebuilding, this openness to hybridity is also a reaction to the hubris and 'arrogant managerialism' of most SSR policy interventions, marked by unrealistic and unachievable social engineering ambitions and ongoing efforts to jam the complex realities of weak and conflict-affected states "into a procrustean bed of pre-set rule of law templates."[4]

This paper explores the role of non-state security provision in SSR contexts against the wider backdrop of an ongoing normative and policy commitment on the part of donors to embed SSR within a rule of law framework. In doing so, it contemplates the possibilities for a 'post-liberal' (if not necessarily post-rule of law) SSR agenda, distinguished from its liberal precursor by a commitment to fashioning SSR strategies on the basis of existing socio-political realities within the society in question rather than on idealized (and possibly unattainable) end-points. This emphasis on starting conditions rather than (or at least in addition to) ultimate outcomes—consistent with Amitai Etzioni's argument that, given the limits of international influence, it makes more sense to build on existing structures and trends "rather than seeking to fashion new ones out of whole cloth"—imposes considerable demands on outside interveners in terms of understanding the local context in all its dynamic complexity.[5] It demands, in short, a systems-analysis approach to SSR, based on a careful reading of the relevant actors, the incentive structures they face, the institutional and relational dynamics that connect them, and the location of potential levers of change. It also leads, almost inevitably, to a form of SSR that is based on the balancing and bridging of existing political forces rather than on Weberian monopolies contained and constrained by a framework of laws capable of regulating political life while simultaneously standing outside of politics. At the same time, while it is unrealistic to expect donors to set aside long-standing commitments to the rule of law in their SSR interventions, it may also be unnecessary. Indeed, the paper makes the case that viewed as one component—albeit one to be progressively expanded over time—of a complex and evolving accountability framework for security provision, the rule of law remains central to the broader SSR enterprise.

The remainder of the paper unfolds as follows. The next section unpacks the key foundational premises of conventional SSR, with a particular focus on the prominence of monopoly and accountability and the enormous challenges of achieving either—let alone both—within the standard timeframes of most contemporary international interventions. Next, the paper considers the awkward relationship between non-state security providers and the rule of law, while at the same time outlining why hybrid security arrangements involving a combination of state-based and non-state security provision are likely to be more conflictual than collaborative. The third section outlines a vision for longer-term security sector evolution grounded in a 'rules-based' framework, emphasizing the emerging ability of state institutions to regulate, rather than monopolize, the provision of security. The conclusion revisits the overall argument, suggesting that to the extent that SSR remains about the systemic transformation of security provision, the rule of law continues to provide an important set of strategic guideposts to guide this process.

Conventional SSR: The Merger of Monopoly and Accountability

Louise Andersen has observed that the so-called monopoly model of SSR—central to the project of establishing liberal peace in fragile states—"involves not merely the taming of the Hobbesian Leviathan but the actual establishing of the Leviathan."[6] This characterization nicely underlines the intertwined principles of monopoly and accountability upon which conventional SSR is premised, while also hinting at the epic scale of the undertaking. It has been clear for some time that SSR's weak empirical track record has a great deal to do with the gap between lofty principles and on-the-ground realities, and between the broader ambition of the SSR agenda and the time, resources, and political capital required to transform that ambition into reality.

On the monopoly question, perhaps the most important insight to have emerged from the last quarter-century of SSR programming concerns the limited remit of the state—and its security and justice apparatus—across a wide range of fragile and conflict-affected environments. It is now commonly asserted and widely accepted (if difficult to verify) that upwards of 80 percent of security and justice provision in the states that are the beneficiaries of SSR programming is provided by non-state actors.[7] Indeed, part of the very essence of state weakness or fragility relates to the inability of governments to exercise effective control over territory, while conflict leads to the further fragmentation of security provision. Given these realities, in most cases conventional SSR programming has struggled to meet the challenge of engineering massive transfers of power from non-state actors—most of whom have proven to be reluctant collaborators—to state-level actors.

As Ken Menkhaus has noted in the case of Somalia, efforts to strengthen the formal security sector in that country are "swimming against powerful currents"; non-state security providers are not only more capable than state-level actors across most of the country, they have also developed powerful economic interests in the maintenance of the status quo.[8] While Somalia may be an extreme case of fragmented security provision, the failure of the monopoly model of SSR to deliver on its core premise is a common theme across a broad cross-section of post-conflict cases.

Conventional SSR has arguably been no more successful in the achievement of its second core principle: ensuring that those who wield coercive force behave responsibly and can be held accountable for their actions. It is here where the rule of law intersects most directly with security governance; in the typology of Thomas Carothers, this represents 'type three' rule of law reform, aimed at ensuring government compliance with the law and, more generally, putting in place robust mechanisms to constrain the powerful.[9] Particularly in the context of volatile and insecure environments, it should come as no surprise that those in positions of privilege see little self-interest in limiting their power by subjecting it, and themselves, to the rule of law. Indeed, as Agnes Hurwitz has noted more generally, "programs seeking to strengthen or re-establish the rule of law in peacebuilding contexts have rarely achieved their nominal objectives of delivering human rights, security or development."[10] This is due, in large part, to the reality that the rule of law is about changing norms at least as much as it is about building institutions, and normative change is almost invariably a long-term endeavor.[11] For domestic elites especially, respect for and adherence to abstract principles such as justice, accountability, and transparency is a tough sell in cost-benefit terms, particularly when set alongside the more prosaic pursuit of political and economic self-interest. Further, as Alex Berg has demonstrated, rule of law in conflict-affected contexts rarely emerges as a result of elites 'coming to enlightenment', but is rather the consequence of specific, and relatively uncommon, patterns of state-society relations—notably regimes rooted in broad or fragmented coalitions and lacking easy access to revenue—that alter the incentive structures facing elites in ways that make it more likely for them to accept legal and institutional constraints.[12]

Given the difficulty of realizing the enormous ambition that lies at the heart of the conventional SSR paradigm—vis-à-vis both restoring monopolies over the legitimate use of force and embedding security governance within a robust legal framework—the search for alternative and more realistic models has become increasingly urgent. In this sense, critiques of conventional SSR echo Marina Ottaway's broader critique of the democratic reconstruction model as attractive in theory but unworkable in practice, given the enormous gulf between ground-level realities and idealized endpoints.[13] Like Ottaway, advocates of second-generation SSR seek more realistic and less hubristic approaches that nevertheless retain a fundamental commitment to improving both human and state security within fragile and conflict-affected contexts. While hybrid approaches promise such realism by eschewing formal templates in favour of strengthening actually-existing mechanisms of security provision, almost by definition hybridity also entails the reconciliation of radically different practices and principles. How to go about reconciling the recognition of non-state security provision with an ongoing commitment to rule of law promotion presents one such paradox.

Non-State Security Providers and the Rule of Law: An Uneasy Relationship

While the flaws of both liberal peacebuilding and conventional SSR have been exposed in recent years, in large part due to the incapacity of each framework to bridge the gap between promise and performance, the rule of law continues, somewhat remarkably, to enjoy deep and near-uncontested legitimacy. This is perhaps even more remarkable given that the rule of law can be considered *primus inter pares* among all of the core principles underpinning liberal interventions in fragile and conflict-affected states: the rule of law is, in other words, an essential background condition for the achievement of key public goods associated with the modern paradigm of good governance, from economic development to human rights to democratization.

While there is a rich literature debating both its meaning and its substantive content, at its core the rule of law can be defined, in the words of Thomas Carothers, "as a system in which the laws are public knowledge, are clear in meaning, and apply equally to everyone."[14] The rule of law, as Carothers also notes, is fundamentally dependent on the fairness, competency, and efficiency of core legal institutions such as courts, prosecutors, and police, and more generally on the embeddedness of government and governance within a comprehensive legal framework.[15]

Two aspects of this definition appear especially relevant for the purposes of thinking about the relationship between the rule of law and non-state security provision in transitional contexts. The first is its undeniably statist framing; while most conceptions of the rule of law contain articulations of the rights of citizens to due process *and* equality before the law, the core puzzle faced by rule of law reformers in fragile and conflict-affected states is ultimately how to both enable and constrain government power, on the wider principle of 'no power without accountability'.[16] As Lisa Denney has suggested, however, the terms 'non-state' and 'informal' remain analytically useful when thinking about hybrid security arrangements *precisely* because "they denote the broad set of arrangements that, in some way, operate beyond the state's accountability net."[17] Acknowledging the reality of *non-state* security provision, in other words, remains a challenge to thinking about SSR as merely the extension of the rule of law into the security realm, in large part because the legitimacy of non-state security providers tends to be grounded in *extralegal* foundations.

The second aspect of the Carothers' definition worth noting in this regard is its seemingly apolitical nature, with laws and their guardians cast as neutral arbiters of political and social life.[18] Framing the rule of law this way, however, conceals as much as it reveals. Given that laws themselves, being little more than words on paper, have no inherent authority, genuine rule of law—as opposed to rule *by* law—requires a robust and durable intersubjective agreement on the part of the constituent elements of any society, especially those in positions of power, to submit themselves to the authority of abstract law. In this sense, acceptance of the rule of law on the part of both rulers and ruled constitutes—at least in liberal democratic contexts—a central component of the social contract through which state-society relations are governed. Historically, the emergence of social consensus on the centrality of the rule of law as a bedrock of governance has come only through prolonged, and often violent, political struggle (think of England's long journey from the Magna Carta to modern constitutional monarchy), the outcome of which is by no means pre-determined. The fundamental challenge facing those seeking to embed the rule of law within conflict-affected states is, therefore, that few good models exist for how to short-circuit the messy and violent dynamics of political contestation in order to build consensus among differentially-empowered (and mutually-distrustful) social actors on the wisdom, desirability, and legitimacy of the rule of law as an overarching governance principle. Ultimately, as Janice Stromseth et al have suggested, "few rule of law theorists have grappled with the issue of *how* rule of law cultures can be created."[19]

While holding to the conviction that the rule of law provides the only durable, sustainable framework for responsible, accountable security governance, then, conventional security sector reform models have never really offered a convincing theory of change for how to bring this about. Nor have they fully come to terms with the reality that, in most cases, both state and non-state security provision will continue to co-exist for an indefinite interim, drawing on a wide range of different sources of legitimacy, offering variable levels of security or insecurity, and forcing citizens—as security consumers—to navigate what are often security terrains of exceptional complexity.[20] For external reformers, such terrains are no less difficult to manage (even if less existentially threatening), in part because of the difficulty of distinguishing good actors from bad ones and in part because of the inherent limits on external leverage. Consequently, donors continue to focus on reforming state-level security and justice systems, while overlooking the majority of mechanisms through which justice and security are delivered on a daily basis.[21] Conversely, beginning to think in terms of 'interim security arrangements', even if the interim in this context may be measured not in years but in decades or even generations, necessarily requires a willingness to engage with—rather than attempt to circumvent or transcend—the messy realities of actually-existing security arrangements.

One of the earliest efforts to frame this kind of engagement in policy terms was provided in 2011 by the Development Assistance Committee of the OECD.

Highlighting the centrality of legitimacy to larger debates around governance, the OECD-DAC made the case that 'grounded legitimacy'—pursued through "deliberate strategies for supporting the marriage of indigenous, customary and communal institutions of governance with introduced, Western state institutions, with a view to creating constructive interaction and positive mutual accommodation"—should be a key guiding principle in efforts to rebuild fragile or war-torn states.[22] While the idea of grafting Western norms and institutions onto pre-existing systems that resonate socially and culturally with local populations is compelling, in the particular realm of security provision such 'marriages' between state and non-state actors are likely to be especially fraught. To highlight such tensions is not to deny that collaborative security arrangements across the state/non-state divide can, and do, exist independent of outside intervention;[23] for example, Baker has described precisely this kind of collaboration between state authorities and customary structures in Somaliland. However, it should be noted that such arrangements may be the exception rather than the norm precisely because of the breadth and range of actors that comprise security systems in conflict-affected environments, the particular nature of power relations in such contexts, and tensions inherent in the private delivery of public security.

In the first place, the universe of non-state security actors is remarkably varied, ranging from traditional chiefs to secret societies, and from neighborhood watch groups to gangs, militias, and warlords. Such actors may have long-standing bonds of reciprocity with their client communities, or they may have emerged from within the conflict context with little history and few direct connections with particular communities. William Reno, for example, has distinguished between protective and predatory militias, with the former dependent on local communities for resources and connected to them by dense webs of values, beliefs, and identities.[24] Complicating matters, of course, is the reality that particular actors may simultaneously be perceived as both predatory and protective by different segments of the communities with whom they interact, with perceptions varying significantly across time. More generally, Baker and Scheye have argued that there are no *a priori* grounds for assuming that non-state actors are less capable than non-state actors of upholding human rights or being held accountable, since they may "more accurately reflect local beliefs and needs and are regarded by local people to be more legitimate."[25] Certainly, the varied experiences of non-state security provision across a range of cases demonstrate that the rule of law is not a pre-requisite for accountability: despite the dramatic power differentials between the providers and recipients of security, there is some evidence of warlords being 'tamed' by links with more traditional forms of organization, and of militias – particularly those that are embedded within specific communities–being 'civilized' by social pressure.[26] Social embeddedness, however, offers no durable guarantee that the 'protected' will be able to reliably hold their 'protectors' accountable, given the shifting and unpredictable nature of most informal governance arrangements: in other words, non-state security provision can just as easily erode as uphold the security of particular communities. Perhaps unsurprisingly then, context remains all-important.

Second, as SSR has always been part of a larger project centred around rearranging the manner in which power is exercised and controlled within particular societies, hybrid security arrangements are as likely to generate competitive power dynamics—both across the state/non-state divide and among non-state security actors—as they are to yield respectful and mutually-reinforcing cohabitation among differentially-situated security providers. There is, on the one hand, the reality that in such contexts the state, given the high stakes involved and the long-standing presumption that security provision is at the very core of what defines contemporary statehood, is unlikely to enthusiastically embrace an emerging norm of hybrid security governance.[27] At the same time, the lingering insecurity of the post-conflict 'moment' and the political economy of private security provision—in contexts of resource scarcity, many security providers find it difficult to resist the temptation to leverage coercive authority for either political advantage or economic gain—point to real risks that in the absence of some form of regulatory framework, ongoing struggles for power and authority could easily turn ugly. Indeed, South Sudan's post-independence descent into civil war can be read precisely through this lens of competitive security dynamics.

Third, as Baker and Scheye have noted, both justice and security are, at their core, public goods, a reality which sits awkwardly with hybridized security arrangements.[28] While there is of course no guarantee that public security providers will take seriously their responsibilities for public security provision—indeed, post-conflict environments are sadly replete with examples of the exploitation of public office for private gain—there is at the very least a normative expectation that over time, public security forces will act in the name of public security. Hybridity, conversely, implies multi-layered and overlapping security provision, with non-state actors in particular providing security to selected slices of a particular population, while representing agents of *insecurity* to others. In such contexts, the provision of 'public security' may be uneven and incomplete at best, while the prospects for encouraging a multiplicity of non-state security providers to embrace a public security ethos remain decidedly uncertain.

In light of such concerns, there remain grounds for caution about the long-term capacities of hybrid security arrangements to offer superior outcomes, in human security terms, to the long–suffering populations of conflict-affected states. Indeed, writing about the specific context of Africa, Kate Meagher warns of the dangers of inverting, rather than overcoming, the essentialist tendencies of previous thinking around security governance. As she suggests, to the extent that "the condemnation of non-state order as institutionally destructive has been replaced by its celebration as a vehicle of embedded forms of order and authority," there's a risk of failing to make important distinctions between constructive and corrosive forms of non-state order.[29] At the same time, in the rush to embrace 'actually-existing' security governance arrangements in lieu of striving for ideal-type outcomes, there is also a danger of losing sight of the reality that SSR is, at its core, about systemic change; indeed, one of the characteristics of the literature on non-state security governance has been an emphasis on tactical improvements to ground-level security arrangements at the expense of a more sustained focus on how wider security systems might be transformed over longer timeframes. I take up this question in the following section, suggesting that even in the context of security hybridity the rule of law, as a set of overarching principles of governance, may continue to offer an important set of guideposts that enable SSR practitioners to go beyond acknowledging the role played by non-state security providers in SSR contexts towards engaging with them in constructive, forward-looking ways.

Squaring the Circle – A Qualified Defence of the Rule of Law

One starting point for reconciling a continued commitment to rule of law promotion with a recognition of the reality of non-state security provision is the realization that most advocates of non-state security strategies are not as radical as they may appear at first glance. Either implicitly or explicitly, most continue to acknowledge a crucial—if somewhat transformed—role for the state within any evolving security governance framework. Likewise, most also continue to acknowledge the imperative of enveloping security governance within an enforceable rules-based framework. Baker and Scheye, for example, posit that regardless of the specific identity of the actors who *provide* security services:

> A principle function of the post-conflict and fragile state might be to monitor, license, and regulate the activities of non-state service providers. This is no longer a state defined in terms of a monopoly control over violence and coercion, but rather a highly circumscribed and limited state, working in varying unique partnerships and associations with non-state actors and CSO's.[30]

Michael Lawrence, similarly, in the context of a broader argument around the need to develop non-state SSR strategies, defends the notion of the regulatory state, empowered to set broad parameters for security provision, "particularly standards of human rights, accessibility and accountability."[31] Even in a context such as Somalia, the classic case of a 'mediated state' where weak central authorities have little choice but to broker deals with powerful non-state actors, Menkhaus concludes that state regulation of private security provision remains a possibility, albeit part of a long, convoluted process "by which state authorities eventually gain primacy over non-state and sub-state security providers."[32]

What emerges from these accounts, therefore, are hints at a long-term, incrementalist theory of security sector transformation aimed at facilitating a gradual shift in the balance of power from non-state to state-level actors, while at the same time repositioning the state as a regulator, rather than monopolizer, of security provision. Crucial to this account of change is the state's developing capacity (and legitimacy) to make and implement rules, laws, and regulations. While the state might have little choice but to defer to the capacity/legitimacy of non-state security providers in the short-term, and share authority with these same actors over the medium term, over the longer term the sovereign state is expected to assert its primacy—through what Menkhaus terms a combination of negotiation, confrontation, and cooperation—over the non-state in matters of security governance.[33] None of this, of course, is necessarily inconsistent with the shorter-term imperative of making 'actually-existing' security governance work better through ongoing efforts to build partnerships, facilitate collaboration, and ease friction across the broad range of security providers.

Seen in this light, a looser conception of how the rule of law might over time link state and non-state, security provider and security consumer, and different kinds of security providers with each other may still provide a reasonably compelling framework for international engagement with the security sectors of fragile and conflict-affected states. While avoiding the perils of both 'legal orientalism' and externally-driven social engineering, the strength of such a vision may lie in its ability to bridge the gap between the imperative of starting SSR from actually-existing conditions and Alice in Wonderland's dictum that you need to know where you are going if you ever hope to get there.[34] In this sense, then, conceptualizing SSR in terms of the gradual expansion of the state's ability to bring security provision within a common framework of rules provides at least some direction and focus to the generic call to 'engage' non-state security providers, without being overly prescriptive in terms of eventual outcomes.

The importance of holding onto at least a thin vision of how external interveners imagine change in security systems unfolding over time should not be underestimated, especially given the gap between the need to think about change in systemic terms and the chronic inability of international actors—despite ritual nods to the importance of 'holism' as a key SSR principle—to engage with the security sectors of conflict-affected states as complex systems. Indeed, the failure to cooperate, coordinate, and plan strategically remains, in many ways, the Achilles' Heel of the entire SSR enterprise, which in too many cases still unfolds more as a series of discrete, time-bound, and unconnected projects than as a coherent and integrated blueprint for shifting conflict-affected societies along a continuum from insecurity to security. Thus, when Michael Lawrence—in an otherwise excellent discussion of hybrid security governance—calls for the development and implementation of non-state SSR strategies, it is not entirely clear who, precisely, is being called on to craft, oversee, or operationalize such a strategy (other than a generic reference to 'local civil society', which seems a poor match for the task).[35] Lawrence suggests, similarly, that "a key goal for a non-state SSR strategy is to open new channels of communication and dialogue between on-the-ground security providers, citizens, civil society, international actors and the state."[36] While it's easy to support such a prescription in principle, the danger of such an approach is that, absent a coherent linkage between means and ends, it adds up to little more than an SSR version of contact theory: bring the key actors together, and assume that good things will result.

While this may represent an overly-minimalist strategy for effective engagement with the interconnected and shifting components of hybrid security governance, marrying an ongoing commitment to loose, context-specific and flexible forms of rule-based security governance with a renewed commitment on the part of SSR interveners to contribute to what Robert Ricigliano has called 'networks of effective action' may offer a more promising approach.[37] As Ricigliano has suggested, systems thinking emphasizes iterative approaches, learning by doing, and working with (and within) the system to identify and exploit opportunities for positive change, which may in turn lay the foundation for larger changes down the road.[38] While this still requires careful, nuanced understanding and analysis of system dynamics, it does not necessarily require sophisticated central planning and coordination. What it does require, rather, are open communication networks, a shared understanding of larger goals and rules of the road, and a willingness on the part of all members to view individual efforts in the context of larger reform dynamics.[39] Within this larger context, a continued commitment to supporting the evolution of rule-based systems may provide a common reference point around which the actions of interveners can converge.

A broad, long-term commitment to the rule of law and to the development of the state's regulatory capacity also, finally, has the potential to mitigate resistance on the part of state-level actors to external engagement with non-state security providers. As the evolution of the discourse on ownership has demonstrated, governments of fragile and conflict-affected states (represented by the so-called g7+) have grown increasingly sensitive to donor infringements—real or perceived—on their sovereign prerogatives. Accordingly, they have attempted in recent years to use international commitments to respecting 'national ownership' as a means of re-asserting control over post-conflict reform agendas. The sensitivities of governing elites, unsurprisingly, are particularly acute in the security governance realm, both because security provision has long been seen as the exclusive preserve of the state and because of the inherent value of security systems as assets through which to maintain control, establish legitimacy, and/or generate political, social, or economic rents.[40] In contexts where governments see non-state actors as being in competition with them for authority or legitimacy, non-state SSR strategies that are insensitive to such tensions run the risk of alienating the very constituency whose support is an essential prerequisite for enabling SSR in the first place. In the words of Erwin van Veen and Maria Derks, "where justice and security initiatives are perceived by elites as potentially threatening to their interests, they are almost guaranteed to fail."[41]

Somewhat paradoxically, therefore, effective engagement with non-state security providers also requires engagement strategies that both acknowledge and align with the incentive structures faced by governing elites. Beyond appeals to pragmatism—that governing elites should support whatever strategies improve security provision, particularly if they can take at least some credit—embedding non-state SSR strategies within a larger framework of state-centric rule of law development may help offset zero-sum calculations on the part of state and non-state actors alike, and provide state-level elites with some assurances that long-term trends still privilege the state's ability to control and regulate—if not necessarily monopolize—the broader security sector. A self-conscious policy of incrementalism may be perceived as an asset rather than a liability in this context as well, especially given the delicate challenge of ensuring that efforts to bring state-level actors and actions–and not just security providers–within the purview of rule-based frameworks also unfold in ways that are not perceived as an overt threat to elite interests.

Conclusion

The ongoing search for viable second-generation approaches to security sector reform reflects a growing consensus on the prescriptive inadequacies of the monopoly model in the vast majority of reform contexts. In a variation on the theme of 'you can't get there from here', most states undertaking SSR are highly unlikely to be able to monopolize security provision within their territorial boundaries within any realistic timeframe. Yet the alternative notion of hybrid security governance—which recognizes the reality of messy, overlapping, unstable mixes of state and non-state security provision characteristic of a great many fragile and conflict-affected states—appears to suffer from the opposite problem of under-prescription. In other words, while hybridity often accurately describes 'actually-existing security governance', it is decidedly less helpful as a roadmap for charting a coherent course towards the sustainable long-term transformation of security provision in conflict-afflicted states.

With a particular emphasis on the relationship between SSR and rule of law promotion, this paper has made the case that the rule of law, loosely defined, still has a useful role to play as a source of strategic direction for SSR. Crucial to this argument is the conceptual delinking of monopoly and accountability. While first-generation approaches emphasized accountability *within the context* of a state monopoly on the legitimate use of force, the argument here—consistent with insights drawn from the literature on non-state security actors—is two-fold: not only that accountability should matter as much, if not more, in situations of hybrid security governance, but that over the longer term the rule of law may still provide the most stable foundation for ensuring accountability. While emphasizing the gradual expansion of the state's ability to bring security provision within a common (and ultimately enforceable) framework of rules, reformers also need to accept the reality of—and embrace the possibilities for working within—an indefinite interim, understanding that norms underpinning the rule of law evolve slowly and recognizing that relationships between providers and consumers of security will continue for the foreseeable future to be characterized by varied configurations of accountability and legitimacy.

Rethinking SSR along these lines also necessarily involves rethinking how external interveners relate to both the security systems and the security actors within reform contexts. In the first place, as Lisa Denney has noted, dealing with non-state security providers is "uncomfortable territory for organizations committed to human rights and good governance principles."[42] Risk-aversion and a distaste for dealing with actors that might otherwise be considered unsavoury represents, therefore, a crucial first obstacle to be overcome in order to create opportunities both for understanding non-state security providers and for beginning to develop "a spectrum of unique partnerships and associations" between state and non-state systems.[43] Along the same lines, external interveners need to increasingly think of themselves as facilitators rather than engineers, with the goal helping to put in place the necessary processes, relationships and dynamics that will enable complex security systems to evolve along constructive channels long after outsiders have gone home. Indeed, Erwin van Veen and Maria Derks have explicitly called for the donor community to adopt "a process approach to programming," which combines, among other elements, a commitment to short-term results (specifically, supporting existing arrangements that 'work' in a given context), flexible results frameworks supported by sophisticated monitoring and evaluation tools and deeper understandings of the incentive structures facing key actors, and mutual long-term commitments (to be realized over a timespan of decades).[44]

While SSR continues to be, at its core, about the regulation, management and control of coercive power, increasingly the focus of outside intervention needs to shift away from the daunting (and perhaps unachievable) challenge of *re-distributing* power, towards a project of gradually bringing existing power relations within a broad and predictable regulatory framework. The objective, ultimately, should be to connect short-term initiatives—particularly those that facilitate constructive engagement across the different categories of security actors that constitute hybrid security orders—with a longer-term strategy for systemic change based on the evolution of existing arrangements rather than on the imposition of external ones.

Notes

1. Catherine Barnes, "Renegotiating the Political Settlement in War-to-Peace Transitions," paper commissioned by the UK Department for International Development (London, UK: Conciliation Services, 20 March 2009), 3, http://www.c-r.org/sites/default/files/Renegotiating%20the%20Political%20Settlement_200903_ENG.pdf.

2. Bruce Baker, "The Future is Non-State", in *The Future of Security Sector Reform*, ed. Mark Sedra (Waterloo, Ontario: The Centre for International Governance Innovation, 2010), 208–228, https://www.cigionline.org/sites/default/files/the_future_of_security_sector_reform.pdf.

3. Kate Meagher, "The Strength of Weak States? Non-State Security Forces and Hybrid Governance in Africa," *Development and Change* 43, no. 5 (2012): 1073–1101, DOI: https://doi.org/10.1111/j.1467-7660.2012.01794.x

4. Kate Meagher, "The Strength of Weak States?" p. 1076; Timothy Raeymaekers, Ken Menkhaus and Koen Vlassenroot, "State and Non-State Regulation in African Protracted Crises: Governance without Government?," *Afrika Focus* 21, no. 2 (2008): 10.

5. Amitai Etzioni, "Bottom-up Nation-building," *Policy Review* 158 (2009-2010): 54.

6. Louise Andersen, "Security Sector Reform and the Dilemmas of Liberal Peacebuilding" (working Paper 31, Danish Institute for International Studies (DIIS), 2011), 12, http://www.diis.dk/files/media/publications/import/extra/security_sector_reform_and_the_dilemmas_of_liberal_peacebuilding_1.pdf.

7. Lisa Denney, *Non-state Security and Justice in Fragile States: Lessons from Sierra Leone*, Briefing Paper No. 73, (London, UK: Overseas Development Institute, April 2012), https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7640.pdf; Peter Albrecht and Helene Maria Kyed, "Introduction: Non-state and Customary Actors in Development Programs" in *Perspectives on Involving Non-state and Customary Actors in Justice and Security Reform*, Peter Albrecht, et al. (Rome: IDLO/DIIS, 2011), 3–22.

8. Ken Menkhaus, "Non-State Security Providers and Political Formation in Somalia", *CSG Papers* No. 5. (Waterloo: Centre for Security Governance, April 2016), 6, http://secgovcentre.org/wp-content/uploads/2016/11/NSSPs_in_Somalia_April2016.pdf.

9. Thomas Carothers, "The Rule of Law Revival," *Foreign Affairs* 77, no. 2 (1998): 95-106, doi:10.2307/20048791.

10. Agnès Hurwitz, "Civil War and the Rule of Law: Toward Security, Development, and Human Rights" in *Civil War and the Rule of Law: Security, Development, Human Rights*, Angès Hurwitz and Reyko Huang, eds. (Boulder, CO: Lynne Rienner, 2008), 2.

11. Jane Stromseth, David Wippman and Rosa Brooks, *Can Might Make Rights? Building the Rule of Law after Military Interventions*, (New York: Cambridge University Press, 2006): 75, DOI: https://doi.org/10.1017/CBO9780511803086.

12. Louis-Alexandre Berg, "Guns, Laws and Politics: The Political Foundations of Rule of Law and Security Sector Reform," *Hague Journal on the Rule of Law* 4, no. 4 (2012): 4–30, DOI: https://doi.org/10.1017/S1876404512000024.

13. Marina Ottaway, "Promoting Democracy after Conflict: The Difficult Choices," *International Studies Perspectives* 4, no. 3 (2003): 314–322, DOI: https://doi.org/10.1111/1528-3577.403007.

14. Carothers,"The Rule of Law Revival," 96.

15. Ibid.

16. Vera Gowlland-Debbas and Vassillis Pergantis, "Rule of Law" in *Post-Conflict Peacebuilding: A Lexicon*, Vincent Chetail, ed., (New York: Oxford University Press, 2009): 321.

17. Denney, *Non-state Security and Justice in Fragile States*, 1.

18. Carothers,"The Rule of Law Revival," 96.

19. Stromseth, Wippman and Brooks, *Can Might Make Rights?*, 77.

20. Menkhaus, "Non-State Security Providers and Political Formation in Somalia."

21. Denney, *Non-state Security and Justice in Fragile States*, 1.

22. Organization for Economic Co-operation Development (OECD), *Supporting Statebuilding in Situations of Conflict and Fragility: Policy Guidance*, (Paris, France: OECD, 2011), http://dx.doi.org/10.1787/9789264074989-en.

23. Bruce Baker, "Policing for Conflict Zones: What Have Local Policing Groups Taught Us?" (paper presented at "Non-State Security Providers and Political Formation in Conflict-Affected States," Waterloo, Canada, Centre for Security Governance (CSG), May 2016).

24. Michael Lawrence, "Towards a Non-State Security Sector Reform Strategy," *SSR Issue Papers* No. 8 (Waterloo: Centre for International Governance Innovation, 2012), 15, http://www.cigionline.org/publications/2012/5/towards-non-state-security-sector-reform-strategy.

25. Bruce Baker and Eric Scheye, "Multi-Layered Justice and Security Delivery in Post-Conflict and Fragile States," *Conflict, Security and Development* 7, no. 4 (2007): 517, DOI: https://doi.org/10.1080/14678800701692944.

26. Meagher, "The Strength of Weak States?,"1080–1181.

27. Lawrence, "Towards a Non-State Security Sector Reform Strategy," 18.

28. Baker and Scheye, "Multi-Layered Justice and Security Delivery," 519.

29. Meagher, "The Strength of Weak States?,"1074.

30. Baker and Scheye, "Multi-Layered Justice and Security Delivery," 519.

31. Lawrence, "Towards a Non-State Security Sector Reform Strategy," 10.

32. Menkhaus, "Non-State Security Providers and Political Formation in Somalia," 38-39.

33. Ibid., 38.

34. Monika Heupel, "Rule of Law Promotion and Security Sector Reform: Common Principles, Common Challenges," *Hague Journal on the Rule of Law* 4, (2012): 168, DOI: https://doi.org/10.1017/S1876404512000097

35. Lawrence, "Towards a Non-State Security Sector Reform Strategy," 17.

36. Ibid., 22.

37. Robert Ricigliano, "Networks of Effective Action: Implementing an Integrated Approach to Peacebuilding," *Security Dialogue* 34, no. 4 (2003): 445–462, DOI: https://doi.org/10.1177/0967010603344005.

38. Timothy Donais, *Towards Vertically Integrated Peace Building: Bridging Top-down and Bottom-up Approaches*, CIGI Workshop Report (Waterloo, ON: Centre for International Governance Innovation, 2013), http://www.cigionline.org/sites/default/files/donais_vertical_integration_workshop_report.pdf.

39. Ricigliano, "Networks of Effective Action,"446.

40. Erwin van Veen and Maria Derks, "The Deaf, the Blind and the Politician: The Troubles of Justice and Security Interventions in Fragile States," *Hague Journal on the Rule of Law* 4, (2012): 85, DOI: https://doi.org/10.1017/S187640451200005X.

41. Ibid.

42. Denney, *Non-state Security and Justice in Fragile States*, 1.

43. Baker and Scheye, "Multi-Layered Justice and Security Delivery," 525.

44. van Veen and Derks, "The Deaf, the Blind and the Politician," 93.

China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities

Emilio Iasiello*

China has been allegedly engaged in a longstanding cyber espionage campaign against the United States, as well as other nations, soliciting negative reactions citing China's malfeasance. The negative press received from these activities is feeding into the perception that China's global 'rise' is predicated on surreptitious intellectual property theft to project it into great power status, and perhaps as a way to seek regional and global military balance with the United States. In order to combat this perception, this article suggests that China has leveraged its 'Three Warfares,' a three-prong information warfare approach composed of Media, Legal, and Psychological components designed to influence the international community, and the United States in particular, in order to forestall the development and implementation of any effective counter strategy. The result has been largely successful to date, enabling China to reach specific milestones set forth in its national development plans while escaping any serious punitive or economic repercussions from the international community, to include recent circumvention of U.S.-imposed cyber sanctions. This article will review Chinese cyber activity, international perceptions of the Chinese cyber threat, how "Three Warfares" apply to Chinese cyber operations, and then provide final conclusions.

*Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting U.S. government civilian and military intelligence organizations, as well as the private sector. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in peer-reviewed journals.

Emilio Iasiello, "China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities," *Journal of Strategic Security* 9, no. 2 (2016): 45-69. DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1489. Available at: http://scholarcommons.usf.edu/jss/vol9/iss2/4

Chinese Cyber Activity

Former National Security Agency (NSA) Director and Commander of U.S. Cyber Command General Keith Alexander estimates the losses incurred by cyber espionage activities at approximately $338 billion, although admittedly not all the result of Chinese efforts.[1] Nevertheless, the intimation of this assessment is that China, identified as the most persistent cyber espionage actor, is suspected of a good portion of this activity.[2] Indeed, the breadth and scope of suspected Chinese sponsored and/or directed cyber espionage begs the question: Despite the tactical success of stealing a diverse spectrum of sensitive and proprietary information in the face of public protest, what is Beijing's strategic game plan?

China has three primary national security objectives: Sustaining regime survival, defending national sovereignty and territorial integrity, and establishing China as both a regional and national power.[3] China views the United States with a cautious mix of skepticism, partnership, and competition. The Chinese believe that the United States is a revisionist power seeking to curtail China's political influence and harm China's interests.[4] One way to counter U.S. supremacy is for China to engage in cyber operations in an effort to extract information from "diplomatic, economic and defense industrial base sectors that support U.S. national defense programs."[5] In this context, cyber operations can be viewed as being more about trying to strengthen China's core and less about diminishing U.S. power. Focusing solely on the United States, suspected Chinese cyber espionage actors have targeted the following industries, among others, during the past two years: Space[6], Infrastructure[7], Energy[8], Nuclear Power[9], Technology Firms[10], Clean Energy[11], Biotechnology[12], and Healthcare.[13]

China's 12th Five Year Plan reflects overall goals and objectives of the government to promote economic industry growth. It is a critically important tool that maps out in five-year cycles the country's future progress via guidelines, policy frameworks, and targets for policy makers at all levels of government.[14] In the current Five Year Plan, which covers 2011-15, China identified seven priority industries to develop, areas in which the United States has typically been an innovator and leader. These "strategic emerging industries" are intended to become the backbone of China's economy in the decades ahead.[15] These industries are:

- New Energy (nuclear, wind, solar sower)
- Energy Conservation and Environmental Protection (energy reduction targets)
- Biotechnology (drugs and medical devices)
- New Materials (rare earths and high-end semiconductors)

- New IT (broadband networks, Internet security infrastructure, network convergence)
- High-End Equipment Manufacturing (aerospace and telecom equipment)
- Clean Energy Vehicles[16]

It is easy to see that a correlation can be made between the types of industries that have been targeted in the United States in the last two years and the strategic emerging industries that China has highlighted for development. Moreover, China views cyber as an ideal tool to accomplish these objectives being an inexpensive facile technique to engage several potential intelligence targets at once. In February 2007, *China National Defense News* defined cyber warfare as the "use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology."[17] The key takeaway here is that cyber warfare is directly related to "information advantage" and not military advantage, suggesting that peacetime cyber activities are more about bolstering China's development in strategic areas and less about establishing military superiority vis-a-vis reconnoitering a future battle space.

The Perceived Chinese Cyber Threat

While some experts believe that the United States, along with China and Russia, are engaged in a cyber arms race,[18] China has yet to be suspected or implicated in an incident involving the destruction of information systems or the information resident on them. Many Chinese strategic military writings advocate the use of information warfare as a pre-emptive weapon prior to the onset of military engagements;[19] however, if China is behind the volume of cyber espionage activity attributed to it, during peacetime China prefers to leverage the benefit of computer intrusions as a means of information collection and commercial advantage, rather than one of deterrence.

Currently, several countries including Australia, Canada, Germany, India, Taiwan, and the United Kingdom, among others, have publicly accused China of intruding into their public and private sector networks.[20] In particular, the United States has been the prime target of suspected Chinese orchestrated or directed cyber operations for approximately a dozen years. While the U.S. government maintained a reserved stance for most of this time, in 2012 it became more outspoken with regard to the volume of cyber espionage activity targeting its public and private sectors. In October 2011, U.S. Congressman Mike Rogers of the House Permanent Select Committee on Intelligence publicly accused China of stealing sensitive information:

> China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.[21]

In 2013, the security company Mandiant published a detailed report identifying a Chinese military unit involved in cyber espionage.[22] Never before had technical evidence and analysis linking activities to a government entity been made public. The Mandiant report proved to be a watershed moment for senior U.S. government officials with several of them, including President Obama, publicly addressing the issue of Chinese cyber espionage. Shortly after publication of the Mandiant report, in March 2013, U.S National Security Advisor Thomas Donilon stated:

> …businesses are speaking out about their serious concerns about sophisticated targeted theft of confidential business information and proprietary information through cyber intrusions emanating from China.[23]

In that same month, President Obama engaged directly with Chinese President Xi Jinping about cyber security and future engagement possibilities,[24] which was followed by a summit in June, where the two leaders more fully discussed cyber security, with Obama opting not to directly accuse the Chinese leader of espionage activity.[25] However, any headway was derailed in May 2014 when the U.S. Department of Justice indicted five Chinese military officers with committing cyber espionage, the first time ever the U.S. government publicly accused members of a foreign government with crimes against U.S. companies.[26] Further reports of another suspected Chinese espionage group like 'Axiom', reputed to be more sophisticated than the one profiled in the Mandiant report, further paints a condemning picture of China as a relentless cyber thief of sensitive information.[27] Given the voluminous cyber incidents pointing toward some level of Chinese government affiliation, Beijing finds itself trying to sustain its 'peaceful rise' image in the midst of growing global public dissent, led at the spear tip by the United States and its threat of imposing cyber sanctions against those entities that benefited from commercial espionage activities.

Three Warfares – A Primer

It seems counterproductive for a country so concerned with 'face' to engage in such blatant and aggressive activities that threaten to harm its global image. Two important concepts in Chinese culture are *guanxi* and *mianzi*. The first, *guanxi*, has been defined as sharing favors between individuals, connections, relationships, and the ability to exert influence. The second, *mianzi*, means 'face,' as in saving face, losing face, and giving face.[28] So why would a country steeped in this mindset willingly risk its image, especially at a time when the country is seen as a peacefully rising world economic power? The implementation of non-kinetic, non-violent, but still offensive operations is best suited for Chinese peacetime strategy of influencing the cognitive processes of a country's leadership and population, or what Sun Tzu describes as "subduing the enemy without fighting."[29] In 2003, the Communist Chinese Party Central Committee and the Central Military Commission approved the concept of 'Three Warfares,' a People's Liberation Army non-military information warfare tool to be used in the run up to and during hostilities.[30] Collectively, the 'Three Warfares' allow China to enter any fray, whether in peace or war, with a political advantage that can be used to alter public or international opinion.[31] They are:

- *Psychological Warfare*—Undermines an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing the enemy military personnel and supporting civilian populations.[32]
- *Public Opinion/Media Warfare*—Influences domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests.[33]
- *Legal Warfare*—Uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended to build international support and manage possible political repercussions of China's military actions.[34]

Media warfare incorporates the mechanism for messages to be delivered, while legal warfare provides the justification of why actions are permissible. Psychological warfare provides the necessary nuance leveraging the dissemination capability of the media and the more formalized legal mechanisms to substantiate its activities to domestic and international audiences. Given that each of these types of warfare rely on the targeting and influencing of a specific target audience, it is easy to see why Chinese analyses almost always link these three types of 'combat' together.[35]

Public Opinion/Media Warfare

Public opinion warfare refers to the use of various information channels, including the Internet, television, radio, newspapers, movies, and other forms of media in accordance with an overall plan and defined objectives to transmit selected news and other materials to an intended audience.[36] The goals are to preserve friendly morale, generate public support at home and abroad, weaken the enemy's will to fight, and alter the enemy's situational assessment. Defensive public opinion warfare is leveraged against adversarial public opinion warfare to neutralize possible effects on the Chinese populace.[37] Given the voluminous hacking allegations levied against China, defensive public opinion warfare is a natural counterbalance. According to Cheng, four themes are inherent in Chinese writings on public opinion:[38]

- *Follow Top-Down Guidance*—The senior leadership will dictate courses of action based on strategic objectives.
- *Emphasize Preemption*—Chinese analyses of public opinion warfare emphasize that "the first to sound grabs people, the first to enter establishes dominance (*xian sheng duoren, xianru weizhu*)."
- *Be Flexible and Responsive to Changing Conditions*—Use of different propaganda activities depending on the audience. "One must make distinctions between the more stubborn elements and the general populace."
- *Exploit All Available Resources*—Civilian and commercial news assets such as news organizations, broadcasting facilities, Internet users, etc., are seen as an invaluable resource in getting China's message before domestic and global audiences.

Public criticism over Beijing-sponsored intrusions surfaced as early as 2005 when it was revealed that suspected Chinese government intrusions dubbed 'Titan Rain' had been targeting U.S. public and private sectors entities since 2003.[39] Since that time, numerous foreign governments have gradually come out publicly to identify the Chinese government, or its operatives, as perpetrators of intrusion activity against their networks.[40] Furthermore, U.S. government entities have long suspected Chinese telecommunications companies Huawei and ZTE as being instruments of the state, and possible mediums that can be leveraged by the Chinese government for intelligence collection.[41] Such debate has risen to the highest levels as seen in 2013 meetings between Chinese president Xi Jinping and U.S. President Barack Obama.[42] In 2014, Secretary of Defense Charles Hagel disclosed U.S. cyber force structure and capabilities to China in an effort to demonstrate military transparency.[43]

Chinese Public Opinion / Media Warfare Applications to Cyberspace

Chinese response has evolved during this period in which it has been framed as an antagonistic cyber presence. Typically, China has met such accusations with a defensive posture, denying allegations and asking for more information in an attempt to help track down the perpetrators. Indeed, senior official statements issued from China's Ministry of Defense,[44] Ministry of Foreign Affairs,[45] and its Prime Minister[46] have towed the same party line, asserting that China is not behind the attacks, that China is a victim not a perpetrator of cyber-crime activity, and that China's laws strictly identify hacking as illegal.[47]

However, China shifted to a more assertive stance once former NSA contractor Edward Snowden released alleged highly classified documents exposing U.S. global surveillance efforts. Instead of trying to deflect accusations, China now points its own finger at the U.S. government. In particular, Beijing has demanded an explanation from the United States over reports of NSA spying on the Chinese company Huawei.[48] The irony is not lost on China, given earlier U.S. government concerns over Huawei's suspected spying on behalf of the Chinese government, which was ultimately not proven after a study was conducted on behalf of the U.S. Congressman and Chairman of the House Permanent Select Committee on Intelligence, Mike Rogers.[49] Although skeptics persisted, in October 2012, the White House conducted its own security review of Huawei and found no clear evidence that Huawei spied on behalf of the Chinese government.[50] Further pushing U.S. cyber malfeasance into the spotlight, in March 2014, China's National Computer Emergency Response Team identified the United States as the top source of intrusion activity against its computers.[51]

U.S. efforts to manage its public image have fallen short after allies and adversaries alike expressed outrage from the Snowden scandal.[52] The subtle nuance from which the U.S. government bases its defense, namely that it conducts such activities to support national security interests and not to provide competitive advantage to U.S. corporations, seems trite, particularly after being caught with its hand in the proverbial cyber cookie jar. Several accusations have surfaced because of leaked documents pointing to the NSA spying on non-national security entities such as Brazil's biggest oil company,[53] the European Union commissioner investigating Google, Microsoft, and Intel,[54] and the International Monetary Fund and World Bank.[55] Even on its home front, the U.S. public and special interest groups seeking to preserve civil liberties have condemned NSA activities.[56]

While the U.S. seemed to have an upper hand and international support regarding suspected Chinese cyber espionage, China has successfully regained some of its public facing pride. China continues to promote itself as a cyber victim as well as a willing cyber security partner. In 2014, China expressed its desire for mutual cyber cooperation with the United States,[57] and as of April 2014, the Pentagon has engaged in military exchanges with China in the spirit of military transparency.[58]

Despite ongoing allegations of Chinese cyber misconduct, China has made strides in somewhat polishing its tarnished image at the timely expense of U.S.

secret cyber activities. Perhaps in light of this, in May 2014, the U.S. Justice Department indicted five Chinese military hackers for cyber espionage.[59] While this landmark decision attempted to directly implicate China's government with cyber espionage, it failed to incriminate China any more in the public's eye. After all, many public and private organizations generally believe that the Chinese government steals intellectual properties and sensitive information. Rather, the onslaught of exposed highly sensitive documents revealing the U.S. government's role in similar activity (against allied and adversary governments alike) proved to be a bigger injustice and a black mark against a government advocating human rights and individual freedoms.

Legal warfare

Legal warfare is one of the key instruments of psychological and public opinion warfare.[60] Legal warfare is typically used in conjunction with one or both of the other two types of warfare as maximum effectiveness is achieved when they build upon each other. In this way, legal warfare provides the basis that strengthens public opinion warfare and psychological warfare.[61] By definition, legal warfare is designed to provide justification for a course of action. There are two influences that help form Chinese legal warfare:

- *Chinese Views of the Role and Rule of Law*—Historical and cultural considerations inform the Chinese government's understanding of legal warfare. Confucianism and Legalist influences were integral to imperialist China but as the government evolved during Mao's tenure, Marxist perspectives advocated that the "law should serve as an ideological instrument of politics."[62] Today, there is a focus on commercial and contract law, while criminal law remains weak.[63]
- *Chinese Perception of Legal Warfare in the West*—China perceives that importance of Western interests to use law as justification for its actions. In the first Gulf War, the United States obtained U.N. authorization for sanctions as well as use of force in Iraq, while in Kosovo, it argued that its actions were "consistent with the law" because they were taken under NATO auspices.[64] Being able to use rule of law or its legal perceptions to justify actions is a powerful tool in Chinese thinking.

Chinese legal warfare applications to cyberspace

As a mode of influence, legal warfare is typically used prior to the outbreak of physical conflict, and occurs only in context of actual warfare. However, since the international spotlight has shifted to cyber espionage activities and China has been called out as a perpetrator of intellectual property theft, evidence suggests that the Chinese may be using tenets of legal warfare to push strategic interests. The following events occurred after several governments publicly blamed China for hacking into their networks and stealing data:

- *2014 U.S. Plans to Relinquish Internet Control*—In December 2012, China along with Russia gained international support to have all states have equal rights to the governance of the Internet. The agreement updated 24-year-old U.N. telecommunications rules.[65] While nonbinding, eighty-nine countries signed it with 55 reserving the right to sign it at a later date,[66] showing the widespread support. This initiative continued the necessary steps for the International Telecommunications Union (ITU) to play an active role in the multistakeholder model of the Internet.[67] Such efforts, coupled with the leaking of sensitive documents pertaining to the National Security Agency's alleged global surveillance, applied considerable pressure on the United States to back away from supporting the Internet Corporation for Assigned Names and Numbers' (ICANN) influence on Internet controls.[68] Gaining international support and using the ITU as an authorized body gave these efforts the auspice of legitimacy. As of January 2016, U.S. officials remained committed to relinquishing federal government control over the administration of the Internet by September.[69]
- *2011/2015 China-Russia Letters to the United Nations*—Since there are no official international laws or even common definitions governing cyber activity, China has been a prominent voice in advocating for norms of behavior for nation states. In 2011, China teamed up with Russia, Tajikistan, and Uzbekistan to submit an international code of conduct for information security to the U.N.,[70] and updated it in January 2015.[71] Essentially, the core of both proposals highlighted identifying the rights and responsibilities of states in the information space, as well as promoting their constructive and responsible behaviors to enhance their cooperation in addressing common threats and challenges. Although as of this writing, the proposal is still being reviewed by member states, China did assume a leading international role in trying to establish behavior norms for nation states using an international body as a validating entity of its efforts.
- *2009 Updating of Chinese Cybercrime Legislation*—China has maintained publicly that hacking is against Chinese laws.[72] In 2009, China extended penalties for those convicted of cybercriminal activities.[73] When accused of

> sponsoring hacking, China is quick to cite its laws as a legal justification of why it does not engage in that activity.[74]

China uses international organizations like the UN, whose authorization is backed by legal considerations, in order to give its efforts legitimacy. This ultimately serves two important strategic objectives: 1) It tempers the negative image of China as a hacking state by showing that it is seeking to work collectively and within the defined rules of established international organizations, and 2) It helps China implement non-kinetic asymmetric means to pursue its political and economic objectives, avoiding the need to use military force or influence, thereby reducing the risk of potential escalation over a given issue.

Chinese psychological warfare

Psychological Warfare is deeply rooted in Chinese strategy; for example, "Chinese writings posit that during peacetime, psychological operations seek to reveal and exploit divisions in the enemy's domestic political establishment or alliance system and cast doubt on the enemy's value concepts."[75] It aims for a high degree of precision in targeting critical nodes in order to achieve nonlinear effects.

Chinese psychological warfare applications to cyberspace

According to Chinese scholars, psychological warfare is an integral part of information warfare.[76] However, defining information warfare in a Chinese context is more challenging, as there is not a published doctrine on information warfare and there are only Chinese doctrinal writings available to provide insight into this complex discipline. Early writings on the subject were largely borrowed from translated United States, Russian, French, and German doctrines.[77] As time has passed, there have been developments in Chinese thinking with regard to information warfare, most notably with regard to the concept of 'information dominance,' which according to Chinese cyber expert Dr. James Mulvenon, is the main objective of Chinese information warfare strategy.[78] Information dominance has two primary targets: The physical information infrastructure and the data that has passed through it, and perhaps more importantly, the human agents that interact with those data, especially those making decisions.[79]

According to Chinese writings, there are five broad tasks associated with psychological warfare.[80] Taking into consideration China's involvement in global intrusion activity, these tasks may be applied to the current environment in the following manner:

1. *Presenting Your Own Side as Just*—China is very much concerned with its public image, which makes its ambivalence toward the negative publicity surrounding suspected hacking activity curious. All attempts to 'blame and shame' China have ended in a resounding failure, which can be attributed to the fact that China has established and maintained the same official position, regardless of what government is finger pointing. Beijing typically parries such claims by consistently denying hacking allegations and then immediately pointing out that they are the victims of hacking.[81] Further, as noted earlier, Beijing frequently cites that hacking is against the law in China, trying to show that, as a country, it is doing its part to best address hostile activities in cyberspace through legal channels.[82] Lastly, China in partnership with Russia, Tajikistan, and Uzbekistan, proposed before the United Nations (UN) a code of conduct in cyberspace for nation states,[83] and updated it in February 2015 after it had received input from member states.[84] This achieved two important objectives:
    i) It showed China being proactive in trying to establish an international set of responsible behavior norms for nation states in cyberspace; and
    ii) It demonstrated China's willingness to collaborate with others as equals. The proposal tendered at the UN further demonstrated China's desire to gain consensus among the international community. Taken collectively, these efforts can be interpreted as China's mitigation of the negative press it receives by presenting itself as responsible and collaborative. The proactive desire to collaborate with other governments on such issues may have been the impetus to lead the United States in June 2015 to agree to negotiate with China on some kind of "code of conduct" in cyberspace.[85]

2. *Emphasizing One's Advantages*—In 2014, China became the world's largest economy. China's gross domestic product blistered from 2003–2013, averaging more than ten percent a year.[86] While the United States has kept Chinese companies at bay from penetrating U.S. markets, China has enthusiastically pursued other markets where the U.S. has typically enjoyed a trade advantage. Recently, China overtook the United States as Africa's and Brazil's largest trade partner.[87] This has translated into economic advantages regardless of negative press about alleged Chinese hacking. These countries simply do not care about the threat, seeing economic engagement and accelerated infrastructure development as outweighing any potential consequence. Brazil is welcoming more Chinese private customers as active

players in more diversified ways of bilateral economic cooperation,[88] and in Africa, China has been the leading supplier of telecommunications equipment.[89] The stigma placed on the Chinese telecommunications company Huawei is a perfect example of China playing to its strengths. Despite the suspicions leveled largely by the U.S. government that Huawei may act as an agent of the Chinese government, the House-driven study didn't yield any conclusive proof of espionage. Furthermore, the company is "the second largest telecommunications provider in the world, with deployed products and solutions in over 140 countries, indicating that several countries in the world are not as concerned with Huawei posing an intelligence threat." [90] Even U.S. allies Australia and the UK appear not to levy the same level of concerns as the United States. The UK's Huawei Advisory Board—an entity composed of both members of the UK's intelligence service GCHQ staff, governmental employees, and members of industry, as well as Huawei personnel—concluded after an audit that Huawei's work in the UK did not pose a national security threat.[91] In 2013, Huawei supported the creation of an Australian Cyber Security Center development to test the security credentials being implemented into critical infrastructure.[92]

3. *Undermining the Opposition's Will to Resist*—There have been several writings on the China cyber threat by civilian and government regional, cultural, and functional experts, in addition to international media and print news channels covering the topic. In each instance, two resounding messages are conveyed: i) The Chinese cyber threat is massive and pervasive representing the largest transfer of wealth in human history,[93] and ii) China seeks access to computer networks not only to steal sensitive information but also to establish "information dominance."[94] Whether described as being sophisticated, rudimentary, or somewhere in between, Chinese espionage activity has been constant and persistent. Even the term "advanced persistent threat," given to it purportedly by the U.S. Air Force in 2006 to be able to discuss it with unclassified personnel,[95] portrays the adversary as skilled and relentless, and considering its lack of covertness, fearless as well. The fact that there have been few consequences suffered by the alleged Chinese cyber operatives for their actions lends further support to the notion that they cannot be beat, or at the very least, their brazen activity cannot be stopped. As Richard Clarke said, "Every major company in the United States has already been penetrated by China."[96] Coming from a man considered the first cyber czar in the U.S. government, such platitudes further paint the adversary as a nearly unbeatable opponent.

4. *Encouraging Dissension in the Enemy's Camp*—This task focuses on disrupting the cognitive processes of policymakers and decision makers, inhibiting their ability to develop a plan of action. The theory suggests that the best strategy is to attack the enemy's mind, leaving him unable to plan,[97] which given U.S. policymakers' history of not being in accordance on cyber issues, makes them a prime exploitable target. One thing is clear: Since suspected Chinese cyber espionage was first discovered in 2003,[98] there has been no concrete course of action as to how to handle Chinese cyber espionage until the United States' creation of cyber sanctions, an effort to deter all grave cyber activities, but in particular, those believed to be conducted or endorsed by China.[99] Previously, agencies supported various courses of action. There were proponents of "active cyber defense" such as U.S. Cyber Command[100] and the Defense Advanced Research Projects Agency[101] as a means to deter adversaries in cyberspace. However, there were some like U.S. Representative Mike Rogers who believed there needed to be a viable strong defense in place before engaging in any offensive cyber operations.[102] Still others, such as the Government Accountability Office (GAO) cited lack of clearly defined roles and responsibilities of federal agencies as a serious impediment to productive cyber security.[103] Continued failure to establish a strong national level cyber security strategy prohibits the U.S. government from going down a unified path with all stakeholders understanding their part in the process. Even a February 2013 Executive Order on Improving Critical Infrastructure Cyber Security has not generated significant support. While a positive step, it failed to clearly mandate changes, relying on companies' willingness to comply with the measures stated in the order. Although it did not reference the February Order, the GAO in a March report still cited the need of an integrated national cyber security strategy complete with milestones, performance measures, and Congressional oversight.[104] Whether intentionally or not, Chinese cyber espionage campaigns have taken advantage of the indecisive climate that had permeated in the U.S. government prior to the 2015 agreement between the two governments not to hack each other for commercial economic advantage.

5. *Implementing Psychological Defenses*—In the Chinese view, it is assumed that an opponent will mount psychological attacks, as well as expose them and defeat them in order to demoralize an opponent by demonstrating the ineffectiveness of his efforts.[105] China has maintained its political stance that it does not conduct hacking. Even after approaching Chinese President Xi Jinping directly about Chinese espionage, Xi deflected blame onto

poor network security, and not the government hacking U.S. targets. Indeed, when the NSA's secret surveillance program was exposed, China immediately jumped on the opportunity to make the U.S. government the bad guy.[106] Even the much-maligned Chinese telecommunications giant Huawei seized the moment to condemn NSA spying and promote a global cyber security dialogue.[107]

When these five psychological warfare tasks are taken collectively, the message being promoted is that China is a dominant cyber force. By denying the accusations, China further builds on this image without having to say it publicly, or leak into the press its involvement in a significant cyber event. After all, unlike the U.S., China has not found the desire or need to bolster its image as a dominant player in cyberspace via public announcements or national strategies; instead, Beijing has relied upon others to speculate on its capabilities and strength, allowing it to concentrate its energies on trying to temper negative press while concurrently maintaining its covert espionage efforts to support its national objectives.

Dodging U.S. Cyber Sanctions

While the Chinese cyber espionage activity has enjoyed relative freedom for a substantial amount of time, the 2015 state visit put China on notice that cyber espionage for commercial advantage would not be tolerated by the United States. In an effort to avoid these penalties, Beijing reached accord days before President Xi's official state visit to the United States in which both agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[108] As a result of the agreement, China arrested hackers identified by the United States,[109] thereby demonstrating its commitment to arresting criminal elements in cyberspace, even if they are China's own citizens. While opinions differ on Beijing's motives for arresting Chinese hackers, it is not without precedent. In 2010, after a lengthy international coordinated effort, Chinese authorities detained a Chinese national for hacking seven National Aeronautics and Space Administration (NASA) systems, according to a testimony from a NASA official to Congress.[110]

While Washington waits to see if Beijing will prosecute these hackers, the more important takeaway is China's demonstration of its willingness to work with the United States—and perhaps by extension other governments as well—on similar cyber issues, something that had not been done previously. Sanctions still loom large on the table if perceived Beijing-sponsored hacking against commercial interests does not abate; however, if handled correctly, the threat of sanctions may ultimately serve China's interests by addressing head-on the biggest black mark against China. Holding fast to the principles of legal and media warfare, China's assurance of "opposing cyber attacks and espionage and combating all forms of hacking activities in accordance with the law,"[111] coupled with public examples of collaborating with stakeholders toward this end, may gradually assuage opponents' concern of the "China threat," and in turn, depict China as a willing partner instead of an antagonist.

Additionally, initiating additional cyber security cooperation with regional governments will further bolster China's message of seeking a stable Internet, safe from criminal and terrorist activities. China has been active in this regard, engaging in cyber security discussions with Japan,[112] Malaysia,[113] and South Korea,[114] as well as a series of no-hack pacts leading to the November 2015 G20 agreement not to conduct cyber-enabled commercial espionage.[115] It can be expected that China will pursue more of these through independent bilateral meetings or through international organizations like the Shanghai Cooperation Organization.

Conclusion

Despite being accused of perpetrating long running and substantial cyber espionage campaigns against the United States as well as several other countries, China has escaped any significant punitive or economic repercussions. China's "Three Warfares," a three-pronged information warfare strategy designed to influence the international community, has played an important role in forestalling any significant deterrence response, while allowing China to promote itself as a viable partner in cyberspace. China has sought to dull public perception of its rising threat by denying accusations, while capitalizing on the Snowden leaks of U.S. global surveillance activities to tarnish the U.S. image. Concurrently, China has used legal mechanisms to help promote itself as a viable cybersecurity partner. The act of championing the right of every state to be included on Internet governance gained enough traction to encourage the U.S. to step down from its governing role. Providing the UN with an updated "code of conduct" for nation state behavior in cyberspace demonstrated its interest to the global community that it was leading efforts toward achieving stability in cyber space. Updating its cybercrime legislation exhibited Beijing's commitment toward penalizing those engaged in hacking, quickly followed by arresting suspected hackers at the U.S. behest in 2015.[116] Finally, China's use of psychological operations (PSYOPS) has presented itself as a law abiding stakeholder in cyberspace while quietly basking in the writings that have identified it as a significant cyber power. The more experts warn of China's powerful cyber capabilities, the more of a cyber equal China is perceived to be without Beijing ever having to intimate it.

As a result, the confluence of these three strategies has kept the West from deterring suspected Chinese espionage for a substantial period of time. In fact, the more time that has been allowed to elapse, the more China has been able to take advantage of it. In the time that the U.S. has mulled over finally levying cyber sanctions against China, Beijing has capitalized on meeting with countries like Japan and South Korea on cyber security issues,[117] as well as engaging in a series of "no hack pacts" between China and Russia,[118] the United Kingdom,[119] and the United States,[120] an effort culminating in the historic November 2015 agreement by members of the G20 not to engage in cyber-enabled espionage for commercial advantage.[121]

Moreover, China has done this while becoming the world's largest economy in the process, and while promoting itself as a regional leader by spearheading efforts for a Maritime Silk Road (a system of linked ports, projects and special economic zones in Southeast Asia and the northern Indian Ocean[122]) and the Asian Infrastructure Investment Bank (which already has 20 governments on board).[123] China's plan may just be to rise through its region first before ascending to a global throne brought on by some of the fruits of its espionage efforts. In this context, China's cyber espionage can be viewed as less about reducing U.S. capability, and more about building itself to assume a larger status in the world.

Notes

[1] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'," *Foreign Policy: The Cable*, 9 July 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatesttransfer-of-wealth-in-history/.

[2] Office of the Director of National Intelligence, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,* (Washington DC: Office of the National Counterintelligence Executive, October 2011), http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

[3] Colonel Jayson M. Spade, *Information as Power: China's Cyber Power and America's National Security*, (Carlisle, PA: U.S. Army War College, May 2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf; Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2014*, (Washington, DC: Annual Report to Congress, 2014), http://www.defense.gov/pubs/2014_DoD_China_Report.pdf; Department of Defense, *Quadrennial Defense Review 2014* (Washington, D.C.: OSD, 2014): V, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

[4] Andrew J. Nathan and Andrew Scobell, "How China Sees America," *Foreign Affairs,* (September/October 2012), http://www.foreignaffairs.com/articles/138009/andrew-j-nathan-and-andrewscobell/how-china-sees-america.

[5] Office of the Secretary of Defense, *Military and Security Developments*.

[6] John Walcott, "Chinese Espionage Campaign Targets U.S. Space Technology," *Bloomberg*, 18 April 2012, http://www.bloomberg.com/news/2012-04-18/chinese-espionage-campaign-targets-u-s-space-technology.html.

7. Tom Simmonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *Technology Review*, 2 August 2013, http://www.technologyreview.com/news/517786/chinese-hacking-team-caughttaking-over-decoy-water-plant/.

8. Ibid.

9. Jennifer Liberto, "New Chinese Hacker Group Targets Governments, Nuclear Facilities," *CNN Money*, 4 June 2013, http://money.cnn.com/2013/06/04/technology/security/cyber-hackergroup/index.html.

10. Stew Magnuson, "Stopping the Chinese Hacking Onslaught," *NDIA*, July 2012, http://www.nationaldefensemagazine.org/archive/2012/July/Pages/StoppingtheChineseHackingOnslaught.aspx.

11. Susan D. Hall, "Chinese Hackers Targeting the Healthcare Industry," *FierceHealthIT*, 20 March 2013, http://www.fiercehealthit.com/story/chinese-hackerstargeting-healthcare-industry/2013-03-20.

12. Nick Paul Taylor, "Chinese Trial Data Hackers Reportedly Active Again," *FierceBioTechIT,* 27 May 2013, http://www.fiercebiotechit.com/story/chinesetrial-data-hackers-reportedly-active-again/2013-05-27.

13. Susan D. Hall, "Chinese Hackers Targeting the Healthcare Industry."

14. "China's 12th Five Year Plan: How it Actually Works and What's in Store for the Next Five Years," (APCO, 10 December 2010), http://www.export.gov.il/UploadFiles/03_2012/Chinas12thFive-YearPlan.pdf.

15. Ibid.

16. "China's 12th Five-Year Plan: Overview," (Beijing, China: KPMG, March 2011), http://www.kpmg.com/cn/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf.

17. Robyn E. Ferguson, "Information Warfare with Chinese Characteristics: China's Future View of Information Warfare and Strategic Culture," (Master's thesis, US Army Command and General Staff College, 2002), 15.

18. Robert Windrem, "Expert: U.S. In Cyber Arms Race With China, Russia," *NBC News Investigations*, 20 February 2013, http://investigations.nbcnews.com/_news/2013/02/20/17022378-expert-us-incyberwar-arms-race-with-china-russia.

19. James Mulvenon, "The People's Liberation Army in the Information Age," (Santa Monica: RAND, 1999), 183.

20. Timothy L. Thomas, "Google Confronts China's Three Warfares," *Parameters* 40, no. 2 (Summer 2010), http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2010summer/Thomas.pdf.

21. "Lawmaker: China Engaging in Cyber Spying," *Fox News*, 4 October 2011, http://www.foxbusiness.com/technology/2011/10/04/lawmaker-china-engaging-incyber-spying/.

22. "APT 1: Exposing one of China's Espionage Units," *Mandiant*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

23. Remarks by Tom Donilon, 11 March 2013, "The United States and the Asia-Pacific in 2013," *The Asia Society*, https://obamawhitehouse.archives.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an.

24. Steve Howard, "Obama, China's Xi Discuss Cybersecurity Dispute on Phone Call," *Reuters*, 14 March 2013, http://www.reuters.com/article/2013/03/14/ususa-china-obama-call-idUSBRE92D11G20130314.

25. M. Alex Johnson and Matthew DeLuca, "Obama Takes Diplomatic Tack on Chinese Cyberespionage Charges," *NBC News*, 7 June 2013, http://usnews.nbcnews.com/_news/2013/06/07/18804533-obama-takes-diplomatictack-on-chinese-cyberespionage-charges.

26. Devlin Barrett and Siobhan Gorman, "U.S. Charges Five in Chinese Military of Hacking," *The Wall Street Journal,* 19 May 2014, http://www.wsj.com/articles/SB10001424052702304422704579571604060696532.

27. Adam Segal, "Axiom and the Deepening Divide in U.S.-China Relations," *Council on Foreign Relations* (blog), 29 October 2014, http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-chinacyber-relations/.

28. "China," Cultural Savvy, http://www.culturalsavvy.com/china.htm.

29. Sun Tzu, *The Art of War,* http://www.theartofwar.ws/The_Art_of_War.pdf.

30. Office of the Secretary of Defense, *Military and Security Developments*, 26.

31. Thomas, "Google Confronts China's Three Warfares."

32. Office of the Secretary of Defense, *Military and Security Developments*, 26.

33. Ibid.

34. Ibid.

35. Dean Cheng, *Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response*, The Heritage Foundation report no. 2745, (Washington, DC: The Heritage Foundation, 26 November 2012), http://www.heritage.org/asia/report/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-robust-american.

36. Ibid.

37. Ibid.

38. Ibid.

39. Nathan Thornburg, "The Invasion of the Chinese Cyberspies," *Time*, 29 August 2005, http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html.

40. Jason Koutsoukis, "Chinese Waging Online Spy War," *The Age*, 10 February 2008, http://www.theage.com.au/news/national/chinese-waging-online-spywar/2008/02/09/1202234232007.html; Roger Boyes, "China Accused of Hacking into Heart of Merkel Administration," *The Times*, 27 August 2007, http://www.thetimes.co.uk/tto/news/world/europe/article2595759.ece; Donna Buenaventura, "China Tried to Hack Our Computers, Says India Security Chief M.K. Narayanan," *Donna's Security Flash* (blog), 18 January 2010, https://blogs.msmvps.com/donna/2010/01/18/china-tried-to-hack-our-computers-says-india-s-security-chief-m-k-narayanan/.

41. Nathan Ingraham, "US Government Claims Huawei and ZTE Pose a Risk to National Security: the Accusations, Responses, and Fallout," *The Verge,* 11 October 2012, http://www.theverge.com/2012/10/11/3488584/huawei-zte-us-governmentsecurity-investigation.

42. "Admit Nothing and Deny Everything," *The Economist*, 6 June 2013, http://www.economist.com/news/china/21579044-barack-obama-says-he-ready-talkxi-jinping-about-chinese-cyber-attacks-makes-one.

43. Joe McReynolds, "Cyber Transparency for Thee, But Not for Me," *The Jamestown Foundation China Brief*, 14, no. 8, http://www.jamestown.org/single/?tx_ttnews[tt_news]=42246&no_cache=1#.VTfXNBdSxdY.

44. Charles Riley, "China's Military Denies Hacking Allegations," *CNNMoney,* 20 February 2013, http://money.cnn.com/2013/02/20/technology/china-cyberhacking-denial/.

45. David Barboza, "China Says Army Is Not Behind Attacks in Report," *The New York Times*, 21 February 2013, http://www.nytimes.com/2013/02/21/business/global/china-says-army-not-behindattacks-in-report.html?_r=0.

46. "Espionage Report: Merkel's China Visit Marred by Hacking Allegations," *Spiegel Online*, 27 August 2007, http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visitmarred-by-hacking-allegations-a-502169.html.

47. "M Trends 2014: Beyond the Breach," *Mandiant*, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

48. Liz Peek, "U.S. and China in a Lethal Game of Cyber Chess," *The Fiscal Times*, 9 April 2014, http://www.thefiscaltimes.com/Blogs/Peek-POV/2014/04/09/USand-China-Lethal-Game-Cyber-Chess.

49. House, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei Technologies and ZTE*, 112th Congress, 8 October 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

50. "Huawei: Leaked Report Shows No Evidence of Spying," *BBC News*, 18 October 2012, http://www.bbc.com/news/technology-19988919.

51. Ben Blanchard, Li Hui, and Paul Carsten, "China Blames U.S. for Rise in Hacking Attacks," *The Fiscal Times*, 28 March 2014, http://www.thefiscaltimes.com/Articles/2014/03/28/China-Blames-US-Rise-Hacking-Attacks.

52. Charly Wilder, "Out of Hand: Europe Furious over U.S. Spying Scandal," *Spiegel Online*, 24 October 2013, http://www.spiegel.de/international/world/angry-european-and-german-reactionsto-merkel-us-phone-spying-scandal-a-929725.html.

53. Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobas," *The Guardian*, 9 September 2013, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

54. Edward Moyer, "NSA Spied on EU Antitrust Official Who Sparred With U.S. Tech Giants," *Cnet*, 20 December 2013, http://www.cnet.com/news/nsa-spiedon-eu-antitrust-official-who-sparred-with-us-tech-giants/.

55. Mark Hosenball, "Obama Halted NSA Spying on IMF and World Bank Headquarters," *Reuters*, 31 October 2013, http://www.reuters.com/article/us-usasecurity-imf-idUSBRE99U1EQ20131031.

56. Charlie Savage, "Watchdog Report Says NSA Is Illegal and Should End," *The New York Times*, 23 January 2014, http://www.nytimes.com/2014/01/23/us/politics/watchdog-report-says-nsaprogram-is-illegal-and-should-end.html?partner=rss&emc=rss&smid=twnytimes&_r=1.

57. "U.S., China Agree to Work Together on Cyber Issues," *Reuters*, 13 April 2013, http://www.reuters.com/article/2013/04/13/us-china-us-cyberidUSBRE93C05T20130413.

58. Peek, "U.S. and China in a Lethal Game of Cyber Chess."

59. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, (Washington, DC: U.S. Department of Justice, 19 May 2014), http://www.justice.gov/opa/pr/us-charges-fivechinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

60. Cheng, *Winning Without Fighting*.

61. Liu Kexin, *Study Volume on Legal Warfare,* (Washington, DC: National Defense University Press, 2006): 18, 34-37.

62. Eric W. Orts, "The Rule of Law in China," *Vanderbilt Journal of Transnational Law*, 1 January 2001, http://www.highbeam.com/doc/1G1-72733959.html.

63. Cheng, *Winning Without Fighting*.

64. Ibid.

65. Amy Thomson, "UN Telecom Treaty Approved Amid U.S. Web-Censorship Concerns," *Bloomberg*, 14 December 2012, http://www.bloomberg.com/news/articles/2012-12-13/u-s-and-u-k-refuse-to-sign-un agreement-on-telecommunications.

66. "U.S. and UK Refuse to Sign UN's Communications Treaty," *BBC News,* 14 December 2012, http://www.bbc.co.uk/news/technology-20717774.

67. Ibid.

68. Craig Timberg, "U.S. to Relinquish Last Control Over the Internet," *The New York Times*, 14 March 2014, http://www.washingtonpost.com/business/technology/us-to-relinquish-remainingcontrol-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html.

69. RRN Prasad, "Towards Freedom of the Internet," *The Financial Express*, 4 January 2016, http://www.financialexpress.com/article/fe-columnist/towardsfreedom-of-the-internet/187447/.

70. UN General Assembly, A/66/359, "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," 12 September 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

71. UN General Assembly, A/69/723, "Letter Dated 09 January 2015 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General," 9 January 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOf-Conduct.pdf.

72. "China Says Cyber Hacking is Against the Law," *Voice of America*, 13 January 2010, http://www.voanews.com/content/china-says-cyber-hacking-is-againstlaw-81473967/111452.html.

73. Gu Jian, "Strengthening international cooperation and joining hands in fighting against transnational cybercrime," *China.org,* 9 November 2010, http://www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm.

74. Jim Finkle, Joseph Menn, and Aruna Viswanatha, "US Accuses China of Cyber Spying on American Companies," *Reuters*, 20 November 2014, http://www.reuters.com/article/2014/11/20/us-cybercrime-usa-chinaidUSKCN0J42M520141120.

75. Mark Stokes, *The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization in China's Revolution in Doctrinal Affairs*, ed. James Mulvenon and David Finklestein (Alexandria, VA: CNA Corporation, 2005), 272.

76. Cheng, *Winning Without Fighting*.

77. Ferguson, "Information Warfare with Chinese Characteristics," 31.

78. James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, ed. James Mulvenon and Richard H. Yang (Washington, DC: RAND, 1999), 180.

79. Cheng, *Winning Without Fighting*.

80. Guo Yanhua, *Psychological Warfare Knowledge* (Washington, DC: National Defense University Press, 2005), 14-16.

81. "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting," *The White House*, 8 June 2013, http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obamaand-president-xi-jinping-peoples-republic-china-.

82. "China Says Cyber Hacking is Against the Law," *Voice of America*.

83. UN General Assembly, A/66/359, "Letter dated 12 September 2011."

84. UN General Assembly, A/69/723, "Letter Dated 09 January 2015."

85. Greg Austin, "China's Cyber Turn: Recognizing Change for the Better," *The Diplomat*, 21 December 2015, http://thediplomat.com/2015/12/chinas-cyber-turnrecognizing-change-for-the-better/.

86. Tom Orlik, "Charting China's Economy: 10 Years Under Hu," *The Wall Street Journal* (blog), 16 November 2012, http://blogs.wsj.com/chinarealtime/2012/11/16/charting-chinas-economy-10-yearsunder-hu-jintao/tab/print/.

87. "More than Minerals," *The Economist,* 23 May 2013, http://www.economist.com/news/middle-east-and-africa/21574012-chinese-trade-africa-keeps-growing-fears-neocolonialism-are-overdone-more; "China Overtakes U.S. as Brazil's Top Trade Partner," *Latin American Times*, 17 October 2013, http://www.laht.com/article.asp?ArticleId=333733&CategoryId=10718.

88. Du Wenjuan, "China Investment in Brazil More Diversified," *China Daily*, 14 May 2013, http://usa.chinadaily.com.cn/business/2013-05/14/content_16498645.htm.

89. "China's Mighty Telecom Footprint in Africa," *New Security Learning,* 14 February 2011, http://www.newsecuritylearning.com/index.php/archive/75-chinasmighty-telecom-footprint-in-africa.

90. Emilio Iasiello, "Stuffing the Genie Back into the Bottle: Can Threats to the IT Supply Chain Be Mitigated?," *Foreign Policy Journal* (3 April 2013), http://www.foreignpolicyjournal.com/2013/04/03/stuffing-the-genie-back-in-thebottle-can-threats-to-the-it-supply-chain-be-mitigated/.

91. Liat Clark, "Huawei Not a Threat to UK. Says Huawei Oversight Board," *Wired*, 27 March 2015, http://www.wired.co.uk/news/archive/2015-03/27/huawei-nota-threat-to-national-security.

92. Hafizah Osman, "Huawei Supports Australian Cyber Security Centre Development," *Arnnet.com*, 23 January 2013, http://www.arnnet.com.au/article/451519/huawei_supports_australian_cyber_security_centre_development_/.

93. Rogin, "NSA Chief: Cybercrime."

94. Marcel A. Green, "China's Growing Cyberwar Capabilities," *The Diplomat*, 13 April 2015, http://thediplomat.com/2015/04/chinas-growing-cyberwarcapabilities/.

95. Testimony of Richard Bejtlich before the U.S. China Economic and Security Review Commission Hearing on "Developments in China's Cyber and Nuclear Capabilities," 26 March 2012, U.S.-China Economic and Security Review Commission, http://www.uscc.gov/sites/default/files/3.26.12bejtlich.pdf.

96. Jonathan Fisher, "China Has Hacked Every Major U.S. Company, Claims Richard Clarke," *Web Pro News*, 28 March 2012, http://www.webpronews.com/china-has-hacked-every-u-s-major-company-claims-richard-clarke-2012-03.

97. Timothy L. Thomas, "New Developments in Chinese Strategic Psychological Warfare," *Special Warfare* 1, no. 9 (2003), http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA434978.

98. Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, 25 August 2005, http://content.time.com/time/nation/article/0,8599,1098371,00.html.

99. Tal Kopan, "White House Readies Cyber Sanctions Against China Ahead of State Visit," *CNN*, 24 September 2015, http://www.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-presidentobama/.

100. Department of Defense, *Strategy for Operating in Cyberspace,* (Washington, DC: U.S. Department of Defense, July 2011), http://www.defense.gov/news/d20110714cyber.pdf

101. Angelos Keromytis, "Active Cyber Defense," Program Information, Defense Advanced Research Projects Agency (DARPA), accessed 28 September 2017, https://www.darpa.mil/program/active-cyber-defense.

102. John Reed, "Mike Rogers: Cool It with Offensive Cyber Ops," *ForeignPolicy.com*, 14 December 2012, http://foreignpolicy.com/2012/12/14/mike-rogerscool-it-with-offensive-cyber-ops/.

103. Government Accountability Office, *National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Washington, DC: Government Accountability Office, February 2013, http://www.gao.gov/assets/660/652170.pdf.

104. Government Accountability Office, *A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges*, Washington, DC: Government Accountability Office, 7 March 2013, http://www.gao.gov/assets/660/652817.pdf.

105. Cheng, *Winning Without Fighting*.

106. "China Accuses U.S. of Hypocrisy Over Internet Spying," *Sydney Morning Herald*, 28 June 2013, http://www.smh.com.au/world/china-accuses-us-ofhypocrisy-over-internet-spying-20130628-2p0uk.html.

107. Ellen Messmer, "Don't Trust the NSA? China-based Huawei Says, 'Trust Us,'" *Network World,* 18 October 2013, http://www.networkworld.com/news/2013/101813-nsa-huawei-274959.html?page=1.

108. "FACT SHEET: President Xi Jinping's State Visit to the United States," *The White House*, 25 September 2015, https://www.whitehouse.gov/the-pressoffice/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

109. "Chinese Hackers Arrested After U.S. Request," *BBC News*, 12 October 2015, available at: http://www.bbc.com/news/technology-34504317.

110. House. *Statement of Paul K. Martin (Inspector General, NASA) on NASA Cybersecurity: An Examination of the Agency's Information Security*, Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, 29 February 2012, https://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf.

111. Ministry of Foreign Affairs, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 13, 2015*, (Washington, DC: Ministry of Foreign Affairs, 13 October 2015), http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1165638.shtml.

112. "S. Korea, Japan, China to Hold Cyber Policy Talks," *Yonhap News Agency*, 13 October 2015, http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315.html.

113. "Malaysia, China to Work Together on Cyber Crimes," *The Malay Mail Online*, 22 August 2014, http://www.themalaymailonline.com/malaysia/article/malaysia-china-to-worktogether-to-combat-cyber-crimes.

114. "S. Korea, Japan, China to Hold Cyber Policy Talks," *Yonhap News Agency*.

115. Ellen Nakashima, "World's Richest Nations Agree Hacking for Commercial Benefits Is Off-Limits," *The Washington Post*, 16 November 2015, https://www.washingtonpost.com/world/national-security/worlds-richest-nationsagree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

116. Ellen Nakashima, "Chinese Government Has Arrested the Hackers Breached OPM Database," *The Washington Post*, 2 December 2015, https://www.washingtonpost.com/world/national-security/chinese-government-hasarrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

117. "S. Korea, Japan, China to Hold Cyber Policy Talks," *Yonhap News Agency*.

118. Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other," *The Wall Street Journal* (blog), 8 May 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/.

119. Katie Bo Williams, "UK, China Mirror U.S. Anti-Hacking Pact," *The Hill*, 21 October 2015, http://thehill.com/policy/cybersecurity/257602-uk-china-mirror-usanti-hacking-pact.

120. "FACT SHEET: President Xi Jinping's State Visit," *The White House*.

121. Nakashima, "World's Richest Nations Agree."

122. David Brewster, "The Bay of Bengal: The Maritime Silk Route and China's Naval Ambitions," *The Diplomat,* 14 December 2014, http://thediplomat.com/2014/12/the-bay-of-bengal-the-maritime-silk-route-andchinas-naval-ambitions/.

123. Thitinan Pongsudhirak, "China's Aspiring Global Leadership," *East Asia Forum,* 25 November 2014, http://www.eastasiaforum.org/2014/11/25/chinasaspiring-global-leadership/.

Operationalizing Protection of Civilians in NATO Operations

Marla B. Keenan[*]
Alexander William Beadle[**]

The protection of civilians is a key objective of most international military operations. Yet civilians still continue to suffer in conflicts around the world. Since the early 1990s, the North Atlantic Treaty Organization (NATO) has conducted operations where the protection of civilians was a key component—either explicitly mandated or carried out by default to successfully achieve the mission—with varying degrees of success, and in some cases failure. This situation is not, however, unique to NATO. Implementation of protection of civilians remains a priority and challenge for many multilateral organizations, including the United Nations (UN) and the African Union (AU). This is partly due to the fact that different organizations understand protection of civilians differently, depending on their mission, capabilities, and areas of operations. While some policy, doctrine, guidance, and training have been developed, the ability to 'operationalize' civilian protection—creating and employing the force capabilities to actually protect civilians and vulnerable populations in a conflict—is still lacking.

This article does not focus on the decision by policymakers to intervene or what happens after an intervention but rather on what happens in the middle—on creating a better operational understanding of protection of civilians for NATO

[*] Marla Keenan is Director of Programs at Center for Civilians in Conflict and is a subject matter expert on civilian harm mitigation, civilian casualty tracking mechanisms and consequence management of civilian casualties. She is a Truman Security Fellow at the Truman National Security Project. Marla has trained military officers at several advanced schools and staff colleges.

[**] Alexander W. Beadle is a research fellow at a CD&E-funded project on Protection of Civilians, as well as a new project on Global Trends and Military Operations. His research has primarily focused on how military force can be used to protect civilians from perpetrators of violence. He has worked on a project with the Norwegian National Joint Headquarters that has developed a Military Planning and Assessment Guide for the Protection of Civilians in military operations.

Marla B. Keenan and Alexander W. Beadle,"Operationalizing Protection of Civilians in NATO Operations," *Stability: International Journal of Security and Development*, 4, no. 1 (2015), p. 55. DOI: http://doi.org/10.5334/sta.gr

that is more in line with civilian expectations and the particular types of threats they will have to be protected from. One useful way to conceptualize the various levels of physical protection is through *The Protection Ladder*, a theory that will be put forward in this paper. It will be shown that the hierarchical illustrative tool helps military planners understand the legal obligations and additional operational layers necessary to protect civilians from physical harm. Finally, the article outlines practical ways to better operationalize civilian protection before, during, and after operations.

It is the authors' hope that the development of a more robust understanding of protection of civilians for NATO will enhance NATO's capability to protect more civilians in future operations.

NATO and the Protection of Civilians

Protection of civilians is a matter of political will, not just military might. Troop-contributing countries may have to make difficult decisions about trading their soldiers' lives for the lives of civilians. At some point, there must also be a transition from armed conflict and stability operations—ideally to a state of peace where the rule of law and full attainment of human rights are made possible. Transitions have not always been successful, representing failures by both military and civilian actors. Experience has shown us that without a holistic approach to stability and peacekeeping, including the protection of civilians, overall mission success may prove elusive.

Once a political decision has been made to intervene in a particular conflict, military planners must develop a cohesive strategy for the military operation. Protection of civilians can become an objective in military operations in two different ways. NATO has experience with both.

First, protection of civilians may be the main objective of an entire operation—for political or moral reasons—to stop large-scale violence being perpetrated against a segment of the population. This was the case during Operation Allied Force to stop the ethnic cleansing of Albanians by Serbian forces in Kosovo (1999) and during Operation Unified Protector to stop the Gaddafi regime's violent crackdown on its own population in Libya (2011). In both instances, NATO played a primary role through its use of airpower to impose no-fly zones and strike Serbian and Libyan military targets. While the operation in Kosovo did not have a mandate from the United Nations Security Council (UNSC), the operation in Libya did.

Second, and most commonly, protection of civilians may be one of several objectives in a larger military operation. For example, in Afghanistan, while protection of civilians was not part of the explicit mandate of NATO's International Security Assistance Force (ISAF), it was arguably one of the most important military-strategic goals of the mission—receiving a greater amount of attention six years into the mission as security and kinetic operations expanded. Operations that are not explicitly mandated to protect civilians usually have a different primary goal such as counterinsurgency or counterterrorism. For example, the protection of civilians in many NATO operations is focused on the strategic goal of containing threats to member states, and others when requested, and preventing the spread of terrorism. But to a lesser extent they are focused specifically on the proactive protection of civilians. It should be noted that a failure to protect civilians—both from harm caused by one's own operations and that of other actors—may severely damage a force's ability to achieve its primary goal.[1]

Regardless of the reason for intervention in a conflict, civilians expect to be protected.[2] They are not always able to differentiate who has harmed them, but they often have a keen understanding of who has the means to provide security and protection. When forces fail to meet civilian expectations of protection or cause harm themselves, anger and resentment grow, and populations can be driven away from the forces they once relied on for protection. In the absence of security provided by NATO, for example, the population will support whatever actor can provide it, as was the case in some areas of Afghanistan.[3] The failure to protect can also damage the legitimacy of the warring parties, lead to state collapse, perpetuate cycles of violence and internal displacement, and affect neighboring countries with refugee flows.

Various NATO doctrine and guidance, including on counterinsurgency (COIN) and counterterrorism (CT), discuss the primacy of the civilian as a military-strategic imperative within each of these contexts. This is clearly laid out in the NATO counterinsurgency doctrine:

> It should be kept in mind that killing numerous insurgents will be seriously counterproductive if collateral damage kills peaceful civilians too. That will create legitimacy for the insurgency and lead to increased support from the population. For this reason commanders have to establish procedures to achieve a balanced use of force and to avoid any excessive use of force that leads to collateral damage.[4]

While most certainly true, this and other examples within doctrine and policy largely ignore the important role of protecting the population from other actors and not just NATO's own operations.[5]

In Afghanistan, for example, one could make a convincing argument that protection—both from ISAF's own operations and the operations of other antigovernment groups—should have been a key focus from the beginning. Research by CIVIC and others has shown that key strategic ground and civilian support was lost due to mounting civilian casualties both from their own operations and the operations of their adversaries.[6] ISAF eventually amended their tactics and became more effective at avoiding civilian harm from their own operations, but it was late in the game and scores of civilians were still being harmed by other groups. For example, one major source of harm to Afghan civilians was anti-government groups' use of inherently indiscriminant improvised explosive devices (IEDs) to target international and Afghan forces. In this case, the mere presence of international forces increased possible harm to civilians by IEDs in some areas, compared to areas where there was no presence. However, ISAF's counter-IED initiatives, which started out as a force protection measure, soon became a proactive protection measure and reduced civilian harm.

Unfortunately, this situation is indicative of the doctrinal gap in many organizations expected to protect civilians today.[7] While interveners may have the best intentions, they often do not have a robust strategic understanding of protection challenges, operational tools, and tactical training needed to effectively protect civilians from violence.

The implementation of protection of civilians requires understanding, knowledge, and training on how to actually achieve this objective on the ground. International, regional, and national military staff generally lacks guidance on *how* to protect civilians more effectively during military operations. This is because there are no historical or tested principles or doctrines to draw upon for military or political staff involved in the planning and execution of the mission. This lack of guidance leaves planners struggling to 'build the plane while flying it'. This is a particular challenge for missions mandated to protect civilians as their primary goal, as lives that are already lost cannot be recovered. Without well-developed doctrine and the ability to effectively implement such a doctrine, failure is likely. It should be noted that to be successful in complex environments militaries must build in flexibility to allow for quick adaptation as the situation on the ground can change rapidly.

What 'Protection' Means

Civilians are entitled to the full spectrum of protection including physical protection from imminent violence, provision of basic necessities, enjoyment of human rights, and enabling conditions. Professor Paul D. Williams offers this definition in his 'protection onion' framework:

> [The Protection Onion is an] adaptation of the ICRC's "egg framework," which was developed in the late 1990s to depict the relationship between patterns of

> abuse and what the organization saw as the three forms of protection activities (responsive, remedial, and environment-building). This emphasizes that protection can be thought of in minimalist (physical survival) or maximalist (the enjoyment of rights) terms and hence as a concept that contains many interconnected layers. Ideally, civilians would be able to enjoy the whole package, but in practice they can lose the outer layers of protection and still survive, although clearly some individuals can endure more than others. The inner core of physical protection, however, is vital for all the other layers.[8]

A military force alone cannot undertake all of these activities. It must understand what the protection of civilians entails and identify where it can be most helpful in the larger protection space. For policy makers and military planners involved in the deployment of intervention forces, the focus should be on the 'inner core of physical protection,' as it is where a military intervention can have the most utility through measured use of force.

To effectively protect, the military force must understand the threats that exist and match capabilities to counter them. This is a unique role, one that other unarmed actors are unlikely able to play. Actors such as NGOs and civil society have other important roles in providing protection—for example, addressing humanitarian concerns. While a military force's main focus will be on physical protection, there may be occasions when it chooses to cooperate with counterparts on other levels, for example, in logistical assistance in the provision of basic necessities. Effective communication with counterparts focused on protection of civilians is imperative to maximize all capabilities.

For any military force to understand and effectively operationalize protection of civilians, it must first have a clear, organization-wide definition and a shared strategic understanding of the concept of protection. For example, the UN defines protection broadly as:

> All activities aimed at obtaining full respect for the rights of all individuals in accordance with international law—international humanitarian, human rights, and refugee law—regardless of their age, gender, social ethic, national, religious, or other background.

The UN further defines protection of civilians in armed conflict as:

> Protection of civilians in armed conflict (POC), whereby all parties to the conflict are responsible for ensuring that the civilian population is respected and protected.

NATO's current understanding of protection of civilians differs greatly from that used by other international and regional organizations such as the UN and the AU. While NATO has yet to adopt a formal definition of protection of civilians, in past conflicts it has focused primarily on protecting the population from their own actions. In an environment where these actors work together, varying definitions of 'protection' can wreak havoc on even the best-laid protection plans.

Conceptualizing Physical Protection

After years of working on this issue, the authors strongly believe that military planners need a more formal structure to understand the several layers of physical protection. The Protection Ladder was designed by Center for Civilians in Conflict as an illustrative tool for military planners and leaders to explain the legal obligations and additional operational layers involved in civilian protection (See Figure 1). The ladder is meant to help conceptualize and operationalize these various layers—what we call 'rungs'. Capabilities must be established on each rung to achieve the full range of civilian protection. The skills learned on each rung provide a foundation for the next. As with any ladder, the greater the number of rungs, the stronger the structure and the greater its reach.

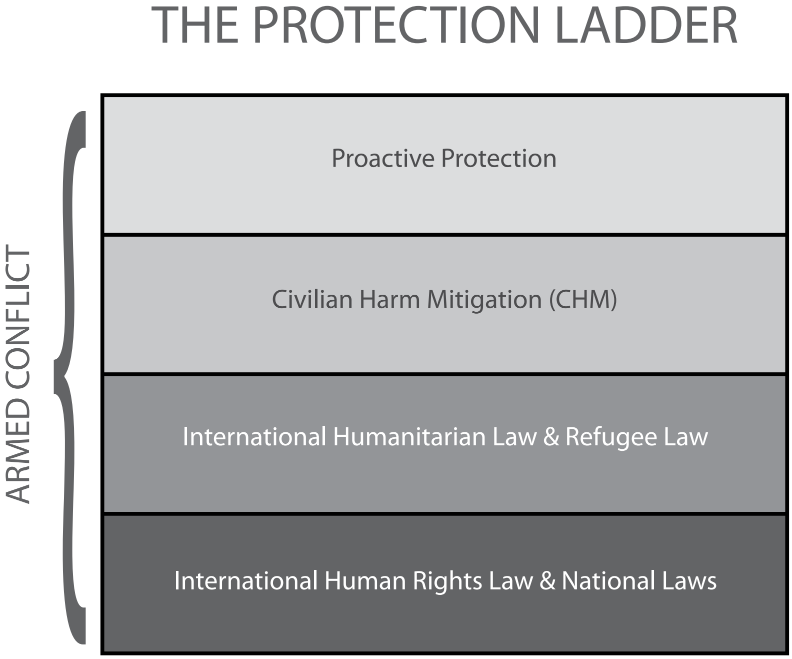
THE PROTECTION LADDER
ARMED CONFLICT
Proactive Protection
Civilian Harm Mitigation (CHM)
International Humanitarian Law & Refugee Law
International Human Rights Law & National Laws

Figure 1

The Protection Ladder is a conceptual framework to understand the various layers of physical protection security forces can provide to civilians either by adherence to existing national and international law or the adoption of specific policies and procedures that go above and beyond what is required.

International Human Rights Law & National Laws

The foundational rung of protection is the application of national law and international human rights law. These laws are applicable during times of peace as well as civil unrest and armed conflict. They are also the foundation for civilians receiving protection from their government and other actors. In most cases police and gendarmerie are the primary upholders of these laws. If security forces and other armed actors are found to have violated these laws, the violators should be prosecuted through the appropriate channels.

International Humanitarian and Refugee Law

International humanitarian law (IHL) and refugee law exist to protect civilians from the dangers of armed conflicts. It prevents parties from directly targeting civilians (distinction) and from causing excessive incidental civilian damage while attacking military targets (proportionality). It also calls on parties to conflict to take all feasible precautions to avoid harming civilians. Militaries who adhere to IHL cause less civilian harm during their combat operations. However, in today's conflicts, many armed actors (both government and armed non-state actors) either fail to consistently adhere to IHL or choose not to adhere at all. When there are violations of IHL, they must be documented and prosecuted.

Civilian Harm Mitigation

Despite the best efforts of a given military operation, and even when the principles of IHL are rigorously applied, harm to civilians may nevertheless occur as a direct consequence of the use of force. This type of harm can happen during planned operations or in self-defense. This 'incidental harm'—often referred to as 'collateral damage'—while not illegal must be minimized, investigated, and appropriately addressed by the military force.

Proactive Protection

Armed actors may also deliberately target civilians, because they believe it can serve their overall objectives. In this case, a third actor is needed to intervene to prevent or mitigate the violence. Those who specifically target civilians are responsible for the vast majority of civilian casualties. This has led to the realization that protecting civilians from physical violence often requires proactive use of force against the perpetrators. This could mean establishing a presence near vulnerable populations, patrols, placing oneself between the perpetrator and the potential victim, and/or proactively seeking out those who wish to harm civilians and neutralizing the threat. The key decision facing staff involved in the planning or execution of such operations, is matching these approaches to particular situations.

Operationalizing Physical Protection

Civilian protection is first and foremost about creating a mindset—a way of thinking among policy makers, military planners, commanders, and soldiers. It must be adopted as strategy and policy and then trained throughout the chain of command to ensure that everyone from the highest commander to the lowest ranking soldier understands the concept and why it is a key part of a successful mission.

A military force cannot undertake all protection activities. It must effectively identify where it can be most helpful. To effectively protect, the military force must understand the threats that exist and match capabilities to counter them—a role that unarmed actors are unable to play. Protection takes place along the entire continuum of a military operation—before, during and after. A protection strategy in itself is not enough; it must be planned, operationalized, and trained at all levels. Below, we discuss practical suggestions on how civilian protection can be effectively addressed during planning, execution, and assessment of military operations conducted by NATO.[9]

Before Operations

Strategy, planning, and training are pivotal to NATO's success in the protection of civilians. Without an explicit focus on protection of civilians in this 'before' stage, there is little chance of effectively protecting civilians in the conflict.

Adopt standing policy and tools

The concept of protection—including a definition in line with other international organizations—should be adopted in standing NATO political and military policy, independent of any given conflict. Protection should be prioritized in strategic planning and taught in scenario-based trainings. It should become a part of the military decision-making process and, indeed, the decision-making process of the individual soldier.

The Civilian Casualty Mitigation Team (CCMT) and the *Nonbinding Guidelines on Monetary Payments to Civilian Casualties in Afghanistan* are examples of effective NATO policy and practice but these exist only in an individual conflict. These practices have yet to be enshrined by NATO in standing policy and therefore the lesson identified in these recent conflicts risk being lost rather than learnt. We discuss these practices further in the *During Operations* section.

Develop a robust threat assessment process

Eventually, it is the perpetrators who decide what kind of threat they pose to civilians. It is impossible to answer the question of "how" civilians can be protected without knowing why, how, and with what methods perpetrators use in the first place.

The *proactive* part of protecting civilians is where guidance is most lacking, and all organizations have struggled to operationalize the task, including NATO. Previous research has found that the overall scope of threats that NATO may face can be divided into seven scenarios.[10]

- **Genocide**, where perpetrators seek to exterminate a communal group (e.g. Rwanda, 1994).
- **Ethnic cleansing**, where perpetrators seek to expel a communal group (e.g. Kosovo, 1999).
- **Regime crackdown**, where regimes use violence to repress any resistance (e.g. Libya, 2011).
- **Post-conflict revenge**, where individuals or mobs take revenge for past crimes (e.g. Kosovo post–1999).
- **Communal conflict**, where whole communities seek both to avenge a previous round of violence and to deter further retribution as a means of protecting themselves (e.g. Ituri, DR Congo, 1999–2003).
- **Predatory violence**, where perpetrators exploit civilians to survive or for profit (e.g. Lord's Resistance Army, 1994–present).
- **Insurgency**, where rebels target civilians as a means to control the population and to undermine the control of other actors (e.g. Afghanistan, 2002–present).

NATO has encountered most of these scenarios and also stands out as one of few actors that may be expected to protect civilians from *all* of these threats, including interventions in the worst-case scenarios of large-scale violence against civilians.

Each of these situations poses a fundamentally different threat to civilians in terms of which civilians are at greatest risk, how they are targeted, what capabilities the perpetrators rely on to conduct violence, and what kind of civilian suffering it is likely to produce. This underscores the importance of identifying the particular type(s) of threats civilians are faced within the area of operation. In most conflicts, however, several scenarios may unfold simultaneously, in different areas or during phases of a conflict. For instance, what started as a regime crackdown on armed and unarmed opposition in Kosovo during the mid-1990s eventually escalated into ethnic cleansing of the Albanian population by 1999, prompting NATO's intervention. Following the Serb withdrawal and NATO deployment, the ethnic cleansing was followed by post-conflict revenge against Serbs and other non-Albanian minorities. This again escalated into ethnic cleansing of the remaining Serbs in 2004.

The point is that continuous threat assessments of the perpetrators are essential to achieve effective physical protection. Some scenarios may also unfold at the same time involving the same perpetrator. For instance, a communal militia may simultaneously be attacking another community as a way to protect their own, while behaving in a predatory manner against all communities in the area. Other motivations for targeting civilians are mutually exclusive. It is for instance impossible to expel and physically exterminate a whole group of civilians at the same time. There may also be different motivations within the perpetrators' ranks. For individual fighters, they may gain respect from their comrades or be driven by a fear of being killed themselves. For mid-level leaders, it may be to acquire power. That said, in order for violence to become systematic and widespread enough to prompt a military response, the overall situation is likely to fall into one of the categories of perpetrator motivations listed above.

The main implication is that different scenarios require different military responses if civilians are to be protected, without causing more harm in the process. On the one hand, this requires responses that reduce the vulnerability of targeted civilians and support their own coping strategies, such as by building infrastructure that allows them to access water within a relatively safe distance and by providing information about possible threats.[11] On the other hand, it often requires using military forces to address the threats of violence more directly.

Different approaches to the use of military force to protect civilians will involve varying levels of proactivity:

- Assistance with the delivery of humanitarian aid to ameliorate the crisis (e.g. transport, air drops, construction of camps or roads, convoys, securing storage facilities).
- Containment of the conflict (e.g. no-fly zones, embargoes, securing weapon depots).
- Deterrence or defense against attacks on civilians (e.g. patrols; escorts; protection of safe areas/zones like villages, stadiums, public buildings or camps; interpositioning).

- Coercive use of force against perpetrators (e.g. threats, show of force, strategic punitive strikes).
- Attack or defeat of perpetrators (e.g. strategic air strikes, direct action, warfighting).

The central question for military planners is: *Which of these approaches are most likely to protect civilians from the conflict situation and the particular type of perpetrator they face?* This question can be answered according to two principles.

First, to have a strategic effect, the response must mirror the perpetrator's original *motivation* for targeting civilians. For example, genocidal perpetrators, who perceive the situation in zero-sum terms and have decided that extermination of a specific group is the only viable option, are highly unlikely to be deterred. Lessons from previous genocides, such as with the Hutu extremists in Rwanda and Nazi Germany during World War II, indicate that these perpetrators will continue exterminating civilians until they are completely defeated. By contrast, predatory armed groups who only target civilians to acquire resources necessary to survive (e.g. by plundering food or forcibly recruiting children to maintain their ranks) are much easier to deter and can be coerced into stopping altogether. This is because their primary motivation is to stay alive, which means that they will seek to avoid confrontation. That is why they typically target undefended locations where risks are low and rewards are high. In the past, even limited shows of force have caused many fighters to demobilize and disarm.

Second, the operation needs to match the perpetrator's specific *modus operandi*. This requires a deeper understanding of how perpetrators target civilians and what they require to do so. For instance, NATO carried out similar actions during the operations in Kosovo and Libya, but the outcomes were quite different in terms of protecting civilians from the respective threats they faced. In both operations, NATO imposed a no-fly zone and conducted air strikes against military targets and command and control locations. However, the threats to civilians were different, which meant the utility of this operational design would differ, too.

In Kosovo, Milosevic sought to expel a large portion of the Albanian population through demonstrative use of violence. The purpose was not to kill or even to control them in the future, but to make them leave. Doing so only requires freedom of movement for irregular, paramilitary units to conduct brutal violence that makes people flee in advance. Thus, striking conventional military units had little effect on the Serbian regime's ability to conduct ethnic cleansing, because these operations could be conducted without support from conventional forces. The operation eventually took far longer than expected, and around 90 percent of Kosovo Albanians were displaced, many of them expelled during the air campaign itself. Even though Milosevic eventually conceded defeat, withdrew his forces, and Kosovo Albanians were allowed to return, it could hardly be argued that the operation itself successfully protected civilians from expulsion.

In Libya, Gaddafi did not seek to kill or expel a certain group of the population but to control the population. To do so, he depended on crushing all opposition, both armed and unarmed. This first and foremost requires substantial firepower (as demonstrated also by the weapons used by Assad in Syria, including aerial bombing, SCUD-missiles, and weapons of mass destruction). In fact, regime crackdowns are the only situations where regular forces and heavy firepower are the units primarily responsible for violence against civilians. Thus, targeting Gaddafi's regular forces and command and control abilities in Libya degraded his ability to target civilians. Compared to the air campaign in Kosovo, civilians were gradually protected from the threat posed by Gaddafi. This threat was removed by Gaddafi's death—likely to be the only way, as few authoritarian leaders whose main objective is to save themselves have ever negotiated themselves out of power. However, the post-conflict revenge that followed was left unaddressed; the gradual deterioration of the security situation has created new and different types of threats to civilians.

Civilian Harm Mitigation

In most of the situations listed above, some sort of offensive use of military force will be needed to reduce the physical threat to civilians. However, this involves the potential risk of causing harm to civilians during protection operations. The more serious the threat to civilians, the more the use of force is likely to be required to confront the perpetrators—and the higher the danger it is likely to pose to civilians.

This risk of harm can be reduced through the adoption and implementation of civilian harm mitigation policy, tools, and practices. For example, while there is often training of forces on the IHL rules of proportionality, distinction, and necessity, state actors or non-state armed groups that want to effectively protect the population from harm need to go much further to ensure this actually happens once a conflict begins. Protection requires advanced planning and tactics to push commanders and soldiers not just to ask themselves '*Can* I pull the trigger' (under IHL, is it legal?), but '*Should* I pull the trigger' (under civilian harm mitigation, is it my best option, what are the ethical and strategic imperatives, is there a better way?), and even 'How can I *prevent* my enemy from pulling the trigger' (under proactive protection, can I prevent harm to civilians?).

Pre-engagement planning activities can include, but are not limited to: assessing the potential of collateral damage with a restrictive framework; adopting rules of engagement that limit civilian harm; training forces with a mindset of civilian protection; acquiring non-lethal weapons to be used whenever possible; ensuring strict and appropriate targeting practices; and, importantly, setting up systems of proper data tracking and analysis, investigatory capacities, and the making of amends.[12]

All of this should be done *in advance* of the start of military operations. As additional lessons are learned, commanders' guidance, rules of engagement, and other directives should be revised accordingly and fed into in-mission trainings.

During Operations
Understanding civilians' reality during conflict

In order to ensure that an armed actor's use of force is actually effective in protecting civilians, commanders must have a real-time understanding of how civilians are being harmed. A military force should maintain a small team to advise the commander on civilian protection. Within this team it is important to develop the capability to consistently track in a centralized database all civilian harm caused and systematically analyze the data for trends, challenges, and lessons learned.[13] While a relatively new concept in warfare a 'tracking cell' generally consists of several expert staff and appropriate hardware and software for data tracking and analysis. By adding this analysis to the commander's feedback loop, challenges to protection can be addressed. Tactics can be adjusted to better protect, and in-mission trainings created to ensure soldiers have up-to-date protection tools, so ultimately, more lives can be saved. Similarly, proper investigations into every incident of potential civilian harm allow the military to absorb crucial data about threats to civilians. NATO has done this in Afghanistan.

In 2008, the International Security Assistance Force—the NATO led security mission in Afghanistan—created a Civilian Casualty Tracking Cell (CCTC) to collect data on civilian casualties—the first of its kind in any conflict. The cell functioned initially simply as a repository for data. In July of 2009, SOP 307 was released providing guidance on how to respond to civilian casualties through a procedural checklist, what military commanders call a 'battle drill'. The SOP strengthened the cell and enshrined it as the "authoritative repository of civilian casualties taking place in the Afghanistan theater of operations."[14] By 2011 the cell was a key part of ISAF's understanding of and response to civilian harm and was renamed the Civilian Casualty Mitigation Team to reflect the more robust form and function.[15]

No less important but much harder to assess is the degree to which one's actions lead to better protection from armed actors deliberately targeting civilians. Assessing physical protection of civilians from perpetrators of violence can be done in several ways.[16] Beyond simply tracking civilian harm, the mission must monitor civilian behavior, civilians' perception of security, shifts in territorial control, delivery of humanitarian assistance, and perpetrator capabilities.

What constitutes a relevant measure obviously depends on the type of threat. For example, there is little point in assessing public opinion when most civilians are being killed (i.e. genocide). There is also little point in focusing on civilian deaths if large numbers of people are being abducted or displaced. What is particularly important from the perspective of military planning and execution is to monitor the perpetrator's *capabilities* of violence. Reducing them is obviously one way of monitoring proactive protection of civilians, including the perpetrator's ability to escalate violence.

The only true way to determine whether civilians are actually being protected is to measure the civilian suffering against what could be expected to happen if the perpetrators succeeded and no protection effort were tried. While difficult, this can be done by assessing the perpetrator's *modus operandi* and empirical evidence from previous conflicts where similar situations have existed. For instance, during previous genocides, more than half of the targeted group's population has actually died. About 80 per cent of the Herero Africans were killed in Namibia (1904), about 67 per cent of European Jews during the Holocaust, and about 75 per cent of Tutsis living in Rwanda (1994). By contrast, only a few per cent of the targeted population is likely to be killed during ethnic cleansing. However, the vast majority (90+ per cent) is likely to be displaced either temporarily (as with the Albanians in Kosovo) or permanently (as with many Muslims who lived in what became Serb-controlled areas of Bosnia).

Addressing Civilian Harm

All incidents of harm to civilians attributable to one's own forces should be fully investigated. Cases found to be violations of international law should be dealt with through appropriate legal channels. Harm to civilians—including property damage, death, or injury—determined to be within the lawful rules of engagement of the peacekeeping force and thereby incidental should be acknowledged. Individuals or communities should be assisted accordingly. Making amends for harm within the lawful parameters of operations contributes to the preservation of human dignity and community healing. Strategically, acknowledging and responding to harm minimizes any hostility that may grow when harm is left unaddressed. Amends can range from apologies and dignifying gestures to other in-kind assistance, in accordance with local culture and victims' preferences.

From early on in the conflict several of the troop contributing countries were making payments to civilian families harmed by their combat operations. However, there were no standardized guidelines across NATO so civilians were treated differently depending on which nation harmed them. This sometimes caused confusion and anger amongst the civilian population.[17] In August 2010, NATO nations approved *Non-binding Guidelines on Monetary Payments for Civilian Casualties in Afghanistan* designed to synchronize troop contributing nation efforts to make amends to civilians harmed as a result of combat operations. While non-binding, these guidelines were incredibly important in getting nations on the same page with regard to how civilians should be treated when harmed by combat operations. Despite the positive effect this development had in Afghanistan they have yet to be enshrined in NATO's standing policy or procedures. In Libya, civilians harmed as a result of the NATO air campaign were requesting these payments but with no policy in place their calls fell on deaf ears.

After Operations
Learning the Lessons of Past Conflicts

One of the most important practices a military force can undertake post-conflict is to gather best practices and lessons identified. Lessons will not be learned until the strategic, operational, and tactical adjustments are adopted into standing policy and practice to ensure better performance in the next conflict. For several years, NATO has been conducting its own lessons identification process, including the release of reports on Libya and Afghanistan and an ongoing effort to map protection of civilian capabilities.

It should also be noted that there is an inherent danger in simply replicating lessons from one theatre of operations to another without adjusting to address the specific threat. This is particularly true of lessons regarding proactive use of force to protect, where the threats to civilians and the utility of different military responses can vary greatly. Direct lessons are only useful insofar as one is faced with the same type of threat to civilians as one was in the conflict in which the lesson was identified. Therefore, lessons should be examined, amended, and applied within the existing conflict and context to ensure maximum efficiency.

Conclusion

As long as wars are fought among, against, and in defense of civilians, the ability to protect civilians will continue to be a key capability.[18] As new potential operations arise where protection of civilians will be important, such as in Syria, Iraq, or even Libya again, NATO should develop its capability to plan and effectively implement protection strategies.

Building an effective protection response capability depends on having a comprehensive understanding of protection of civilians and a strategic focus on developing capabilities in implementation. NATO should develop its planning, preparation, execution, and assessment capabilities of future missions—regardless of whether protection of civilians is the primary objective or is essential for military-strategic reasons. Its success in future endeavors depends upon it.

Notes

[1] Paul Williams, "Enhancing Civilian Protections in Peace Operations: Insights from Africa" Africa Center Research Paper no.1 (Washington, DC: Africa Center for Strategic Studies, 20 September 2010, http://africacenter.org/wp-content/uploads/2010/09/ACSS-Research-Paper-1.pdf.

[2] Based on a decade of CIVIC's independent research with civilians garnering their perceptions, wants, and needs. Research has been conducted in Iraq, Syria, Afghanistan, Somalia, Pakistan, and Mali, etc.

[3] Headquarters, Department of the Army, "Army Tactics, Techniques, and Procedures (ATTP) 3-37.31, Civilian Casualty Mitigation," July 2012, 1-8, para. 1-43, https://fas.org/irp/doddir/army/attp3-37-31.pdf

[4] North Atlantic Treaty Organization, "Allied Joint Doctrine for Counterinsurgency (COIN), - AJP-3.4.4," 2011, https://publicintelligence.net/nato-allied-joint-doctrine-for-counterinsurgency/.

[5] Protecting civilians from one's own actions—commonly referred to as civilian harm mitigation (CHM)—is a very important part of the larger concept of protection of civilians but NATO has historically interchanged the definition of protection of civilians with CHM.

[6] E.L. Gaston and Rebecca Wright, *Losing the People: The Costs and Consequences of Civilian Suffering in Afghanistan*, Campaign for Innocent Victims in Conflict (CIVIC) Conflict Series (Washington DC: CIVIC, 18 February 2009), http://civiliansinconflict.org/wp-content/uploads/2017/09/losing-the-people_2009.pdf.

[7] Alison Giffen, *Addressing the Doctrinal Deficit: Developing guidance to prevent and respond to widespread or systemic attacks against civilians*, Report from an International Experts Workshop, 21-24 September 2009, (Washington DC: The Henry L. Stimson Center, 2010), https://www.stimson.org/sites/default/files/file-attachments/1_-_Addressing_the_Doctrinal_Deficit_2010.pdf.

[8] Paul Williams, "Enhancing Civilian Protections in Peace Operations".

[9] The Norwegian Defence Research Establishment (FFI) has developed guidance for military staff on how key considerations on protection of civilians can be included during a regular NATO military planning process. See Alexander W. Beadle and Stian Kjeksrud, "Military planning and assessment guide for the protection of civilians", FFI-rapport 2014/00965 (Kjeller: Norwegian Defence Research Establishment, 2014).

[10] Ibid.

[11] Aditi Gorur, *Community Self-Protection Strategies: How peacekeepers can help or harm*, Civilians in Conflict Issue Brief no. 1 (Washington DC: The Henry L. Stimson Center, August 2013), https://www.stimson.org/sites/default/files/file-attachments/Stimson_Community_Self-Protection_Issue_Brief_Aug_2013_0.pdf.

[12] Making amends is the practice of warring parties providing recognition and assistance to civilians they harm within the lawful parameters of their combat operations, despite having no legal obligation to do so. At its core, the practice of making amends is a gesture of respect to victims. Amends can take a variety of forms and must be culturally appropriate. They can include public apologies, monetary payments, livelihood assistance programs, and other offerings in accordance with victims' needs and preferences.

13. Two distinct but connected approaches to documenting harm in armed conflict are emerging as good practice among militaries worldwide: 'civilian harm tracking' and 'casualty recording'. Casualty recording is the process of recording every individual killed in armed violence (which includes but is not limited to armed conflict as defined by IHL) in a systematic and continuous manner. Civilian harm tracking refers to the warring party itself (state militaries, peacekeepers, military coalition members) systematically gathering and analyzing data about their operations and its effects on the civilian population, including data on civilian deaths, injuries, property damage and other civilian harm as appropriate. The goal of tracking is to use the analysis to update the warring party's tactics and training in order to lessen civilian harm in future operations, ensure thorough investigations, and enable warring parties to respond properly to civilian harm, including by making amends for losses. Both casualty recording and civilian harm tracking are necessary and useful in that they work towards providing recognition of those killed and their families and serve to inform distinct actors who seek to address harm and improve protection. And where feasible, information from both approaches can be combined to produce the fullest understanding of civilian harm.

14. Jennifer Keene, *Civilian Harm Tracking: Analysis of ISAF Efforts in Afghanistan*, Campaign for Innocent Victims in Conflict (CIVIC) (Washington DC: CIVIC, 2014), http://civiliansinconflict.org/uploads/files/publications/ISAF_Civilian_Harm_Tracking.pdf.

15. Ibid.

16. Alexander W. Beadle and Anders S. Våge, "Assessing Protection of Civilians in Military Operations", FFI-rapport 2014/00966 (Kjeller: Norwegian Defence Research Establishment, 2014).

17. E.L. Gaston and Rebecca Wright, *Losing the People*.

18. Alexander W. Beadle, "Protection of Civilians as a New Objective for Military Forces" in *International Military Operations in the 21st Century: Global trends and the future of intervention*, eds. P M Norheim-Martinsen and T Nyhamar (New York: Routledge, 2015), 195–205.