Marine Corps University JOURNAL

Volume 6, Number 2 Fall 2015

Subscribe Today

Subscriptions to *Marine Corps University Journal* are free. To join our subscription list or to obtain back issues of the *Journal*, send your mailing address to Marine Corps University Press at MCU_Press@usmcu.edu.

Article Submission

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

Cover: The Nigerian Army prepares to deploy for another mission against Boko Haram as they attempt to locate the missing Chibok schoolgirls.

Photo courtesy of *Vice News.*

Marine Corps University JOURNAL

Volume 6, Number 2 Fall 2015

Marine Corps University Press
3078 Upshur Avenue
Quantico, VA 22134

Information about MCU Press and the *Journal*, as well as submission guidelines, can be found online at
https://www.mcu.usmc.mil/mcu_press

Marine Corps University Journal (Print)
ISSN 2164-4209

Marine Corps University Journal (Online)
ISSN 2164-4217

Marine Corps University Journal • Marine Corps University Press • 3078 Upshur Avenue • Quantico, VA 22134
(703) 432-4888

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

Marine Corps University
JOURNAL
Volume 6, Number 2 Fall 2015

Articles

MARINE CORPS UNIVERSITY

MARINE CORPS UNIVERSITY PRESS

President's Foreword

In 2009, a militant Islamist group commonly known as Boko Haram began a campaign of terror across northeastern Nigeria with the main purpose of removing all Western influences and replacing the national government with an Islamic state. For more than a decade, the U.S. government has worked extensively with foreign governments to counter these types of acts around the world, often with mixed results. As such, interoperability, or the capacity of one element of the government to work with another, has become a critical component of America's international relations and national security policies. As we transition from U.S. involvement in ground wars in Iraq and Afghanistan to monitoring civil unrest throughout the Middle East and Africa, American forces must continue to apply the fundamentals of counterinsurgency (COIN) and cultural operations to their roles within the evolving battlespace.

This issue's opening article—"Rethinking the U.S. Approach to Boko Haram"—focuses on how regional issues in western Africa have become international concerns for countries with interests in the area, particularly the United States. Julia McQuaid and Patricio Asfura-Heim paint a vivid picture of the resilience of Boko Haram to internal and external pressures as the viciousness of their actions escalates, causing widespread fear among the general populace even though the group seems to lack real power to force change on the government. The authors also found that the lack of legitimacy of Nigeria's government, combined with the fractured nature of the Islamic community, directly impacts whether nongovernmental actors can counter Boko Haram's radical narrative and violent behavior. McQuaid and Asfura-Heim then present a variety of methods, with a particular focus on traditional COIN operations and a whole-of-government approach, for combating the effects of terrorism in Nigeria. The authors' research highlights the fact that internal and external agencies have, failed to focus on a single effective strategy that coordinates stakeholders for a shared goal along common timelines.

José de Arimatéia da Cruz and Taylor Alvarez continue the discussion on the effectiveness of international strategies with "Cybersecurity Initiatives in the Americas." Their article takes a somewhat ironic look at how a growing population of cybercriminals, who are not bound by morals or ethics, use the Internet to pursue illegal agendas while law enforcement and government officials are restricted to legal means to create solutions for these problems. In an effort to thwart some of these unlawful cyberevents, the authors focus on the shared initiatives of Argentina, Brazil, Cuba, Mexico, and Venezuela to improve their responses to computer-generated threats. In the wake of the Sony and Edward Snowden–National Security Agency information leaks, many Latin American nations began cooperative agreements to improve their defense capabilities through Cyber Security Incident Response Teams. In spite of these actions, the proliferation of digital technology in Third World and developing nations means that terrorists have fewer boundaries and more tools to spread their message without fear of retaliation or consequence. The significant increase in cyberwarfare incidents demonstrates quite graphically that Latin American states must have a deeper understanding of the cyberthreats made against their intellectual property, and international efforts to counter cybercrime must encourage collaboration across geographic borders and social science disciplines.

In the final article, Tal Tovy further explores international and cross-disciplinary efforts in "Sociocultural Intelligence Apparatus." Tovy posits that understanding a society's characteristics lies at the center of preventing the general population's support of insurgent activities during a time of conflict. In this framework, war conduct is a "direct outcome of a society's cultural makeup." Although modern insurgencies in Iraq or Afghanistan immediately come to mind, Tovy believes that many of the issues faced by our military in these modern examples can also be seen in earlier conflicts, such as the Vietnam War. In his article, he examines the role of anthropological studies as a tool for war propaganda in Vietnam. In this instance, Tovy focuses on how propaganda was used by the United States and the Republic of Vietnam (South Vietnam) to encourage desertion among the Viet Cong. Modern COIN theories, as a result, place a great deal of emphasis on how the general population becomes the center of gravity for any guerilla force. Thus, Tovy's article further illustrates the significance of cultural understanding and psychological warfare that still resonates today: take care of the people and deprive the insurgents of everything else necessary for war.

As Marine Corps University prepares for 2016 and beyond, including our move into the Brigadier General Edwin H. Simmons Marine Corps History Center and the Warner Center for Advanced Military Studies, we must reflect on the lessons of the past as we continue preparing students for the future. As we equip America's military leaders to rise against global terrorist threats, we would do well to remind ourselves of this aphorism: "Five percent of the people think; 10 percent of the people think they think; and the other 85 percent would rather die than think." We must continue to challenge existing notions of military academia and the part it plays in American security and international relations to ensure that professional military education meets the challenges of the future, including small wars, irregular wars, and cyberwars. By maintaining this focus, we will be able to look back with satisfaction on our efforts to prepare students to be part of the 5 percent who think.

H. G. Pratt
Brigadier General, U.S. Marine Corps Reserve
President, Marine Corps University

Rethinking the U.S. Approach to Boko Haram: The Case for a Regional Strategy

by Julia McQuaid and Patricio Asfura-Heim
with contributions from Daniella Mak and Alexander Powell

Since 2009, the Nigerian Islamist group Jama'a Ahl as-Sunna Lida'wa wa-al Jihad, commonly called Boko Haram, has been waging a violent insurgent campaign in the northeastern part of Nigeria (see map 1). Its goal is to expel the political community from northern Nigeria, remove all Western influences, and eventually overthrow the national government and establish an Islamic state in its place.[1] Since 2010, Boko Haram has been responsible for more terrorist attacks in Nigeria than all other militant groups combined,[2] destroying vital infrastructure and devastating the already weak economy in the northeast of the country. Attacks on the Christian community in the south exacerbate preexisting religious tensions, reversing some of the country's hard-won gains in building national unity. Boko Haram has clearly become the most serious physical threat to stability in Nigeria.

The Nigerian government's military-oriented response has failed to stem the violence. While the Nigerian military has occasionally

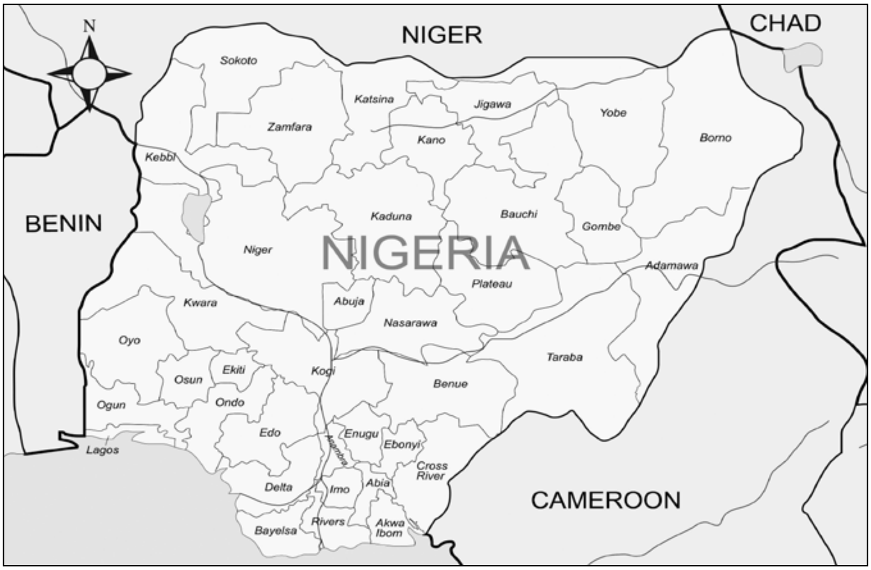
McQuaid is a senior political-military analyst in CNA's Center for Stability and Development. Her research focuses on a range of strategic and operational issues, such as building partner capacity, counterterrorism, insurgencies and nonstate actors, and maritime security. She has conducted research throughout Africa and the Middle East, including in Oman, Jordan, Mali, Benin, Morocco, and Algeria.

Asfura-Heim is an irregular warfare expert. He has conducted numerous studies on community self-defense groups and partner capacity building and has carried out fieldwork in Iraq and Afghanistan on behalf of the U.S. Marine Corps. He has authored and coauthored numerous articles, including "The Rise of Mexico's Self-Defense Forces: Vigilante Justice South of the Border," which was written with Ralph Espach for *Foreign Affairs*.

[1] National Counterterrorism Center, *Counterterrorism Guide*, "Terrorist Groups: Boko Haram," 31 July 2014, http://www.nctc.gov/site/groups/boko_haram.html.

[2] James J. F. Forest, *Confronting the Terrorism of Boko Haram in Nigeria,* JSOU Report 12-5 (MacDill Air Force Base, FL: Joint Special Operations University, May 2012), http://cco.dodlive.mil/files/2012/09/Boko_Haram_JSOU-Report-2012.pdf.

Map 1. Nigeria's administrative divisions



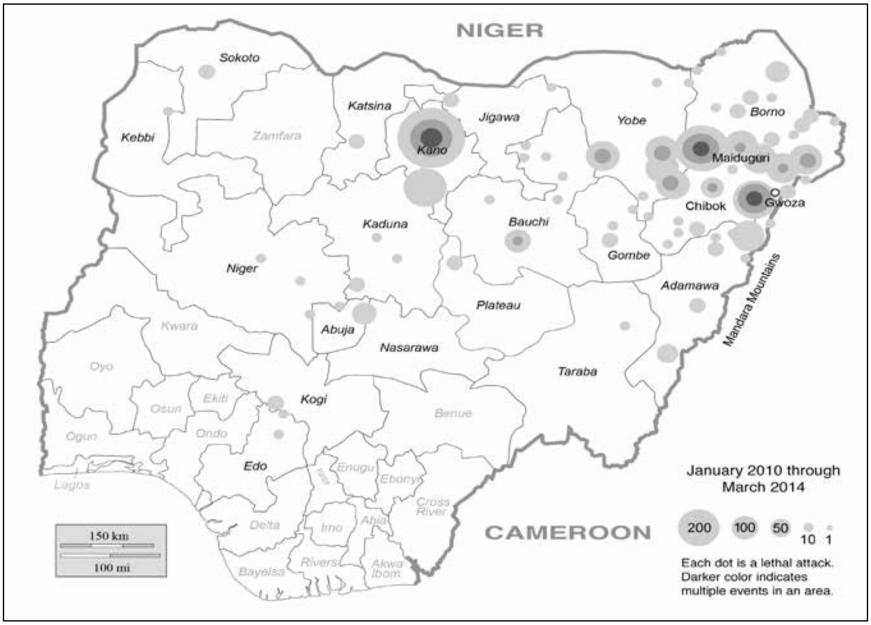
Map courtesy of Michael Markowitz, CNA.

eliminated elements within Boko Haram's leadership and rank and file, the group has proven to be highly resilient. After declaring a state of emergency in the northeast, the government launched an offensive targeting Boko Haram's safe havens in May 2013. Despite this initial disruption of activities, Boko Haram grew increasingly active, brazen, and tactically sophisticated in its attacks against both civilians and government targets in 2014 (see map 2).[3] The failure of the government to contain the violence, the recent bombings in the south and the Federal Territory of Abuja, and Boko Haram's threats to disrupt the 2015 presidential election have created a legitimacy crisis for the Nigerian government.

In recent years, the United States has been working in partnership with the government of Nigeria to counter Boko Haram. The American government recognizes Boko Haram as a threat to its interests in Africa, and potentially to the homeland, resulting in the

[3] Jacob Zenn, "Leadership Analysis of Boko Haram and Ansaru in Nigeria," *CTC Sentinel* 7, no. 2 (24 February 2014): 1–9, https://www.ctc.usma.edu/posts/leadership-analysis-of-boko-haram-and-ansaru-in-nigeria.

Map 2. Boko Haram attacks (January 2010–March 2014)



Adapted from 2014 Reuters map by Marine Corps University Press.

State Department designating the group a foreign terrorist organization in November 2013.[4] America regards Nigeria as a key strategic partner because it is "Africa's most populous nation, its largest democracy, a significant contributor to peacekeeping efforts across the continent, [and] a crucial partner for economic growth, trade and direct investment with the United States."[5] As a senior government official stated, "Peace and security in Nigeria is one of our highest foreign policy priorities in Africa."[6]

[4] An organization must meet three criteria to be designated a foreign terrorist organization: (1) it must be a foreign organization; (2) it must engage in terrorist activity or retain the capability and intent to engage in terrorist activity or terrorism; and (3) its terrorist activity or terrorism must threaten the security of U.S. nationals or the national security (national defense, foreign relations, or the economic interests) of the United States. For more information and designated groups, see http://www.state.gov/j/ct/rls/other/des/123085.htm.

[5] U.S. Department of State, "Secretary Clinton Meets with Nigerian Foreign Minister Ajumogobia," *DIPNOTE* (blog), 5 August 2010, https://blogs.state.gov/stories/2010/08/05/secretary-clinton-meets-nigerian-foreign-minister-ajumogobia.

[6] *Boko Haram: The Growing Threat to Schoolgirls, Nigeria, and Beyond*, *Before the Committee on Foreign Affairs,* 113th Cong. 172 (21 May 2014) (statement of Sarah Sewall, under secretary for civilian security, democracy, and human rights), http://www.state.gov/j/226424.htm.

U.S. assistance to Nigeria increased after Boko Haram kidnapped 270 schoolgirls from the northeastern town of Chibok in April 2014.[7] In response, President Barack H. Obama "directed that the U.S. government do everything it can to help the Nigerian government find and free the abducted girls and, more broadly, combat Boko Haram in partnership with Nigeria, its neighbors, and other allies."[8] The president made clear that U.S. support would come in "many forms but the goal is singular: to dismantle this murderous group."[9]

Over the past decade, the United States acted extensively in partnership with foreign governments to counter militant extremist organizations across the globe. For example, America supported Iraq and Afghanistan in taking on insurgencies that continue to shake the stability of both countries. The United States continues to support the governments of Yemen, Pakistan, and the Philippines to quell violence and instability caused by terrorist groups in these countries. Unfortunately, this work has been difficult, taxing, and expensive, and it has not always paid off in ways the American government intended. Generally speaking, America's track record assisting other countries in their fights against militant and extremist groups is mixed: there have been some successes (such as in the Philippines and Colombia), but also real setbacks. Key determinants to success seem to be the quality of the counterinsurgent regime and its willingness to accept assistance employing a whole-of-government approach to address the conflict.

An Assessment of the Boko Haram Conflict

The conflict in northeast Nigeria is complex, driven by a mix of historical, political, economic, and ethnic antagonisms. Resolving it

[7] Aminu Abubakar and Josh Levs, " 'I Will Sell Them,' Boko Haram Leaders Says of Kidnapped Nigerian Girls," CNN News, 6 May 2014, http://www.cnn.com/2014/05/05/world/africa/nigeria-abducted-girls/.

[8] White House Office of the Press Secretary, "Fact Sheet: U.S. Efforts to Assist the Nigerian Government in Its Fight against Boko Haram," 14 October 2014, https://www.whitehouse.gov/the-press-office/2014/10/14/fact-sheet-us-efforts-assist-nigerian-government-its-fight-against-boko-.

[9] Ibid.

will require a deep understanding of conflict dynamics as well as the motivations and capabilities of various key actors. To date, few such comprehensive analyses of the Boko Haram conflict have been attempted. As a result, there is still some debate as to exactly what kind of conflict—insurgency, interethnic warfare, opportunistic criminality, or revolutionary terrorism—is actually taking place in northeast Nigeria. To develop an effective response to the threat posed by Boko Haram, the Nigerian government and its international partners must properly diagnose the conflict and comprehend it as an evolving system that can be affected through strategic interventions.

A conflict assessment was conducted to accurately diagnose the Boko Haram conflict.[10] This analytical process helped identify and explain the dynamics of violence and instability; informed the development of an independent, balanced view of the conflict; uncovered the crucial elements of the armed conflict; and assessed interactions among key actors. Planners can use the information to develop programs that effectively support partner nations' efforts to manage conflict. These conflict assessments help identify conflict sensitivity strategies to ensure assistance programs achieved intentional impacts.[11]

The conflict assessment framework was developed by combining relevant elements of existing analytical frameworks designed by various government agencies and academic scholars to dissect and understand internal conflicts, insurgency, and violent extremist organizations in Nigeria. The framework consists of the following elements:

1. Context—framing the conflict by mapping out longstanding conditions resistant to change; immutable facts on the ground; and historical narratives, including northern Africa's ethnoreligious schisms, fundamentalist and seces-

[10] Patricio Asfura-Heim and Julia McQuaid, *Diagnosing the Boko Haram Conflict: Grievances, Motivations, and Institutional Resilience in Northeast Nigeria* (Arlington, VA: CNA, 21 January 2015), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA613302.

[11] U.S. Agency for International Development (USAID), *Conflict Assessment Framework, Version 2.0* (Washington, DC: USAID and the Office of Conflict Management and Mitigation, June 2012), http://pdf.usaid.gov/pdf_docs/pnady739.pdf.

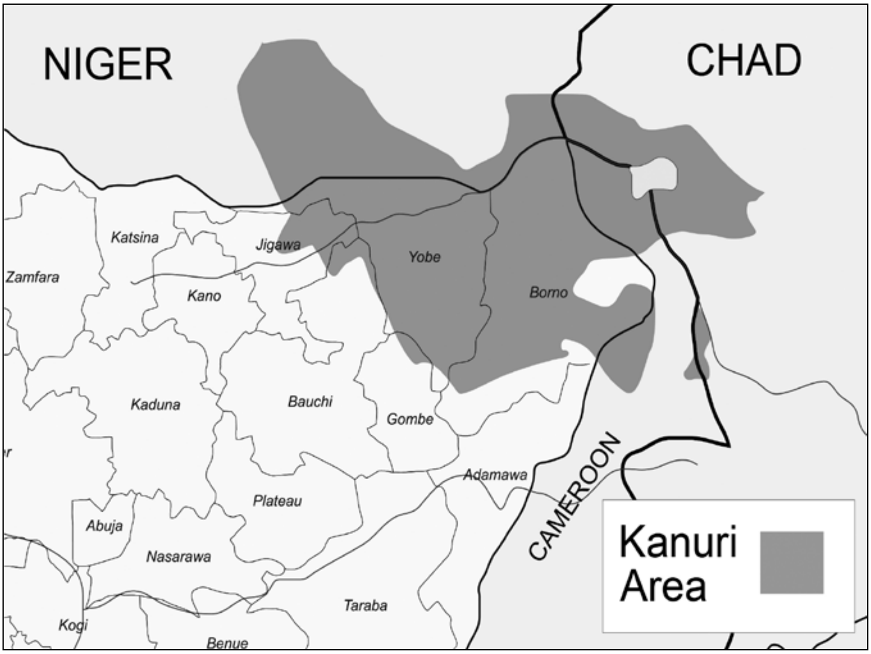
sionist tendencies, and economic transformation, as well as structural factors such as the political rules of the game.

2. Sources of tension and conflict drivers—identifying contemporary sources of tension contributing to Boko Haram's emergence and the conflict drivers sustaining the group. The examination includes specific national governance failures, political exclusion, institutionalized corruption, economic disenfranchisement, and persistent sectarian violence.
3. Institutional resilience—assessing institutions created to resolve state and social disputes through nonviolent means, including official state rule of law institutions and established northern religious leadership.
4. Key actors—supporting people and organizations influencing social patterns and institutional performance, shaping perceptions, mobilizing people, and providing means to other key actors. Specific examinations identify and assess motivations and grievances, interests, means and resources (including funding and recruitment), relations with other key players, strategies and tactics, capacity, and levels of public support for various parties to the conflict including the Boko Haram militant group, national governments, and important traditional leaders and civil society.
5. Conflict diagnosis—interpreting and categorizing the phase and nature of the conflict based on the crucial elements and recognized typologies from internal conflict, counterinsurgency (COIN), and counterterrorism (CT) literature.
6. Trajectory of the conflict—determining conflict trends and generating potential scenarios to direct effective assistance program responses.

Results of the Conflict Assessment

Our analysis concludes that *Boko Haram is a local, ethnic-based (Kanuri) revolutionary insurgency* using subversion, classic guerilla tactics,

Map 3. Kanuri areas in a four-border region: Nigeria, Niger, Chad, and Cameroon



Map courtesy of Michael Markowitz, CNA.

and terrorism to achieve its goals (see map 3).[12] Its fundamental objective is to replace the existing political order by overthrowing the secular Nigerian state and installing an Islamic government.[13] This movement is a product of local context and conditions and represents an extreme manifestation of local identity politics. It is motivated by a variety of social, political, and economic grievances and organized around a fundamentalist/rejectionist ideology sustained

[12] The Department of Defense defines insurgency as "the organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency can also refer to the group itself." *Dictionary of Military Terms*, Joint Publication 1-02 (Washington, DC: Department of Defense, 2015), 119. Insurgencies use such methods as guerrilla warfare, terrorism, coercion/intimidation, propaganda, subversion, and political mobilization.

[13] Some analysts argue that the conflict is merely a separatist insurgency intent on carving out an Islamic state in the north but does not in actuality have a national agenda. Others argue the group is simply a terrorist organization or a criminal syndicate. However, taken at face value, Boko Haram's communiqués and propaganda suggest larger objectives, which include the overthrow of the current regime.

by the Nigerian government's neglect and counterproductive security measures.[14]

Currently, Boko Haram is a destabilizing force, but not an existential threat to the Nigerian government or its security services. Because of extreme tactics, indiscriminant violence, and unpopular ideology, Boko Haram currently lacks grassroots support even though many northern Nigerians share its grievances, and its goals resonate with a large percentage of Nigerian Muslims.

Reports suggest that Boko Haram (unlike other insurgent groups, such as Afghanistan's Taliban) is attempting to carry out a politically organized insurgency, which by definition requires the development of complex political structures in tandem with military operations. Boko Haram does not appear to employ any form of "shadow governance" to control territory or attempt political mobilization of the population. Instead, Boko Haram imposes order by administering Sharia law in occupied towns and villages and relies exclusively on a military model to achieve its insurgent goals. Beginning in 2009 as an urban-cellular insurgency relying primarily on terrorism, Boko Haram has since morphed into a rural insurgency with guerilla tactics added to its repertoire.[15] This type of insurgency is what COIN scholar David Galula has termed the Bourgeois-Nationalist, or shortcut, pattern. It begins with sensational acts of terrorism to "get publicity for the movement . . . to attract latent supporters."[16] Today, Boko Haram uses enforcement terror to instill fear in wavering supporters and employs agitation terror against representatives of the government and those who support it.

[14] USAID, *Nigeria Cross-Sectoral Conflict Assessment* (Bethesda, MD: Democracy International, August 2014), http://www.usaid.gov/sites/default/files/documents/1866/Nigeria%20Cross-Sectoral%20Conflict%20Assessment%20Final%20Report.pdf.

[15] Guerrilla tactics are intended not only to wear down the government's conventional forces, but also to provoke them into conducting reprisals against the general population, which they rightly or wrongly perceive as aiding the insurgents.

[16] David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CT: Praeger Security International, 1964), 43. A digital version is available at http://louisville.edu/armyrotc/files/Galula%20David%20-%20Counterinsurgency%20Warfare.pdf. While this approach may save years of organizational and political work, it has a weakness: the terrorist group's tactics may backfire by losing any public support it could have hoped to gain.

At this stage in the conflict, Boko Haram's operational objective appears to be separating the Muslim population from the government by subverting northern elites and undermining government legitimacy. While the long-term strategy is difficult to discern, theoretically Boko Haram believes military successes in conjunction with weakening the functions and legitimacy of the government will cause the Muslim population to rally to its cause.

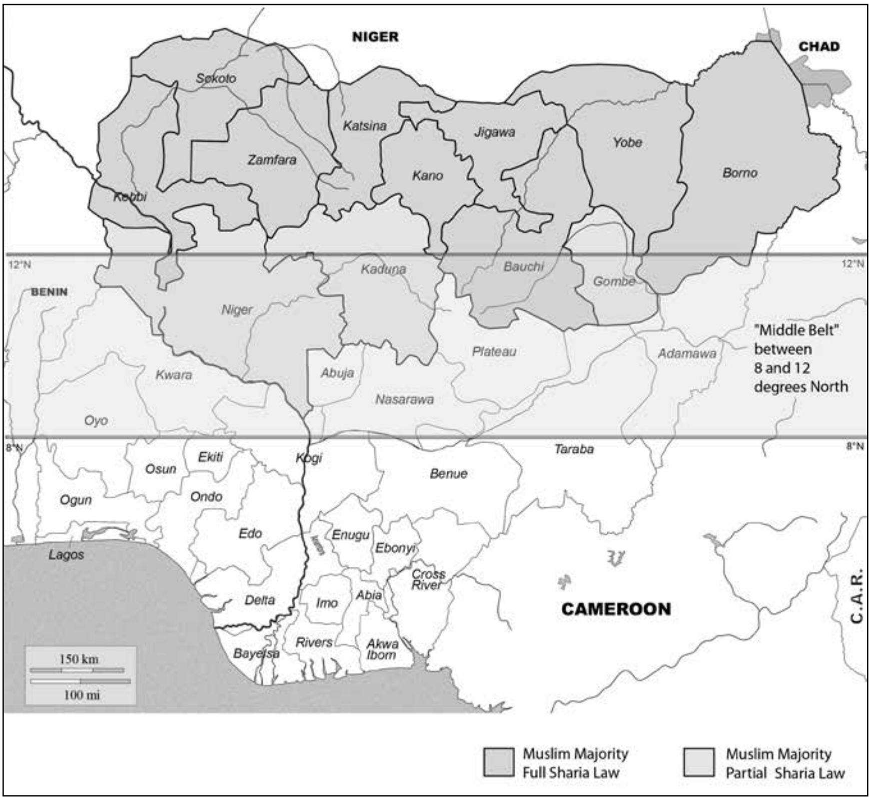
The causes and drivers of the conflict have been profoundly reshaped as the conflict has evolved. First and foremost, the grievances currently driving Boko Haram to achieve regime change relate to poor governance and north-south economic disparities. Underlying conditions—including large numbers of unemployed youth, strong Islamic fundamentalist/rejectionist currents in the northeast, ethnoreligious tensions, and competition over political power—ensure that Boko Haram can recruit enough new members to stay viable.

The Nigerian government's heavy-handed CT strategy perpetuates the conflict by paying little attention to underlying contextual realities and root causes. This approach further alienates the already disaffected northeastern communities, maintains the population's hesitancy to cooperate with security forces, and limits intelligence required for pinpoint, network-centric operations. Because the government is unable to conduct surgical strikes against the insurgents, operations often result in indiscriminate killings. Consequently, the pool of potential insurgent recruits expands, and the sense that the government is an equally liable party to the violence solidifies. Moreover, despite an increased military presence in the north, the government has been unable to protect the population from Boko Haram attacks and retaliatory raids, the insurgency retains considerable freedom of movement in the northeast, and the militants retain access to sanctuaries in the Kanuri-dominated areas of Chad, Niger, and Cameroon; all resulting in Nigeria's lost credibility.

Lastly, traditional leaders and civil society organizations contaminated by their relationships with the government or cowed by Boko Haram's murder and intimidation campaign weaken northeastern Nigeria's ability to mitigate the conflict, thereby prolonging hostilities. The lack of legitimacy of the Nigerian government as well as the fractured nature of the Islamic community in the north has had direct implications on Nigeria's nongovernmental actors' ability to counter Boko Haram's radical narrative.

Although inappropriate and ineffective responses to increased violence decreased the Nigerian government's legitimacy, Boko Haram failed to capitalize on it. The insurgency's extreme tactics and indiscriminant violence perpetuated by new leadership squandered the grassroots support it enjoyed before 2009. At least temporarily, even the backing of the most fundamentalist segments of Nigeria's Muslim population has been lost, although both share rejectionist, antistate sentiments (see map 4). Importantly, Boko Haram struggles to garner substantial external support (moral, political, technical, financial, or military) from other jihadi groups or foreign governments.

Map 4. Nigeria's Muslim majority



Map courtesy of Michael Markowitz, CNA.

At this time, it is unclear how the insurgency will be resolved. If a stalemate develops, Boko Haram could evolve into a criminal or terrorist organization with some factions negotiating truces with the government. If Boko Haram moderates its extremist tactics (potentially brought about by a change in leadership or the creation of a political front) to tap into the vast reserves of antigovernment sentiment and religious fundamentalism in the north, the conflict may expand and a secessionist Islamic Caliphate may be created. If Boko Haram sufficiently accelerates Nigeria's centrifugal forces (ethnoreligious divides, power politics, and economic grievances) to cause the state to collapse from within, a more ominous, if less likely, outcome could be the Somaliazation of Nigeria.

Divergent Approaches to Countering Boko Haram

Since Boko Haram is an insurgent group, an effective response to the group should follow the tenets of a traditional COIN approach. Determinants of this approach are illustrated by comparing Nigerian and American interactions and current and past government efforts relative to eight identified best practices.

Counterinsurgency Best Practices

Eight generic best practices provide a framework for effective COIN strategies for any government. Authorities should distribute resources, programs, activities, and other efforts appropriate to each of these best practices in the context of the specific conflict. Insurgencies differ from country to country and through time; therefore, each conflict's internal political, economic, and social dynamics greatly vary from one to the other. As a result, the appropriate blend of best practices will differ from conflict to conflict.

Table 1 identifies these best practices and describes the corresponding steps for governments investing in COIN and for other stakeholders.

Comparing Current Efforts to COIN Best Practices

The Nigerian and U.S. governments have both taken measures to counter Boko Haram. In this section, comparison of these efforts to

Table 1. COIN best practices

Best practice	Description
1. Devise a strategy built on an analytical conflict assessment	Devise a strategy rooted in a balanced assessment of the conflict, and identify programs, activities, and actions that address conflict drivers
2. Implement a coordinated whole-of-government approach	Pursue an integrated, multiagency approach drawing from and coordinating resources, expertise, and programs from across the spectrum of government functions, including military, diplomacy, and development*
3. Bolster government legitimacy	Focus on taking measures garnering the population's support for the government as the legitimate authority in power responsible for providing security and protecting citizens; practicing good governance; and using legitimacy to discredit the insurgency
4. Protect the population	Provide humanitarian support and employ local defense groups as appropriate
5. Address the root causes of the conflict	Identify, assess, and take measures to ameliorate the political, economic, and social conditions contributing to the rise and perpetuation of the insurgency
6. Attack the insurgent network	Employ kinetic (military, law enforcement) and nonkinetic (intelligence, technological) assets to physically dismantle the insurgency's infrastructure and target its leadership and membership
7. Cut off support and eliminate sanctuaries	Cut off internal and external support to the insurgency group, including financial, logistical, ideological, and physical sanctuary
8. Pursue opportunities to reach a settlement to the conflict	Identify and devise a political plan agreed upon by all stakeholders to settle differences, including negotiations, concessions, incentives, settlements, amnesty, and ceasefires

* Jim Garamone, "New National Strategy Takes 'Whole-of-Government' Approach," American Forces Press Service, 27 May 2010, http://www.defense.gov/news/newsarticle.aspx?id=59377.

the COIN best practices explain which elements have been implemented and to what degree.

Best Practice 1: Devise a Strategy Built on an Analytically Derived Conflict Assessment

To be successful, the government needs to articulate a COIN strategy based on an accurate diagnosis of the conflict. The strategy should direct activities, programs, and resources at the same objectives for the conflict and on matching timelines. Otherwise, efforts risk being misdirected, inappropriate for the goals, overlapping, or unnecessary altogether. The same is true for supporting partners.

Nigeria. Under the administration of President Goodluck Jonathan, Nigeria's approach to the Boko Haram conflict has not been clearly articulated in an overarching or comprehensive strategy with stated objectives or timelines. The approach to date primarily consists of reactive efforts, haphazardly carried out by various government entities involved in the conflict. The little strategy detected in the government's rhetoric resembles more of a CT strategy than a COIN strategy. Officials propagate the notion of Boko Haram as a terrorist organization with links to global terrorist networks operating in Nigeria; however, there is no public recognition that the conflict results from conditions and grievances originating in Nigeria.

In May 2014, the Chief of Defense Staff Air Chief Marshal Alex Badeh declared that Nigeria was "at war with the international terror organisation, al-Qaeda, in North and West Africa, and not Boko Haram."[17] Similarly, a Maiduguri military base spokesman noted, "Here they call it Boko Haram, but Boko Haram is totally al-Qaeda. The name does not matter. The characteristics are the same. All the terrorists are in one group. They have one activity, one [way of] thinking. Al-Qaeda has no boundary. There are perfect

[17] Gbade Ogunwale, "We Are Fighting Al-Qaeda, Not Boko Haram, Says CDS," *Nation*, 29 May 2014, http://thenationonlineng.net/new/fighting-al-qaeda-boko-haram-says-cds/.

links. It's exactly the same as al-Qaeda."[18] These notions contribute to Nigeria's narrow CT approach that might be appropriate for countering an al-Qaeda branch operating in Nigeria, but not for a full-blown insurgency.

Some Nigerian government officials depict Boko Haram as merely the most recent manifestation of a long history of militant groups in Nigeria with antigovernment agendas. This perspective downplays the threat, pointing to the fact that the violence has been confined to the northeast and has not affected most of Nigeria's 180 million people.

United States. As a supporting partner, America pursues Boko Haram within the context of its relationship with Nigeria. Countering Boko Haram's intensified hostility, the United States expanded the range of program activities specifically addressing the conflict. The strategy continues to evolve in response to the conflict and potential threats to U.S. interests in Nigeria.

Best Practice 2: Implement a Coordinated Whole-of-Government Approach

Complex political, social, and economic dynamics within a country initiate and perpetuate insurgencies. Therefore, affected governments must devise a whole-of-government approach to select and coordinate government agencies and activities effective for the range of dynamics at play across diplomatic, economic, development, intelligence, and law enforcement functions.

Nigeria. Nigeria's primary employment of state security, military, and law enforcement over other agencies in response to the conflict in the northeast demonstrates a narrow CT approach contrary to a whole-of-government strategy. Nigeria, like many of its African neighbors, is a relatively young nation still developing state institutions. Likewise, the typical response to challenges of authority from internal, armed groups is to employ the instruments of state power to regain control and restore law and order through the use of

[18] Alex Perry, "Boko Haram: Terror's Insidious New Face," *Newsweek,* 4 July 2014, http://www.newsweek.com/2014/07/18/boko-haram-terrors-insidious-new-face-257935.html.

force.[19] Historically, armed forces are at the forefront during periods when law and order have broken down; in past conflicts similar to the Boko Haram conflict, the Nigerian government sent in military forces to restore normalcy.[20]

What little government coordination has taken place exists mainly within a joint task force (JTF), a model that the Nigerian government uses to coordinate military and police activities in response to internal crises or conflicts. Specifically, the JTF includes elements from "the Nigerian Army, the Nigerian Police Force, the State Security Service, the Air Force, and a host of security intelligence units."[21] While the JTF model has served, at least theoretically, as a coordinating mechanism, it has only drawn from the military and security assets of the state and not integrated other government functions required to end the conflict.

In March 2014, official rhetoric concerning response to the conflict shifted. National Security Adviser Colonel Sambo Dasuki announced that Nigeria would pursue a soft approach strategy to the situation, including far reaching socioeconomic programs in the north to improve education in affected areas, reduce extreme poverty, and improve relations between various religious elements. As of February 2015, there was little evidence of Nigeria implementing this soft approach.

The administration of Nigerian President Jonathan focused heavily on winning the 2015 election. During his time in office, Jonathan personally displayed a generally tepid reaction toward the northeast, even in the aftermath of the Chibok kidnappings. By sending in the military during negotiations with Boko Haram, he directed national

[19] LtCol Ko Ukandu, "The Whole-of-Government Approach to Managing Internal Security Threat in Nigeria," Ahmadu Bello University, 2014, http://www.academia.edu/6239934/THE_WHOLE_OF_GOVERNMENT_Final_corrected_VERSION_2.

[20] Ibid. In the 1990s, Nigeria used a military approach to crush the Maitatsine Movement, an Islamist movement in Nigeria that is in some ways considered a precursor to Boko Haram. Its success may have left the erroneous impression that the government could use the same approach and achieve the same outcome with Boko Haram years later.

[21] Victoria Ibezim-Ohaeri, "Opinion: Disbanding the JTF in the North-East Was a Grave Mistake," *YNaija*, 10 March 2014, http://ynaija.com/opinion-disbanding-the-jtf-in-the-north-east-was-a-grave-mistake/.

attention and resources in a way that seemed to allow him to take credit for something while actually achieving little.[22]

United States. State Department official Robert P. Jackson described the United States' "multifaceted" assistance to Nigeria as congruent with a whole-of-government approach to Boko Haram.[23] Similarly, President Obama stated that the "war against Boko Haram requires [a] holistic approach."[24] In this vein, the United States pursued the following efforts to counter Boko Haram:

- Diplomacy—the U.S. government consistently sends the message that success requires a whole-of-government approach to the Boko Haram conflict in that "the fight against Boko Haram requires more than just military action, it requires a comprehensive approach to improving the lives of people in Northeast Nigeria."[25]
- Military support—while there are limitations, the United States provided training, equipment, and advisement to the Nigerian military in its fight against Boko Haram, with a focus on professionalism and human rights practices.
- Law enforcement—the American government provided investigation, forensic, and negotiation support to the Nigerian police forces.
- Intelligence—the United States trained and advised Nigeria on intelligence practices as well as explored ways to share information respective of the conflict's dynamics.
- Development—the U.S. government focused on improving governance in Nigeria while continuing long-term invest-

[22] Jonathan failed to maintain popular support and lost to Muhammadu Buhari. See Aislinn Laing, "Nigeria's President Goodluck Jonathan Hands over to Former Dictator Muhammadu Buhari," *Telegraph*, 29 May 2015, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/nigeria/11637544/Nigerias-president-Goodluck-Jonathan-to-hand-over-to-former-dictator-Muhammadu-Buhari.html.
[23] Representative Karen Bass, "Africa Policy Breakfast: Instability in Northern Nigeria and the Ongoing Threat of Boko Haram," video on Web site, from a meeting held on 10 July 2014 in Washington, DC, 1:59, http://bass.house.gov/nigeriamatters.
[24] Abiodun Oluwarotimi, "Obama–War Against Boko Haram Requires Holistic Approach," *allAfrica*, 15 May 2014, http://allafrica.com/stories/201405151415.html.
[25] *Boko Haram: The Growing Threat to Schoolgirls.*

ments in programs to improve education, health, gender issues, and other development issues in conflict affected areas.

- Humanitarian aid—the United States provided humanitarian assistance to populations in the northeast.
- Countering violent extremism (CVE)—the American government worked to improve governance for communities vulnerable to Boko Haram recruitment and devised ways to counter radical narratives.[26]

When the Nigerian government requested U.S. assistance in the aftermath of the Chibok kidnappings, the level of American involvement in the Boko Haram conflict spiked. The United States deployed a multiagency team of 16 experts who focused on assisting Nigeria in five areas: intelligence, law enforcement, humanitarian aid, diplomacy, and development. Support for the effort included sharing specific intelligence, surveillance, and reconnaissance information about the abducted girls, training Nigerian security forces, augmenting U.S. embassy personnel, facilitating strategic communications, and preventing future incidents.[27]

Best Practice 3: Bolster Government Legitimacy

In any uprising, the government competes with the insurgency for the support of the local population. To prevail, the affected government must foster a sense of trust that *it* is the legitimate authority in power over the insurgent group. In broad terms, practicing good governance, adhering to the rules of law, remaining responsive to the needs of the people, and generally demonstrating that the state has the population's protection and interests at heart all contribute to government legitimacy. Governments can bolster their legitimacy by establishing that they will defeat the insurgent group and restore order in a way that does not result in greater misery or harm for

[26] U.S. Department of State, *Boko Haram and U.S. Counterterrorism Assistance to Nigeria* (Washington, DC: U.S. Department of State, 14 May 2014), http://www.humanrights.gov/fact-sheet-boko-haram-and-u.s.-counterterrorism-assistance-to-nigeria.

[27] White House, "Fact Sheet: U.S. Efforts to Assist."

populations living in the conflict areas. Government actions that fail to protect people—or worse, that cause them harm—erode state legitimacy.

Nigeria. Five years into Nigeria's efforts countering Boko Haram, many people in the northeast are deeply suspicious of the state. They do not trust the government's intentions or its ability to defeat Boko Haram. Nigeria's actions have failed to bolster any level of government legitimacy in the eyes of the local population even though Boko Haram does not enjoy popular support either. In fact, although the group's grievances may resonate with the average person living in northeast Nigeria, those in the affected areas generally revile the group due to its harsh, inhuman tactics.

Many of Nigeria's actions not only undermined its legitimacy, they also drove the conflict by serving as a useful tool for Boko Haram's recruitment efforts. Many examples illustrate this dynamic, such as the 2009 summary execution of the group's first leader Mohammed Yusuf while in Nigerian police custody.[28] The military JTF, which is intended to be Nigeria's primary asset in defeating Boko Haram, has failed to crush the group while sowing mistrust and doubt within the population. Locals accuse it of operating like an army of occupation. Unable to distinguish Boko Haram members from innocent civilians, the JTF resorts to arbitrary dragnet arrests, collective punishments, illegal detentions, and, in some instances, extra-judicial killings. Nigeria's endemic corruption has eroded the population's confidence and trust in the political leadership at *any* level of government.

United States. When competing with an insurgency, the government is ultimately the only actor that can establish legitimacy in the eyes of its population through its decisions and actions. As a supporting partner, the United States assisted Nigeria's efforts to improve governance and reform elements that theoretically bolster state legitimacy in the eyes of the people. However, the results of this strategy depend on the people's perceptions of Nigeria's sincerity and program implementation.

[28] Ibid.

The USAID led U.S. programs in Nigeria striving to foster good governance, address corruption, and provide human rights training.

> USAID supports responsive governance at state and local levels, enhanced credibility for elections, and increased capacity for civic engagement. USAID builds capacity in key government agencies to strengthen fiscal responsibilities and improve transparency. In addition, USAID advances the rule of law by strengthening the capacity and transparency of the justice system and increasing judicial independence at the federal level.[29]

In addition, the American government relies on a variety of diplomatic channels to encourage reform and improve governance across all levels of government. For example, launched in 2010, the Regional Security Working Group of the U.S.-Nigeria Bi-National Commission aims to support Nigeria's efforts to increase public confidence in the military and policymakers' effectiveness responding to the extremist threat.[30] The United States also involves the Nigerian embassy in Abuja regarding these assistance programs.

Best Practice 4: Protect the Population

Protecting the population from the violence perpetrated by insurgent groups is a key factor in an effective COIN approach. The state theoretically monopolizes force; therefore, an inability to protect the population undermines the legitimacy of the state. Furthermore, the government engaged in COIN needs to respond to the humanitarian needs (shelter, food, medical care, etc.) of the population affected by the conflict. Beyond issues of morality, failing to meet the basic needs of local populations creates potentially desperate situations that could drive civilians into the hands of the insurgency. For similar reasons, it is critical that governments threatened by an insurgen-

[29] USAID, "Democracy, Human Rights, and Governance Nigeria," 2 December 2014, http://www.usaid.gov/nigeria/democracy-human-rights-and-governance.

[30] See Lauren Ploch Blanchard, *Nigeria's Boko Haram: Frequently Asked Questions* (Washington, DC: Congressional Research Service), 10 June 2014, http://fas.org/sgp/crs/row/R43558.pdf; and the United States Diplomatic Mission to Nigeria, "U.S.-Nigeria Bi-National Commission," http://nigeria.usembassy.gov/us-nigeria-bnc.html.

cy use kinetic force carefully and discriminately to avoid killing or harming innocent people.

Nigeria. The Nigerian Army and its security forces have not provided protection to the local population during the conflict. Boko Haram's near-daily acts of violence, such as attacks by gunmen, kidnappings for ransom, burning of public buildings, and bombings, perpetuate a constant state of public insecurity.[31] Nigerians accuse security forces of executing men in front of their families; arresting and beating people who have not been charged; and burning houses, shops, and cars.[32] Economic activity and income-earning activities have slowed to a halt, curfews and movement restrictions have been violently enforced as part of the state of emergency, and people have been driven to leave their homes and villages by the sense of crippling fear—all disrupting "normal productive agricultural and commercial activities."[33] Boko Haram and Nigerian security forces and military personnel rampantly and persistently violated human rights. As a result, the conflict in northern Nigeria displaced at least 3.3 million people as of October 2014.[34] At least 11,000 people on all sides of the insurgency have died since July 2009.[35] This number may actually be considerably higher since the data on casualties are not well tracked or reported.

Recently, the Nigerian Army tried to make up for its inability to improve the safety of civilians by endorsing civilian JTFs, which are militias and self-defense groups mobilized against Boko Haram. In Borno State, these groups work with state security forces to protect

[31] Al Chukwuma Okoli and Philip Iortyer, "Terrorism and Humanitarian Crisis in Nigeria: Insights from Boko Haram Insurgency," *Global Journal of Human-Social Science* 14, no. 1 (2014): 38–49, https://globaljournals.org/GJHSS_Volume14/6-Terrorism-and-Humanitarian-Crisis-in-Nigeria.pdf.

[32] Ibid.

[33] Ibid., 44.

[34] European Commission, *ECHO Factsheet: Nigeria* (Brussels: Humanitarian Aid and Civil Protection, 3 November 2014), http://ec.europa.eu/echo/files/aid/countries/factsheets/nigeria_en.pdf.

[35] Nathaniel Allen, Peter M. Lewis, and Hilary Matfess, "The Boko Haram Insurgency, by the Numbers," *Monkey Cage* (blog), *Washington Post,* 6 October 2014, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/10/06/the-boko-haram-insurgency-by-the-numbers/.

their neighborhoods and villages and reduce instances of collateral damage and civilian deaths during military operations.[36] Media reports suggest that these groups have had some success improving security in the capital city of Maiduguri, in spite of increasing violence in June after the president was sworn in and headquartered his forces there.

From a humanitarian perspective, conditions have severely deteriorated in the northeast since 2009. The ongoing state of emergency declared in 2013 in the states of Yobe, Borno, and Adamawa hampered the ability of aid organizations to meet the greatest humanitarian needs. Aid organizations report that the conflict has resulted in one of the grimmest humanitarian crises in Nigerian history. Instead of remedying the humanitarian situation over the course of the conflict, the government of Nigeria allowed the situation to continue to deteriorate.

In May 2014, the Nigerian National Emergency Management Agency (NEMA) began providing limited humanitarian relief in the form of emergency relief items, medical supplies, food, and other assistance to internally displaced persons (IDPs). Leading the humanitarian response in Chibok, the agency furnished medical support to the families and girls who have escaped[37] and constructed approximately 20 IDP camps across the three states.[38] The Borno state government dedicated $150 million to a rehabilitation program for individuals who have escaped from Boko Haram captivity.[39] In partnership with the United States, the Nigerian government set up programs to provide medical and psychiatric support to the most affected populations, focusing on Maiduguri.[40]

United States. The United States, via USAID and its implementing partners, has been providing a wide range of humanitarian relief in

[36] Blanchard, *Nigeria's Boko Haram*.
[37] United Nations, *Humanitarian Bulletin for Nigeria* (Geneva: Office for the Coordination of Humanitarian Affairs, 4 December 2014), http://reliefweb.int/sites/reliefweb.int/files/resources/Nigeria%20Humanitarian%20Bulletin%20April%202015.pdf.
[38] Michael Olugbode, "NEMA—We Have Registered 700,000 IDPs in Borno, Yobe and Adamawa," *allAfrica*, 20 November 2014, http://allafrica.com/stories/201411200437.html.
[39] United Nations, *Humanitarian Bulletin for Nigeria*.
[40] Ibid.

northern Nigeria to increase education for women, provide food aid, deliver health services (including vaccinations), and offer support for IDPs and refugees in Cameroon.[41] As of July 2014, $10.7 million in U.S. humanitarian assistance to "vulnerable and conflict-affected households in Nigeria" had been distributed as follows:[42]

- Water, sanitation, and hygiene (17 percent)
- Economic recovery and market systems (18 percent)
- Health (5 percent)
- Humanitarian coordination and information management (11 percent)
- Logistics and relief commodities (18 percent)
- Agriculture and food security (5 percent)
- Protection (26 percent)

Best Practice 5: Address the Root Causes of the Conflict

Most insurgencies at least partly arise from (and are eventually fueled by) realities that place some portion of a population at a distinct disadvantage from others. Examples of such realities include political marginalization, unfair distribution of resources and infrastructure, and social (e.g., religious, ethnic) discrimination. In an insurgency, these conditions play into the hands of the insurgents, who then may attempt to supplant the government by addressing these conditions and pointing to the government's failure to do so, which can be used as a powerful tool for recruitment. For any COIN effort to be successful, such imbalances and perceived injustices must be addressed.

Nigeria. The Nigerian government has not addressed the multitude of well-known, proximate sources of tension and drivers of conflict that directly contributed to the emergence and sustainment of extremist militant groups such as Boko Haram in northeast Nigeria.

[41] *Congressional Budget Justification: Foreign Operations, Appendix 3: Regional Perspectives, FY 2015* (Washington, DC: U.S. Department of State, 14 June 2012), http://www.state.gov/documents/organization/224070.pdf.

[42] *Nigeria–Complex Emergency, Fact Sheet #1* (Bethesda, MD: USAID, 30 July 2014), http://photos.state.gov/libraries/usun-rome/164264/PDF/NigeriaFS01.pdf.

These contemporary tensions and drivers promote an environment in which these violent groups easily gain sympathy for their causes and recruit new members. Three of the most egregious sources of conflict-related tension that Nigeria has failed to address are as follows:

1. *Economic disparities between the north and the rest of the country.* Seventy-two percent of northerners live in poverty compared to 27 percent of southerners and 35 percent in the Niger Delta.[43] Northern Nigeria's gross domestic product is approximately twice as much as the south's.[44] Poverty and lack of services affecting the northern Muslim population caused intense resentment of the political status quo and fueled extremist and rejectionist thinking.[45] Nigeria has not implemented broad-based efforts addressing the deep socioeconomic disparities between the north and the south, begun major infrastructure improvement projects, or improved programs to meet the social service needs of the local population.

2. *Endemic corruption among political and economic elites and extensive poor governance.* Nigeria consistently ranks as one of the most corrupt countries in the world,[46] touching aspects of political and economic life across the country. However, venality is particularly acute in the northeast where there are few legitimate pathways to wealth. Accusations of government officials' complicity in the conflict

[43] Mohammed Aly Sergie and Toni Johnson, *CFR Backgrounders: Boko Haram* (New York: Council on Foreign Relations, 7 October 2014), http://www.cfr.org/nigeria/boko-haram/p25739. Since this article was written, the content on this page was updated on 5 March 2015.

[44] Forest, *Confronting the Terrorism of Boko Haram*.

[45] Lauren Ploch, *Nigeria: Current Issues and U.S. Policy* (Washington, DC: Congressional Research Service), 24 April 2013, https://www.fas.org/sgp/crs/row/RL33964.pdf; and Akinola Olojo, *Nigeria's Troubled North: Interrogating the Drivers of Public Support for Boko Haram* (The Hague: International Centre for Counter-Terrorism, October 2013), http://www.icct.nl/download/file/ICCT-Olojo-Nigerias-Troubled-North-October-2013.pdf.

[46] International Crisis Group, *Curbing Violence in Nigeria (II): The Boko Haram Insurgency*, Africa Report No. 216 (Brussels: International Crisis Group, 3 April 2014), http://www.crisisgroup.org/en/regions/africa/west-africa/nigeria/216-curbing-violence-in-nigeria-ii-the-boko-haram-insurgency.aspx.

are rampant as people claim that individuals in positions of power are accepting payments from Boko Haram.[47] Local influential clerics in the north have been accused of taking bribes from the group, not only out of personal financial interests but also to avoid being attacked by the insurgency or to guarantee a position of power in the event that Boko Haram comes to power in the region.[48] In 2002, Nigeria stood up the Economic and Financial Crimes Commission to investigate financial crimes, including those by the government, but it is frequently criticized and described as ineffective.

3. *Perceived deterioration of the "zone" power-sharing arrangement.* Nigeria has long struggled to govern a nation in which numerous ethnoreligious factions compete for political power. Since the election of President Olusegun Obasanjo in 1999, there has been a power-sharing arrangement between the country's six ethnoregional zones. The 2010 death of the Muslim president Umaru Yar'Adua, who was only two years into his four-year term, and the ascension of his vice president, Goodluck Jonathan, a Christian from the southern Niger Delta, raised questions about the future of the zone power-sharing arrangement. Many northerners viewed the Jonathan administration as illegitimate, arguing that he ignored an informal power-rotation agreement that should have kept a Muslim as president through the next election cycle.

United States. The U.S. interagency approach reflects an understanding of the complex social, economic, and political drivers of the conflict in northeast Nigeria. As such, State Department and USAID

[47] Chantal Uwimana and Leah Wawro, "Corruption in Nigeria's Military and Security Forces: A Weapon in Boko Haram's Hands–Transparency International," *Sahara Reporters*, 19 June 2014, http://saharareporters.com/2014/06/19/corruption-nigerias-military-and-security-forces-weapon-boko-haram%E2%80%99s-hands-transparency.

[48] "Nigerian Muslim Clerics Recruiting, Gov't Officials Take Bribes from Boko Haram," *Talk of Naija*, 26 April 2014, http://www.talkofnaija.com/local/nigerian-muslim-clerics-recruiting-gov-t-officials-take-bribes-from-boko-haram-us-military-report-details.

programs seek to improve civil society, governance, education, and economic development in Nigeria. In particular, USAID has focused heavily on increasing education in northern states. According to testimony by the USAID assistant administrator for Africa, "Education programs [implemented] in the North [have] increased access to basic education services for over 15,000 orphans and vulnerable children, strengthened the capacity of 24 education-related non-governmental organizations to responsibly manage their finances, and influenced Nigeria's Educational Research and Development Council to include reading as a part of the education curriculum."[49]

Economic growth and poverty alleviation programs have been a priority. State Department programs therefore targeted the agricultural, power, and petroleum sectors. Similarly, USAID focused on "build[ing] the capacity of export firms; help[ing] medium-sized, small, and micro enterprises gain access to loans; and support[ing] the development of a new customs and excise management act to reform and modernize the Nigerian customs service."[50]

Beyond education and poverty, USAID programs address the conflict through civil society and governance issues to build transparency. The agency's conflict mitigation program "reconstituted and trained Conflict Management and Mitigation Regional Councils, and carried out phone-in interfaith dialogues."[51] The USAID has been working most actively in the northern states. For example, USAID "helped the Sokoto and Bauchi State Houses of Assembly pass public procurement and fiscal responsibility laws, trained over 900 government officials in public procurement and financial management practices, and assisted with the passing of the federal freedom of information act and its adoption at the state levels."[52]

[49] *#BringBackOurGirls: Addressing the Growing Threat of Boko Haram*, *Before the Senate Subcommittee on African Affairs* (15 May 2014) (statement of Earl W. Gast, assistant administrator for African affairs of USAID), http://www.usaid.gov/news-information/congressional-testimony/may-15-2014-earl-gast-aa-africa-bringbackourgirls-nigeria-boko-haram. See also the testimony available from the U.S. Senate Committee on Foreign Relations at http://www.foreign.senate.gov/download/gast-testimony-05-15-14.

[50] Ibid.

[51] Ibid.

[52] Ibid.

Lastly, U.S. programs to counter violent extremism in Nigeria aim "to limit recruits to [Boko Haram] by reducing sympathy and support for its operations through three primary objectives: (1) building resilience among communities most at risk of recruitment and radicalization to violence; (2) countering [Boko Haram] narratives and messaging; and (3) building the CVE capacity of government and civil society."[53]

Best Practice 6: Attack the Insurgent Network

COIN approaches that attack and dismantle the insurgent network employ the military, security forces, and law enforcement to physically weaken and ultimately destroy an insurgency's ability to operate effectively. Attacking the network, however, must be done in such a way that limits the consequences for the local civilian population and infrastructure. Additionally, this approach must be a single piece of a broader strategy that coalesces civilian elements of the state. A COIN government's military, security forces, and law enforcement hold an undeniably important role; however, the use of force should be precise, and military operations should be effectively executed to maximize insurgent losses while limiting civilian losses.

Nigeria. Nigeria's response to the Boko Haram conflict has been severe, emphasizing kinetic tactics and narrowly focusing on eradicating the group through violence, arrests, detentions, interrogations, and other harsh tactics. On paper, "With 200,000 troops and 300,000 paramilitary personnel, Nigeria's military is large enough to fight [Boko Haram]."[54] Yet, despite years of deploying military forces to the conflict, the number of Boko Haram's attacks and casualties has grown significantly over time. An estimate of nearly 4,000

[53] U.S. Department of State, *Boko Haram and U.S. Counterterrorism Assistance to Nigeria.*

[54] International Institute for Strategic Studies, *The Military Balance: The Annual Assessment of Global Military Capabilities and Defence Economics* (London: Routledge, 2007), 286, http://www.iiss.org/en/publications/military-s-balance, quoted in Mariah V. Barber et al., "U.S. Foreign Policy & Conflict Resolution: Fostering Regional Stability," *Public Policy & International Affairs Fellowship: Junior Summer Institute 2014* (New Jersey: Princeton University), 14, http://wws.princeton.edu/sites/default/files/content/Fostering%20Regional%20Stability%20IR%20Final%20Report.pdf.

dead since January 2014[55] serves as one of many indications that the group's operational capabilities have not been weakened.[56] Numerous factors contribute to the Nigerian Army's lack of success. Specifically, it

- is not prepared (trained or equipped) for counterinsurgency;
- lacks human intelligence needed to execute successful operations against the group;
- lacks airlift capacity;
- suffers from very low morale;
- suffers from corruption, in general, and in the procurement of military equipment, in particular;
- suffers from deep mistrust among the population; and
- engages in human rights abuses.

Nigeria's overly militaristic approach has many risks, including the possibility of failing to weaken the insurgent group and eroding progress in other COIN areas, particularly protecting the local population, bolstering government legitimacy, and addressing the root causes of the insurgency. The Nigerian government's hard-line approach fuels recruitment as well as passive support for Boko Haram among civilian victims of state-perpetrated violence.

Despite Nigeria's poor record of defeating Boko Haram militarily, it has taken several encouraging steps recently, including efforts to establish a regional security arrangement with its neighbors of Chad, Cameroon, and Niger.

United States. U.S. support of Nigeria's efforts to defeat Boko Haram militarily includes a range of bilateral and multilateral security assistance, training, equipment, and exercise activities. Compared to that of other West African countries, "U.S. security assistance to Nigeria is sizeable . . . totaling almost $20 million in FY2012 State

[55] Interview with U.S. government official, October 2014.

[56] Erin Conway-Smith, "Since #BringBackOurGirls, Boko Haram Has Only Gotten Stronger," *Global Post,* 10 November 2014, http://www.globalpost.com/dispatch/news/regions/africa/141110/despite-the-international-outrage-boko-haram-getting-stronger.

Department funding, and $16 million in FY2013."[57] The following programs are addressed:

- counterterrorism
- military professionalism and human rights
- border security
- training
- equipment
- law enforcement
- improvised explosive devices
- regional cooperation
- intelligence and reconnaissance
- strategic communications

In response to Nigeria's request for assistance following the Chibok kidnappings, the United States deployed an interagency team to provide military and law enforcement assistance as well as intelligence, surveillance, and reconnaissance support.[58] As part of this effort, U.S. Special Operations Forces began training a newly established 650-person ranger battalion in Nigeria to fight against Boko Haram. This action differs from previous training that prepared Nigerian units for peacekeeping missions.[59] In addition, the U.S. embassy in Nigeria provides ongoing COIN and humanitarian assistance training.[60]

[57] *Human Rights Vetting: Nigeria and Beyond*, *Before the Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations*, 113th Cong. 196 (10 July 2014) (statement of Lauren Ploch Blanchard, specialist in African affairs at the Congressional Research Service), 11, http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg88627/html/CHRG-113hhrg88627.htm.

[58] *#BringBackOurGirls*.

[59] Paul McLeary, "U.S. Sending Team of Combat Trainers to Nigeria," *Defense News*, 9 May 2014, http://www.defensenews.com/article/20140509/DEFREG04/305090021/US-Sending-Team-Combat-Trainers-Nigeria.

[60] *The Ongoing Struggle Against Boko Haram*, *Before the House Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations*, 113th Cong. 220 (11 June 2014), http://foreignaffairs.house.gov/hearing/subcommittee-hearing-ongoing-struggle-against-boko-haram.

The American government provided assistance to multiple Nigerian security forces, including the Nigerian Army, the Nigerian Police Force, the Nigerian Navy's Special Boat Service, and the Nigerian State Security Service. The United States worked with Nigerian law enforcement and border security forces and "established a $40 million Global Security Contingency Fund for Cameroon, Chad, Niger, and Nigeria to fight Boko Haram."[61] In addition, in August 2014, following the U.S.-Africa Summit in Washington, DC, the White House announced that Nigeria would be part of "the Security Governance Initiative (SGI), a new joint endeavor between the United States and six African partners that offers a comprehensive approach to improving security sector governance and capacity to address threats."[62]

Several factors have limited the scope and scale of U.S. military assistance to Nigeria to counter Boko Haram. First, documented human rights violations against the Nigerian armed forces conflict with U.S. laws established to prevent empowering units known for abuse. These two U.S. laws, collectively referred to as the "Leahy Law," require units in countries known to commit human rights abuses to be vetted through a Department of Defense and State Department process before receiving U.S. training and equipment.[63] Second, the Nigerian Army has a history of struggling to maintain and operate procured equipment, and the U.S. government does not want to provide Nigeria with equipment it cannot operate, maintain, or use appropriately. Third, Boko Haram routinely steals equipment

[61] Siobhan O'Grady, "Is Goodluck Jonathan Trying to Get Re-elected by Blaming Uncle Sam for Boko Haram?" *Foreign Policy*, 12 November 2014, http://foreignpolicy.com/2014/11/12/is-goodluck-jonathan-trying-to-get-re-elected-by-blaming-uncle-sam-for-boko-haram/.

[62] White House Office of the Press Secretary, "Fact Sheet: Security Governance Initiative," 6 August 2014, http://www.whitehouse.gov/the-press-office/2014/08/06/fact-sheet-security-governance-initiative.

[63] The Leahy Law (or Amendment) prohibits the United States from providing military training and equipment to foreign military forces that have committed human rights abuses. As part of the law, units must be vetted and, if found to be "clean," they are eligible for assistance. The American government has been unable to work with Nigerian units in the past because they failed the vetting process. See U.S. Department of State, "Leahy Vetting: Law, Policy, Process," 15 April 2013, http://www.humanrights.gov/wp-content/uploads/2011/10/leahy-vetting-law-policy-and-process.pdf.

from Nigerian armed forces, and the United States wants to avoid inadvertently providing equipment to the insurgency.

These factors breed U.S.-Nigerian tension and U.S. hesitancy to provide security assistance. In 2014, for example, the Nigerian ambassador to the United States publicly "castigated Washington for refusing to sell . . . [Nigeria] lethal equipment that would have brought down the terrorists within a short time."[64] According to the State Department, however, "The only denial was the transfer of some Cobra attack helicopters to Nigeria 'due to concerns about Nigeria's ability to use and maintain this type of helicopter in its effort against Boko Haram and ongoing concerns about the Nigerian military's protection of civilians when conducting military operations.'"[65] Conversely, in early December 2014, Nigeria requested a cessation of U.S. training for the 143-person Ranger unit while government officials attempted to confirm the third planned round of training.[66]

Best Practice 7: Cut Off Support and Eliminate Sanctuaries

To defeat an insurgency, the COIN government must cut off support to the group as part of its broader effort. An uprising typically receives support (either directly or indirectly) from other actors, such as criminal groups, corrupt government officials, foreign governments, other insurgent or terrorist organizations, and the local population. Support can come in many forms, including physical support such as weapons, training, and materiel; ideological support; and financial support. Sanctuaries or safe havens support insurgen-

[64] Michelle Faul, "Nigerian Ambassador Blasts US Refusal to Sell Arms," AOL, 11 November 2014, http://www.aol.com/article/2014/11/11/nigerian-ambassador-blasts-us-refusal-to-sell-arms/20991767/.

[65] "U.S. Denies It Refused to Sell Military Equipment to Nigeria," *Sahara Reporters*, 13 November 2014, http://saharareporters.com/2014/11/13/us-denies-it-refused-sell-military-equipment-nigeria.

[66] Chris Stein, "Nigerian Military Training Cancellation Baffles U.S. Experts," *Voice of America News*, 3 December 2014, http://www.voanews.com/content/nigeiran-military-training-cancellation-baffles-us-experts/2544161.html.

cies by enabling unfettered operations within a physical territory for training, recruiting, storing weapons, and planning.[67]

Nigeria. Nigeria took limited steps to cut off support to Boko Haram. As part of the May 2013 state of emergency declared in the three most affected states of Yobe, Borno, and Adamawa, the state altered laws and functions of government. Nigeria took such measures as curfews, roadblocks, mass arrests and detentions, and cordoning off suspected insurgency operation areas to exercise control of the population.

President Jonathan attempted to extend the state of emergency in November 2014; however, lawmakers voted against the extension, claiming that after 18 months the state of emergency was not having positive effects on the conflict.[68] There is little to suggest that these actions improved the situation. Indeed, "before the emergency, Boko Haram was operating mainly around Damaturu and Maiduguri . . . but since the emergency we have seen Boko Haram moving and occupying from 14 to 16 local governments in all the states. Even the Chibok girls were abducted during the emergency rule."[69]

Furthermore, the Nigerian government has a severely limited, and ultimately delayed, capacity to monitor and secure its northern borders. For the past several years, Boko Haram has found sanctuary operating across the border in neighboring Niger, Chad, and Cameroon.[70] Until the May 2014 Paris summit, Nigeria and Cameroon

[67] Daniel L. Byman, Peter Chalk, Bruce Hoffman, William Rosenau, and David Brannan, "Assessing the Impact of External Support," in *Trends in Outside Support to Insurgent Movements* (Santa Monica, CA: Rand Corporation, 13 December 2014), http://www.rand.org/content/dam/rand/www/external/congress/terrorism/phase2/insurgent.pdf.

[68] Asumpta Lattus, "Nigeria's State of Emergency 'A Failure'," *DW*, 21 November 2014, http://www.dw.de/nigerias-state-of-emergency-a-failure/a-18079380.

[69] Ibid.

[70] William Tuleu and Colby Goodman, *Nigeria: What Could the New U.S. Border Control Program Include?* (Washington, DC: Center for International Policy, Security Assistance Monitor, 7 December 2014), http://www.securityassistance.org/blog/nigeria-what-could-new-us-border-control-program-include.

had not been collaborating to resolve the border problem.[71] Niger and Nigeria have an agreement allowing troops to cross the border, and Nigeria is forging a similar agreement with the government of Chad.[72] At the Paris summit, the regional governments "agreed to share information and coordinate their intelligence work, to keep joint watch over their borders, and to develop the capacity to intervene swiftly in response to threats."[73] They each agreed "to send 700 troops to the Lake Chad region. . . . However, that promise has yet to be fully honoured."[74]

Nigeria has struggled to cut off financial support to Boko Haram. It is clear that Boko Haram has a fundraising system in place, but it is intricate and opaque.[75] Kidnapping for ransom, trafficking illegal weapons and drugs, robberies, and assassinations for hire generate income for the insurgency.[76] These are difficult sources of funding to cut off, given that many of the transactions take place on the black market.

Finally, Nigeria has struggled to cut off the flow of arms and ammunition to the group. Substantiating the fact that effective border security is key, insurgent support continues to transport armament across the border into Nigeria illegally. [77] Boko Haram obtains weapons, ammunition, and other materiel from the Nigerian Army, usually after defeating government soldiers, raiding barracks and outposts, or receiving redirected supplies from corrupt military officials in exchange for money.[78]

[71] John Irish and Bate Felix, "Paris Summit to Try to Rally Region against Nigeria's Boko Haram," Reuters, 16 May 2014, http://www.reuters.com/article/2014/05/16/us-nigeria-girls-summit-idUSBREA4F0BQ20140516.

[72] Ibid.

[73] Agence France-Press, "Cameroon Soldiers Desperate for Help in Boko Haram Fight," *Daily Mail*, 2 December 2014, http://www.dailymail.co.uk/wires/afp/article-2858415/Cameroon-soldiers-desperate-help-Boko-Haram-fight.html.

[74] Ibid.

[75] Terrence McCoy, "Paying for Terrorism: Where Does Boko Haram Gets Its Money From?," *Independent*, 6 June 2014, http://www.independent.co.uk/news/world/africa/paying-for-terrorism-where-does-boko-haram-gets-its-money-from-9503948.html.

[76] Blanchard, *Nigeria's Boko Haram*.

[77] McCoy, "Paying for Terrorism."

[78] Michelle Faul, "Report: 10 Generals Guilty of Arming Boko Haram," Yahoo News, 3 June 2014, http://news.yahoo.com/report-10-generals-guilty-arming-boko-haram-100856925.html.

United States. The United States established the Trans-Sahara Counterterrorism Partnership more than a decade ago to limit terrorist activity in the African Sahel region that includes Nigeria, Chad, and Niger. The key focus of improving border security through a multilateral forum promotes border security between member states to stop the flow of people, weapons, and commercial activities that could support Boko Haram and other terrorists in the region.[79] More recently, the American government pressed for a more robust multinational effort in the Sahel, including Cameroon, to address the cross-border issues related to Boko Haram, and in September 2014, a State Department official announced that "the U.S. is planning a 'major' new security program to help Nigeria battle Boko Haram terrorists."[80]

This multipronged approach to cut off the population's support to Boko Haram includes addressing development and humanitarian efforts, but there is also an important strategic communications aspect of COIN. For example, the United States plans to launch a 24-hour television channel in northeast Nigeria to broadcast messaging intended to counter the Boko Haram narrative.[81]

On the financial front, Boko Haram has largely been immune to sophisticated U.S. Treasury Department tools used to track terrorist funding because the bulk of the insurgency's financial activity occurs outside the banking system.[82] Criminal activity, kidnapping for ransom, and other transactions are untraceable through formal financial systems, and these processes contribute to the U.S. struggle to cut off Boko Haram's monetary support.

[79] Lesley Anne Warner, *The Trans-Sahara Counter Terrorism Partnership: Building Partner Capacity to Counter Terrorism and Violent Extremism* (Alexandria, VA: CNA, March 2014), https://lesleyannewarner.files.wordpress.com/2014/05/tsctp-building-partner-capacity-to-counter-terrorism-and-violent-extremism2.pdf.

[80] Russell Berman, "U.S., Nigeria, Cameroon, Chad and Niger Team Up to Thwart Boko Haram," *Wire*, 4 September 2014, http://www.govexec.com/defense/2014/09/us-nigeria-cameroon-chad-and-niger-team-thwart-boko-haram/93194/.

[81] David Storey, "U.S. to Finance Nigeria's Anti-Militant TV Channel in Northern Nigeria," Reuters, 6 June 2014, http://www.reuters.com/article/2014/06/06/us-nigeria-usa-television-idUSKBN0EH2H320140606.

[82] Phil Stewart, "Here's How Boko Haram Is Outsmarting U.S. Efforts to Choke the Terror Group's Financing," *Business Insider*, 1 July 2014, http://www.businessinsider.com/how-boko-haram-is-outsmarting-us-efforts-to-choke-its-financing-2014-7.

Best Practice 8: Pursue Opportunities to Reach a Settlement to the Conflict

An insurgency can end in any of four ways: the COIN government wins, the insurgency wins, the conflict evolves into something else, or a negotiated settlement is reached.[83] While a contemporary insurgency rarely sees one side or the other emerge as the clear victor, a negotiated settlement can effectively end violence and should be pursued by the affected government. Conditions must be right for stakeholders to reach a negotiated settlement. Primarily, both the government and insurgency must believe they cannot defeat their opponent and neither must want to continue fighting indefinitely. In other words, a stalemate usually occurs before both parties agree to settle differences nonviolently.[84]

Nigeria. The dynamic of Nigeria ramping up its military response each time Boko Haram increases the number and lethality of attacks creates a mindset of mutual escalation that limits the effectiveness of negotiations. The government's previous efforts to negotiate with Boko Haram have failed for multiple reasons.[85] At times, once negotiations were taking place, Boko Haram backed out, "pointing to a lack of sincerity on the part of the government."[86] Nigeria presented similar accusations regarding the insurgency. As recently as October 2014, Nigeria announced cease-fire talks with Boko Haram; however, that agreement fell through. Likewise, Nigeria realized minimal effects from numerous amnesty and rehabilitation programs to reintegrate Boko Haram fighters, supporters, and family members back into society.

[83] *Guide to the Analysis of Insurgency 2012* (Washington, DC: U.S. Government, 7 December 2014), http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/COIN/Doctrine/Guide%20to%20the%20Analysis%20of%20Counterinsurgency.pdf.

[84] U.S. Joint Chiefs of Staff, *Counterinsurgency,* Joint Publication 3-24 (Washington, DC: Joint Chiefs of Staff, 22 November 2013), http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf.

[85] For detailed information on the Nigerian government's attempts to negotiate with Boko Haram, see Marc-Antoine Pérouse de Montclos, *Nigeria's Interminable Insurgency? Addressing the Boko Haram Crisis* (London: Chatham House, Royal Institute of International Affairs, September 2014), 29, http://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20140901BokoHaramPerousedeMontclos_0.pdf.

[86] Ibid.

Nigeria continues to seek a settlement to the conflict. First, a settlement would offer a quick, easy way to end the fighting, which politically could have been viewed as a great accomplishment for President Jonathan leading up to elections. Second, the right deal could potentially avert the harder work of addressing the root causes of the conflict, such as corruption. Exchanging financial incentives for peace worked in the 2009 Movement for the Emancipation of the Niger Delta (MEND), but it also served to quell other militant activities after years of ongoing unrest and violence in the country's oil-rich delta region.

To settle the delta conflict, the government launched a $500-million-per-year program that includes amnesty for militants and financial incentives ranging from direct payments (estimated at $410 per month for ex-fighters) to job training and employment.[87] This program mostly ended the violence but remains on shaky ground because Nigeria has not addressed the underlying causes of the conflict. Essentially, the program is a payoff with a high price tag, which may not be sustainable over the long term.[88]

Pursuing a similar financial incentive settlement program for the battles with Boko Haram may be a waste of Nigeria's time since that conflict differs fundamentally from the delta one. The delta groups could directly impact, and essentially hold hostage, the country's primary source of income—oil. But oil does not exist in the north; thus, Nigeria has no incentive to offer a settlement as acceptable to Boko Haram as the lucrative one offered to the delta groups. Unlike the delta groups at least initially motivated by the oil wealth not trickling down to the local populations, "Boko Haram includes a popular, religious millenarian dimension"[89] absent in the delta that "makes it immune to the accepted ways Nigerian politicians 'settle' their opponents; mostly by payoffs."[90]

[87] Will Ross, "Has Nigeria's Niger Delta Managed to Buy Peace?," BBC News, 1 May 2013, http://www.bbc.com/news/world-africa-22357597.
[88] Ibid.
[89] John Campbell, "Nigeria's Boko Haram and MEND Similar?," *Africa in Transition* (blog), Council on Foreign Relations, 4 October 2012, http://blogs.cfr.org/campbell/2012/10/04/nigerias-boko-haram-and-mend-similar/.
[90] Ibid.

United States. Legal concerns restrict the United States' role in negotiating a settlement between Nigeria and Boko Haram. The State Department's declaration of Boko Haram as a foreign terrorist organization in 2013 is due to the fact that "any form of support, including expert advice or assistance . . . is considered material support of terrorism"[91] and makes it illegal for U.S. entities to be involved in the negotiations. Furthermore, given its ideology, Boko Haram is unlikely to consider any settlement involving the United States. Alternatively, the American government could encourage regional partners, such as Chad, to continue to support Nigerian–Boko Haram negotiations.[92]

Conclusions

Nigeria's Narrow Counterterrorism Approach

The Nigerian government has not pursued an approach supporting the eight best practices to combat insurgency. Rather, its CT approach primarily focuses on trying to defeat the group through military, security, and law enforcement means. As indicated by the continued conflict intensification and group growth, Nigeria's approach has been ineffective and counterproductive thus far. The government's attempts to negotiate a deal that would incentivize the group to shut down its illegal and typically violent operations have not been successful.

While recent efforts have been made to change this approach, Nigeria has neither worked effectively with its neighbors to cut off support to Boko Haram nor taken the steps necessary to weaken the group's hold on the local population. It has failed to protect civilians from harm and has not effectively responded to the humanitarian needs of those living in conflict-affected areas. Given the large (and increasing) number of casualties, kidnappings, and refugees/IDPs, any efforts to protect the population and provide humanitarian relief to date have fallen short in significant ways.

[91] Kay Guinane, "U.S. Law Limits Options for Nonviolent End to Nigerian Girls Nightmare," *World Post*, 16 May 2014, http://www.huffingtonpost.com/kay-guinane/us-law-limits-options-for_b_5339013.html.
[92] Berman, "U.S., Nigeria, Cameroon, Chad, and Niger Team Up."

Nigeria's response reflects an analysis of the conflict that draws from the country's history with internal violence and is simplistic and inaccurate but politically convenient for those in power. Were Nigeria to change its mind and accept the conflict as an insurgency requiring a broad-based whole-of-government approach, it would mean pursuing tangible change and real reform beyond just rhetoric. At least two factors make this unlikely in the foreseeable future: systemic corruption and the government's proximate political priorities.

The U.S. Whole-of-Government Approach

In stark contrast to the Nigerian government, the United States, as a supporting partner, provided resources to Nigeria in a whole-of-government approach more closely following the eight COIN best practices. American efforts range from targeting underlying root causes of the conflict to addressing the military aspects of COIN and responding to the humanitarian needs of the people in the conflict area. That said, the American approach has been executed in piecemeal fashion. To date, U.S. agencies have not been using a single strategy that coordinates activities and programs in a way that has all stakeholders working toward a shared goal on common timelines.

The U.S. government provided limited military equipment and training to defeat Boko Haram, which left it open to Nigerian and domestic criticism. For example, Capitol Hill called for Leahy Law exceptions so that the United States could provide Nigeria with more materiel and training to fight the insurgency.[93] It is likely, however, that the United States will continue to make decisions concerning training and equipping the Nigerian Army contingent on their human rights practices. Thus, until the Nigerian Army demonstrates progress in this area, training and equipping will likely remain at current levels.

[93] Melanie Hunter, "Royce Calls for Temporary Waiver of Leahy Law so U.S. Can Help Nigeria Recover Kidnapped Girls," CNS News, 21 May 2014, http://cnsnews.com/news/article/melanie-hunter/royce-calls-temporary-waiver-leahy-law-so-us-can-help-nigeria-recover.

Given the difficulties American leaders have had working with the Nigerian government on the military front, the multilateral approach to the Boko Haram conflict recently began increasing involvement with Nigeria's neighbors. This approach may open doors for the United States that would not be opened by an exclusive focus on Nigeria as the primary partner in dealing with the conflict.

The U.S. government addresses the humanitarian situation in a way that appears quite robust compared to Nigeria's own response, particularly given that Nigeria is not a poor country. Based on its oil wealth, Nigeria should have the resources available to meet the humanitarian needs of the people in the northeast, but it has not done so to date. As such, the question arises: should the government continue to implement a whole-of-government approach with a partner that is taking a fundamentally different approach?

Changes Nigeria Would Need to Make to Implement a COIN Approach

To understand the tangible steps Nigeria would need to take to shift to a more COIN-like approach, the authors identified specific gaps between current efforts and an appropriate blend of the best practices (best practice[s] in brackets):

- Devise a strategy grounded in a balanced view of the conflict as an insurgency. Reject and abandon the notions that Boko Haram is merely a manifestation of an external global terrorist phenomenon and not the result of underlying, internal problems and that it is only the most recent in a long line of troublemakers that can be quickly crushed by the military or pacified with large sums of money. [Devise a strategy that is built on an analytically derived conflict assessment.]
- Identify and coordinate activities of the appropriate range of interagency partners needed to implement an effective whole-of-government approach to address the insurgency. Reduce overreliance on military forces to solve the problem. [Implement a coordinated whole-of-government approach.]

- Improve governance through transparency and accountability and reduce corruption. Target complicit local political elites, religious leaders, military commanders, and law enforcement officers. Focus on stopping government forces' illegal and extrajudicial practices; publicly hold accountable those guilty of these practices. [Bolster government legitimacy.]
- Identify and address the underlying socioeconomic causes of the conflict. Include the particular economic disparities between the north and the south, the unfair distribution of national wealth, and the perceived favorable treatment of one group (ethnic, religious, etc.) over others. [Bolster government legitimacy.]
- Devise a communications strategy that bolsters the government's legitimacy in the eyes of the local population. Present a realistic and consistent depiction of the conflict, articulate the government's strategy for ending the conflict and improving security, dispel Boko Haram's narrative against the government, and state how the government of Nigeria will address the immediate humanitarian needs of the affected populations. [Bolster government legitimacy, protect the population, and provide humanitarian relief.]
- Provide security and protection to people living in conflict-affected areas. Legitimate state security forces (the military and the police) would need to be in the lead with each having its own appropriate, and limited, role. [Protect the population in affected areas and provide humanitarian relief.]
- Ramp up the humanitarian response in affected areas significantly. Focus on providing shelter, food, and medical care to the people driven from their homes. [Protect the population in affected areas and provide humanitarian relief.]
- Consider increasing the role of vigilante groups, such as the civilian JTF, to atone for the current lack of military capabilities and capacity. Pursue a deliberate plan to demobilize

the groups when they are no longer needed.[94] [Protect the population in affected areas and provide humanitarian relief.]

- Restructure the military response from a CT approach to a broader COIN approach. Consider the spectrum of posture and positioning, training and equipping, and community relations. [Attack the insurgent network.]
- Cut off support to the group. Formalize a mechanism to work with regional partners also affected by the conflict, specifically Niger, Chad, and Cameroon. Focus on improving border security and eliminating sanctuary. Tackle the insurgency's communications, social media, and ability to recruit. [Cut off support and eliminate sanctuaries.]
- Continue negotiating a settlement with Boko Haram that includes amnesty, rehabilitation, and deradicalization programs. [Pursue opportunities to reach a settlement to the conflict.]

[94] Patricio Asfura-Heim, *Risky Business: The Future of Civil Defense Forces and Counterterrorism in an Era of Persistent Conflict* (Arlington, VA: CNA, October 2014).

Cybersecurity Initiatives in the Americas: Implications for U.S. National Security

by José de Arimatéia da Cruz and Taylor Alvarez

The importance of developing domestic and international cybersecurity initiatives to counter threats to the world's communication technology infrastructure becomes more evident as Internet accessibility increases.[1] The United States and Europe currently recognize the threat of cyberterrorism; Latin America, however, focuses more on cybercrime due to the "highest rates of real and perceived

Dr. da Cruz is a professor at Armstrong State University (ASU) in Savannah, Georgia, where he teaches both undergraduate and graduate courses in Latin American and African foreign policy, Third World national security, and insurgency/counterinsurgency. He also is currently a visiting research professor at the U.S. Army War College, and has a visiting teaching appointment at the Center for Latin American Studies at the School of Economics in Prague. His credentials include; an MS in criminal justice with an emphasis in cyberaffairs and security from ASU and a PhD in political science from Miami University in Oxford, Ohio.

Alvarez is a senior political science undergraduate student at ASU minoring in Spanish and international studies. She will graduate in December 2015 with an honors distinction and looks forward to working in the U.S. security sector after pursuing her master's in international intelligence and security.

[1] Cybersecurity initiatives include strategies and programs intended to protect public, private, and government technology networks. The multilayered approach to identify and respond to cyberterrorism and cybercrime involves government policymakers and technology professionals as well as users. See White House, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: Executive Office of the President of the United States), https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf. Although the exact meaning of "cyberterrorism" is obscure, U.S. Federal Bureau of Investigation Special Agent Mark M. Pollitt coined the working definition of a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents." See Serge Krasavin, *What Is Cyber-Terrorism?* (Zurich: *Computer Crime Research Center*, 2002), http://www.crime-research.org/library/Cyber-terrorism.htm. Cybercrimes are categorized by the damage inflicted on computer and technology assets, fraud targeting individuals and organizations, and perpetration of human abuse and trafficking. See Interpol, "Cybercrime," http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

insecurity"[2] and the rapidly growing Internet population.[3] A comparison of these initiatives and responses to cybercrime in Argentina, Brazil, Cuba, Mexico, and Venezuela illustrates the usefulness of cooperative efforts the United States might adapt into policy to improve their response to similar issues.

Increasingly, international, statewide, and independent actors work together to encourage digital capabilities and continue funding "to defend sovereignty and to project power."[4] The Inter-American Committee Against Terrorism, composed of members from the Organization of American States (OAS), works to advance countercyber strategies and techniques. The Symantec Corporation, SecDev Foundation, and Igarapé Institute are examples of independent organizations that, like Inter-American Committee and OAS, conduct studies of state efforts to collect information and provide advice to boost current cybercrime countermeasures. One such neutralizer fights cybercrime and bolsters cybercapability through public awareness. The "Stop.Think.Connect."[5] campaign informs the public about safe Internet practices and individual digital information security practices. Led by the Anti-Phishing Working Group and the National Cyber Security Alliance, Stop.Think.Connect. is gaining traction in the United States, Brazil, and a few other countries throughout the Americas. A number of states also have or are in the process of implementing analogous initiatives and national response policies.

[2] Graham Denyer Willis, Robert Muggah, Justin Kosslyn, and Felipe Leusin, *Smarter Policing: Tracking the Influence of New Information Technology in Rio de Janeiro*, Strategic Note 10 (Rio de Janeiro: Igarapé Institute, November 2013), 2, http://igarape.org.br/wp-content/uploads/2013/10/Smarter_Policing_ing.pdf.

[3] Organization of American States (OAS) and Symantec, *Latin American + Caribbean Cybersecurity Trends* (Washington, DC: OAS Secretariat for Multidimensional Security/Symantec Corporation, June 2014), 11, http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf.

[4] Kenneth Geers, "Pandemonium: Nation States, National Security, and the Internet," *Tallinn Papers* 1, no. 1 (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014), 12, https://ccdcoe.org/publications/TP_Vol1No1_Geers.pdf.

[5] Stop.Think.Connect., "About Us," (2014), http://www.stopthinkconnect.org/about-us/.

As the world becomes increasingly "swamped in malware" and populated by potential cybercriminals,[6] individuals, criminals, and law enforcement professionals are developing substantially stronger Internet skills. While law enforcement professionals and government officials are restricted to lawful activities, criminals and terrorists limitlessly traverse the Internet to pursue their illicit agendas. Deviants can more effectively target and strike at citizens with poor device security—a noted current major issue with unprotected mobile phones[7]—and more easily recruit members or carry out criminal acts via the Internet. State officials and international actors are progressively recognizing the danger of, and preparing to defend themselves against, cybervulnerabilities and possible attacks. This progression can be seen in the responses and policy changes in the wake of Edward J. Snowden's revelations[8] and the attack on Sony possibly sanctioned by and, at the least, publicly supported by North Korea.[9]

Latin America and Cyber(In)Security

Argentina

The Argentine government substantially improved cybersecurity during the past few years in response to growing domestic and international concerns. One of the first Latin American countries to implement a national cyber-response team, the National Office of Information Technology National Program for Critical Information Infrastructure and Cyber Security created the Argentine Computer Emergency Response Team in 1994,[10] which developed into the National Program for Critical Information Infrastructure and Cyber Security. Unfortunately, it is very difficult to effectively combat

[6] Geers, "Pandemonium," 11.

[7] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 21–23.

[8] In 2013, security contractor Edward Snowden released information about secret National Security Agency (NSA) programs collecting information on domestic and foreign Internet activities ranging from official government business, energy operations, and illegal activities. See Anthony Boadle, "Latin American Nations Fuming over NSA Spying Allegations," Reuters, 9 July 2013, http://www.reuters.com/article/2013/07/10/us-usa-security-latinamerica-idUSBRE96900920130710.

[9] CBS News, "The Attack on Sony," *60 Minutes*, 12 April 2015, http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/.

[10] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 35.

cybercrimes without standardized policy and a legal framework. And, since the public typically endures the most malicious technology-based attacks, countering cybercrime begins with public knowledge of how to spot and report cyberincidents. The Argentine public awareness campaign, "Internet Sano," provides this information, best practices, and possible risks inherent to using modern technology.[11] See table 1 for other states that have established computer security incident response teams (CSIRTs) throughout Latin America.

The Snowden leaks prompted many Latin American nations to build multilateral partnerships, such as the cooperative agreement between Argentina and Brazil, to improve cyberdefense capabilities announced in September 2013.[12] Argentina takes a more proactive approach to digital data protection, which has been "recognized by the European Commission as the only Latin American country with an adequate level of protection."[13] Namely, Internet privacy rights are similar to other forms of media. Argentina's "Personal Data Protection Law No. 25.326, passed in 2000 . . . exists to guarantee individuals' rights of honor and privacy, and to give them access to their personal data."[14] The Argentine government has yet to explicitly declare a stance regarding privacy concerns despite Snowden's revelations and growing cybersecurity concerns.

Brazil

Approximately 22 million Brazilians were victims of cybercrimes in 2012,[15] and that number continues to grow. This large number of

[11] Ibid., 36; and Family Online Safety Institute (FOSI), "Global Resource and Information Directory: Argentina," *FOSI*, 2014, http://www.fosigrid.org/south-america/argentina.
[12] "Argentina, Brazil Agree on Cyber-Defense Alliance against U.S. Espionage," RT News, 15 September 2013, http://www.rt.com/news/brazil-argentina-cyber-defense-879/.
[13] Xath Cruz, "Data Protection and Privacy Issues in Latin America," *CloudTimes*, 21 November 2012, http://cloudtimes.org/2012/11/21/data-protection-privacy-issues-latin-america/.
[14] BakerHostetler, *2015 International Compendium of Data Privacy Laws* (Washington, DC: BakerHostetler Privacy and Data Protection Team, 2015), 1, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.
[15] Rachel Glickhouse, "Explainer: Cybercrime in Latin America," Americas Society and Council of the Americas, 21 October 2013, http://www.as-coa.org/articles/explainer-cybercrime-latin-america.

Table 1. CSIRTs established throughout Latin America*

Country	Name and/or reference of the legislation
Argentina	ICIC—National Program for Critical Information Infrastructure and Cyber Security (*Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*)
Brazil	CERT.br—Computer Emergency Response Team-Brazil (*Centro de Estudos, Reposta e Tratamento de Incidentes de Seugurança no Brasil*) CTIR Gov—Center of Security Incident Handling in Computer Networks of the Federal Public Administration (*Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Aministraçâo Pública Federal*)
Chile	CLCERT—Chilean Computer Emergency Response Team
Colombia	colCERT—Cybernetic Emergency Response Group of Columbia (*Grupo de Repuesta a Emergencias Cibernéticas de Colombia*)
Guatemala	CSIRT.Gt—Computer Security Incident Response Team-Guatemala (*Centro de Respuestas a Incidentes de Seguridad Informática de Guatemala*)
Mexico	UNAM-CERT—Computer Security Response Team of the National Autonomous University of Mexico (*Equipo de Respuesta a Incidentes de Seguridad en Cómputo de la Universidad Nacional Autónoma de México*)**
Paraguay	CSIRTPy—Security Incident Response Team of Paraguay (*Equipo de Respuesta a Incidentes de Seguridad de Paraguay*)
Peru	peCERT—Emergency Coordinator of Telecommunication Networks of Peru (*Coordinadora de Emergencias de Redes Teleinformáticas de Peru*)
Uruguay	CERTUy—National Center of Information Security Incident Response (*Centro Nacional de Respuesta a Incidentes en Seguridad Informática*)
Venezuela	VenCERT—National System of Telecommunication Incident Management of the Bolivarian Republic of Venezuela (*Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela*)

*English designations differing from literal translation reflect currently accepted agency titles.

**The Mexican CSIRT is located at a university and addresses incidents nationally.

Source: Gustavo Diniz and Robert Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America*, Strategic Paper 2 (Rio de Janeiro: Igarapé Institute, 2012), 15.

cybervictimization occurs despite "advanced capabilities in cybersecurity and deterring cybercrime, with numerous state institutions and agencies playing active roles."[16] The Brazilian Information and Communication Technology Management Committee established their Cyber Security Incident Response Team in 1997, which was renamed CERT.br in 2005. CERT.br establishes and maintains supportive partnerships, conducts cybercrime trend analyses and training, builds awareness, and monitors networks[17] to respond to cyberincidents. Private-public cooperation in Brazil embodies an ideal cyberdefense situation because the public sector voluntarily shares cyberincident information, thereby enabling CERT.br to plan prevention strategies and responses appropriate to the most prominent types of cyberattacks and high-value targets in the absence of legal direction.[18]

Atypical among Latin American states, Brazil invests in military-based cyberdefense capabilities to curb cybercrime. Created and operational in 2010, the Cyberdefence Center of the Brazilian Army[19] currently coordinates the army's cybersecurity actions. Eventually, the center will also oversee the Brazilian Navy and Air Force to ensure federal and military network protection from foreign and domestic attacks. Brazil also provides an interesting case study for attempting to quell the growing conflict among criminals, law enforcement, and the public with the Unidade de Policia Pacificadora (UPP). Also known as Pacification Police Units, UPP offers a community-based approach to policing via technology to quell social unrest, police corruption, and cyber and traditional crime incidents through accountability and oversight (table 2).[20] Police officers immerse themselves in the local community by patrolling on foot and giving out personal emails and phone numbers. By forging these

[16] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 41.

[17] Brazilian Internet Steering Committee, "About CERT.br," *Núcleo de Informação e Coordenação do Ponto BR*, 19 March 2012, http://www.cert.br/about/.

[18] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 41.

[19] Diniz and Muggah, *A Fine Balance*, 16–17.

[20] One Brazilian *favela* (slum or shantytown) added 24-hour camera coverage to the UPP patrol area to ensure honesty in the reporting of and responses to crimes. It also led to Internet accessibility for police stations and stronger community relations. See Willis et al., *Smarter Policing*.

Table 2. A sample of police units devoted to cybercrime in Latin America*

Country	Name and/or reference of the legislation
Argentina	Federal Computer Security Division of the Interior Superintendence Federal Argentina Police (*División de Seguridad Informática Federal de la Superintendencia del Interior–Policía Federal Argentina [PFA]*)
Bolivia	Cybercrime Division of the Special Force to Fight Crime National Police (*División Delitos Informáticos de la Fuerza Especial de Lucha contra el Crimen [FELCC] de la Policía Nacional*)
Brazil	Enforcement Cybercrime Unit Federal Police (*Unidade de Repressão a Crimes Cibernéticos [URCC] da Policía Federal*)
Chile	Cyber Crime Investigation Brigade of the National Police Headquarters-Chilean Economic Crimes Investigations (*Brigada Investigadora de Ciber Crimen [BRICIB] de la Jefatura Nacional de Delitos Económicos–Policía de Investigaciones de Chile [PDI]*)
Colombia	Technology Research Group of the Division of Criminal Investigation (Investigative Area against Economic Wealth) of the Criminal Investigation and Interpol of the National Police of Columbia (*Grupo de Investigaciones Tecnológicas de la Subdirección de Investigación Criminal [Área Investigativa contra el Patrimonio Económico] de la Dirección de Investigación Criminal e Interpol [DIJIN] de la Policía Nacional de Colombia*)
Dominican Republic	Crimes Investigation Department of High Technology of the Central Directorate of Criminal Investigations National Police (*Departamento de Investigaciónes y Crímenes de Alta Tecnología [DICAT] de la Dirección Central de Investigacioues Criminales [DICRIM] de la Policía Nacional*)
Honduras	Special Computer Crime Unit of the National Directorate of Special Investigation of the National Police (*Unidad Especial de Delitos Informáticos de la Dirección Nacional de Servicios Especiales de Investigación [DNSEI] de la Policía Nacional*)
Mexico	Cyber Police Intelligence Sector of the Federal Preventive Police and the Secretariat of Information Technology of the Federal Public Security Secretariat (*Policía Cibernética del Sector de Inteligencia de la Policía Federal Preventiva [PFP] y de la Subsecretaría de Tecnologías de la Información de la Secretaría de Seguridad Pública Federal [SSP]*)

Peru	Research Division High Tech Crime of the Criminal Investigation and Support Justice National Police (*División de Investigación de Delitos de Alta Tecnología [DIVINDAT] de la Dirección de Investigación Criminal y de Apoyo a la Justicia [DIRINCRI] de la Policía Nacional*)
Uruguay	Computer Crime Department of the National Police (*Departamento de Delitos Informáticos de la Policía Nacional*)

*English designations differing from literal translation reflect currently accepted agency titles.
Source: Diniz and Muggah, *A Fine Balance*, 16–17.

personal connections with citizens, law enforcement hopes to bridge the gap between state and public spheres; however, it has increased the opportunity for contention between the two groups.[21] Even with these attempts of combatting traditional and cybercrime within the state, Brazil still expresses concern over criminalizing cyberoffenses. The lack of a cohesive corresponding legal framework addressing various offenses inhibits prosecuting those who commit recognized cybercrimes.[22]

Cuba

While Cuba has seen an increase in the proliferation of Internet and mobile phone users in recent years, the market is still highly restricted to those who can afford such devices.[23] Cuba's Internet penetration rate was reported to be at 25.71 percent as of 2013,[24] but most users can only access the "government-filtered" Intranet domain in place of the global Internet.[25] According to the National Statistics Office, approximately 2.9 percent of the Cuban population has Internet access. However, according to outside experts, the estimate is

[21] Having friendly relations with law enforcement officers builds a sense of trust and cohesiveness necessary to turn the tide of crime, but it also provides greater visibility and exposure to hostile citizens, such as traffickers or others threatened by the police presence, which has led to altercations. See Ibid.

[22] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 42.

[23] Freedom House, *Cuba: Freedom on the Net 2014* (Washington, DC: Freedom House, 2014), https://www.freedomhouse.org/report/freedom-net/2014/cuba.

[24] International Telecommunications Union, "Percentage of Individuals Using the Internet," http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls.

[25] Freedom House, *Cuba: Freedom on the Net 2014*.

more likely to be 5–10 percent due to black market sales of dial-up minutes.[26] Although some may determine that this small percentage of citizens with Internet access prevents cybercrime from being a major concern for Cuba, the United States' intent to reestablish diplomatic ties and improve public communications accessibility must also be considered.[27] Authorized and unauthorized channels already exist by which citizens bypass the state's Internet blocks. There is a growing quasi-business for those who can construct antennas to access illegal dial-up connections, post content on foreign networks, or sell time on illegally shared accounts.[28] Thus, allowing even a small degree of this flow of communication and information creates opportunities for cybercriminals to target newly introduced Internet users and the government's institutions from both inside and outside the state. In other words, despite claims of government-controlled networks, states wrestle with this important and intrusive aspect of cybersecurity.

Mexico

The rising levels of hacktivism[29] throughout the world are staggering and Mexico has been ranked "as one of the world's most vulnerable countries to cyberattacks."[30] It saw an estimated 40 percent[31] and a

[26] Andrea Rodriguez, "In Cuba, Mystery Shrouds Fate of Internet Cable," Yahoo News, 21 May 2012, http://news.yahoo.com/cuba-mystery-shrouds-fate-internet-cable-180553388--finance.html.

[27] White House Office of the Press Secretary, "Fact Sheet: Charting a New Course on Cuba," 17 December 2015, http://www.whitehouse.gov/the-press-office/2014/12/17/fact-sheet-charting-new-course-cuba.

[28] Freedom House, *Cuba: Freedom on the Net 2014*.

[29] Hacktivism uses cybercrime techniques, such as phishing, information theft, and Web page defacement, not with the intention of economic gain but to further a social or political agenda. See Benjamin Mattern "Cyber Security and Hacktivism in Latin America: Past and Future," *Council of Hemispheric Affairs*, 24 July 2014, http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/.

[30] Rebecca Conan, "Defending Mexico's Critical Infrastructure Against Threats," Report Company, 22 July 2013, http://www.the-report.net/mexico-prw/600-defending-mexico-s-critical-infrastructure-against-threats.

[31] OAS and Trend Micro, *Latin American and Caribbean Cybersecurity Trends and Government Responses* (Washington, DC: OAS Secretariat for Multidimensional Security / Trend Micro, May 2013), 7, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

staggering 113 percent[32] increase in the number of cybercrime incidents in 2012 and 2013, respectively. Largely attributed to the presidential campaign,[33] expanding hacktivism activities, growing Internet penetration, and an upward trend of criminals implementing cybertechnology also contribute to this increase.[34] Simultaneously, limited collaboration developing a national—much less international—cyberstrategy enables unconventional actors to achieve substantial success. Cartels, long a concern for the Mexican government, embrace the Internet to recruit new members, complete transactions, and search for new and more targets to exploit. Likewise, the proliferation and anonymity of the Internet fosters hacktivist recruitment for groups such as Anonymous and improves their ability to escape prosecution. Combined with perceived declines in social and economic conditions, hacktivism is likely to increase. Specifically, situations such as the retaliatory kidnapping of a hacker with the group Anonymous who threatened the Los Zetas cartel and their cohorts with cybertactics will be more likely.[35]

In addition to the concerns associated with prosecuting conventional crime, ambiguous cyberspace jurisdictions make it difficult to arbitrate responses to individual involvement in such events.[36] In essence, nation-states recognize the dichotomy of hacking—strategic hacking can undermine the campaign against criminal hacking—that adds yet another complex dimension to the current cybersecurity situation for Mexican policymakers and law enforcement officials regarding cyber and traditional criminals.

Prioritization of cyberthreats has yet to rise like other national security concerns that result from the environment along the U.S.-Mexico border, such as that of traditional cartel violence and

[32] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 65.
[33] Glickhouse, "Cybercrime in Latin America."
[34] José Abreu, "Mexican Drug Cartels and Cyberspace: Opportunity and Threat," *InfoSec Institute*, 21 March 2012, http://resources.infosecinstitute.com/mexican-cartels/; and Conan, "Defending Mexico's Critical Infrastructure."
[35] Ibid.
[36] Pierluigi Paganini, "Hacktivism: Means and Motivations . . . What Else?," *InfoSec Institute*, 2 October 2013, http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/.

corruption among Mexican law enforcement officials.[37] Formal attempts for cyberdefense and proactive cyber-response efforts did not start in Mexico until 2012 with the creation of its national cyberincident response center, CERT-MX.[38] Despite this late start, Mexico has recently become more proactive in raising awareness for increased cybersecurity of its citizens and public and private sectors. It has also been actively seeking to improve cybersecurity efforts by building cooperative relationships with international organizations and governments, including the CSIRTs of Colombia, the United States, Holland, and Japan.[39] Mexico also seeks similar collaboration from such international organizations as the Forum of Incident Response and Security Teams and the OAS.[40]

Venezuela

Almost half (about 44.1 percent in 2014) of Venezuelan citizens had access to the Internet, and the volume of cyberconcerns is a burden on the limited capacity of the national response team, VenCERT.[41] Venezuela claims to have an interest "in increas[ing] transparency" while encouraging cooperation between the public and private sectors while "ensur[ing] technological sovereignty."[42] Venezuela's Special Law against Computer Crime introduced in 2001 defines types of "crimes against information systems, economic property and patrimony, personal privacy, and communications."[43] The Interoperability Act of 2012 standardizes "an appropriate level of interoperability in information systems used by state agencies and entities" and con-

[37] With corruption reaching even the federal levels, law enforcement has been monitoring and purging corrupted officers since 2005. See Ted Galen Carpenter, "Corruption, Drug Cartels, and the Mexican Police," *National Interest*, 4 September 2012, http://nationalinterest.org/commentary/corruption-drug-cartels-the-mexican-police-7422?page=show.

[38] Conan, "Defending Mexico's Critical Infrastructure."

[39] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 64.

[40] Ibid.

[41] Ibid., 81–82.

[42] Ibid., 82.

[43] Electronic Privacy Information Center (EPIC), *EPIC–Privacy and Human Rights Report, 2006: Bolivarian Republic of Venezuela* (New South Wales, Australia: World Legal Information Institute), http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Bolivari.html.

sequences for inhibiting the system's operation.[44] Combined, these two major Venezuelan laws comprise part of the legal framework that allows coordinated, informed, and effective responses to cybercriminal offenses (table 3).

In the aftermath of the Snowden affair and the announcement of the National Security Agency's espionage activities, Venezuela's public scrutinized the extent to which this legislation allows the infringement of privacy in exchange for a stronger sense of national security. "In the Plan of the Nation 2013 to 2019, which seek[s] to deepen the socialist model that [the late] President [Hugo] Chávez began," Venezuela seeks tighter constraints on the public's use of and access to information on the Internet, social media, and communication.[45] As with Cuba, the government is willing to forego individual privacy to increase national security. Much like Brazil, the Venezuelan plan for the nation also seeks to bolster military-based cyberdefense.

Venezuela's restrictive Internet usage guidelines improved the government's ability to respond to cybercrime incidents. The government likewise strengthened national cybersecurity efforts by hiring additional highly qualified personnel and informing the public about safe Internet practices. The "Information Security Begins with You" campaign began in 2009 as a way of "educating the staff of government institutions and organized communities"[46] and encouraging Venezuelans to support cybercrime initiatives. Venezuela also conducts regular capacity building programs for cyber-related personnel through relevant coursework, and while not in any official cooperative efforts with other state actors, Venezuela has successfully responded to previous cyberincidents by collaborating with CSIRTs

[44] Ley de Interoperabilidad [Law of Interoperability], Gaceta Oficial N° 39.945 [National Diary Number 39.945], Decreto N° 9.051 [Decree Number 9.051] (15 June 2012), http://interoperabilidad.gobiernoenlinea.gob.ve/index.php/conceptos/sobre-promociones/promociones/96-ley-de-interoperabilidad.

[45] Sandra Benítez, "Venezuela: Spying in Venezuela through Social Networks and Emails," in *Global Information Society Watch 2014: Communications Surveillance in the Digital Age* (Melville, South Africa: Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries, 2014), 270–75, http://www.giswatch.org/sites/default/files/spying_in_venezuela_through_social_networks_and_emails.pdf.

[46] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 82.

Table 3. Key legislation for cybercrime in selected Latin American countries

Country	Name and/or reference of the legislation
Argentina	Cybercrime Law 26.388, 2008 (*Ley 26.388 de Delitos Informáticos*, 2008)
Bolivia	Cybercrime Law 1768, 1997 (*Ley 1768 de Delitos Informáticos*, 1997)
Chile	Cybercrime Law 19.223, 1993 (*Ley 19.223 de Delitos Informáticos*, 1993)
Colombia	Protection of Information and Data Law 1273, 2009 and Data Messages, Electronic Trade, and Digital Signatures Law 527, 1999 (*Ley 1273 de la Protección de la Información y de los Datos*, 2009 and *Ley 527 de Mensajes de Datos, del Comercio Electrónico y de las Firmas Digitales,* 1999)
Costa Rica	Cybercrime Law 8148, 2001 (*Ley 8148 de Delitos Informáticos*, 2001)
Dominican Republic	Cybercrime Law 53, 2007 (*Ley 53 de Delitos Informáticos*, 2007)
Ecuador	Electronic Trade, Signatures, and Data Messages Law 67, 2002 (*Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos*, 2002)
Guatemala	Penal Code altered to include cybercrime (2000)
Mexico	Penal Code altered to include, among others, cybercrime (1999)
Panama	Penal Code Articles 216, 222, 283, 362, 362, and 364 and Documents and Electronic Signatures Law 51, Article 61, 2008 (Articles 216, 222, 283, 362, and 364 of the Penal Code and Article 61 from *Ley 51 Documentos y Firmas Electrónica*, 2008)
Paraguay	Law 1.160, 1997 (*Ley 1.160* alters the Penal Code in order to include, among others, cybercrime, 1997)
Peru	Cybercrime Law 27.309, 2000 (*Ley 27.309 de Delitos Informáticos*, 2000)
Uruguay	Copyright Protection and Related Rights Law 17.616, 2003 (*Ley 17.616 de Protección del Derecho de Autor y Derechos Conexos* contains explicit provisions regarding digital intellectual property, 2003)
Venezuela	Special Law Against Cybercrime, Decree 48, 2001 (*Decreto 48 Ley Especial Contra los Delitos Informáticos*, 2001)

Source: Diniz and Muggah, *A Fine Balance*, 13.

internal and external to the Southern Common Market trade organization.[47] Furthermore, Venezuela began encouraging industry cooperation regarding technology information sharing and cyberattack reporting to intensify Venezuela's cyberdefense.

Cyber Strategic Implications for the United States

Just as friends reconnect through virtual relationships, the Internet leads to political alliances and enmities extending into cyberspace, thereby adding a new and intriguing dimension to traditional statecraft. As the Chairman of the Joint Chiefs of Staff, Army General Martin E. Dempsey, stated, "The spread of digital technology has not been without consequence. It has also introduced new dangers to our security and our safety."[48] For international jihadists, the Internet has become the most cost-effective means of delivering its messages worldwide and coordinating attacks. The Internet allows jihadist organizations to recruit new members without leaving the confines of their safe havens. For example, three teenagers ran away from their homes in northwest London and travelled to Syria with the intent of joining the Islamic State of Iraq and the Levant (ISIL).[49] The terrorist organization recruited the three young women—ages 15 and 16—via the Internet.[50] In secret and without fear of retaliation, jihadist groups and terrorist organizations are using the Internet as a tool to conduct cyberplanning—"the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed."[51]

[47] Ibid.

[48] Claudette Roulo, "DOD Must Stay Ahead of Cyber Threat, Dempsey Says," American Forces Press Service, 27 June 2015, http://www.defense.gov/news/newsarticle.aspx?id=120379.

[49] ISIL in this article represents the terrorist organization also known as ISIS, the Islamic State of Iraq and Syria, the Islamic State of Iraq and ash-Sham, or the Islamic State.

[50] Polly Mosendz, "Three British Teens Who Ran Away to Join ISIS Spotted in Syrian Sharia Camp," *Newsweek*, 9 March 2015, http://www.newsweek.com/three-british-teens-who-ran-away-join-isis-spotted-syrian-sharia-camp-312278.

[51] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters* 33, no. 1 (Spring 2003): 112–23, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/03spring/thomas.pdf.

For example, ISIL uses modern technology significantly more than many other violent nonstate actors. While al-Qaeda and the Taliban rejected the tools of modernity, ISIL embraces technology to successfully advance their cause by spreading its message and barbarities, linking itself to the world news. For example, "one of ISIL's more successful ventures is an Arabic-language Twitter app called The Dawn of Glad Tidings, or just Dawn. The app, an official ISIL product promoted by its top users, is advertised as a way to keep up on the latest news about the jihadi group."[52] Using technology, ISIL "proselytize[s], recruit[s], and raise[s] money, and this is a clear sign of modernity."[53]

As a 2013 Council on Foreign Relations report states, "Cyberspace is now an arena for strategic competition among states, and a growing number of actors—state and non-state—use the Internet for conflict, espionage, and crime."[54] Recent incidents involving Russia and the Republic of Georgia, in which Georgia's government Web sites were bombarded with a Distributed Denial of Service (DDoS) and eventually were brought to a standstill, show the awesome power of cyberwarfare.[55] Cyberwarfare is indeed a power multiplier. It also shows that "cyber[warfare] can only be an enabler of physical effort. Stand-alone (popularly misnamed as 'strategic') cyberaction is inherently grossly limited by its immateriality."[56] Cyberterrorists and rogue nation-states have realized the dual utility of the Internet. Martin C. Libicki points out, "Cyberattacks have neither fingerprints nor the smell of gunpowder, and hackers can

[52] J. M. Berger, "How ISIS Games Twitter," *Atlantic*, 16 June 2014, http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/; and Loretta Napoleoni, *The Islamist Phoenix: The Islamic State and the Redrawing of the Middle East* (New York: Seven Stories Press, 2014), 63.

[53] Ibid., 113.

[54] John D. Negroponte, Samuel J. Palmisano, and Adam Segal, *Defending an Open, Global, Secure, and Resilient Internet*, Independent Task Force Report 70 (New York: Council on Foreign Relations, June 2013), 66, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836.

[55] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, 13 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[56] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle Barracks, PA: U.S. Army War College Press, April 2013), 49, http://www.strategicstudies-institute.army.mil/pubs/download.cfm?q=1147.

make an intrusion appear legitimate or as if it came from somewhere else."[57] Given the attribution problem, we could very well see a proliferation of attacks coming from such states as North Korea, Venezuela, Iran, China, and Russia, and yet be unable to directly attribute any of the attacks to those countries.

The Internet is becoming an integral part of the globalized international system of the twenty-first century and part of the "new wars . . . in which the difference between internal and external is blurred; they are both global and local and they are different both from classic inter-state wars and classic civil wars."[58] In the globalized world of the twenty-first century, nation-states and violent nonstate actors alike will make use of the power of technology to advance their activities without fear of retaliation, prosecution, or concerns from geographical boundaries. In Latin America, governments have become extremely concerned about the proliferation of the Internet as a force multiplier in the commission of crimes. For example, governments in Latin America are concerned with "criminal practices of individuals and crime networks connected to cyberspace with the intention of making illicit economic gains. Common examples range from e-banking scams to drug trafficking and child pornography."[59] The prevalence of drug trafficking increases in relation to "the [Internet emerging] as a critical interface in the selling and purchasing of all manner of commodities, including both prescription and illicit narcotics. . . . Likewise, drug profits are often laundered through the Internet through the purchasing of goods and services and the transferring of cash."[60] In this new brave world, a "new criminality" is emerging in cyberspace. The realm of "the Internet and related social media tools have not just empowered citizens to exercise their rights, but also enabled and extended the reach of gangs, cartels, and organized criminals."[61]

[57] Martin C. Libicki, "Don't Buy the Cyberhype: How to Prevent Cyberwars from Becoming Real Ones," *Foreign Affairs Snapshot*, 14 August 2014, https://www.foreignaffairs.com/articles/united-states/2013-08-14/dont-buy-cyberhype.

[58] Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era,* 3d ed. (Redwood City, CA: Stanford University Press, 2012), vi.

[59] Diniz and Muggah, *A Fine Balance*, 5.

[60] Ibid., 7.

[61] Ibid., 1.

The ability to be vigilant regarding the proliferation of the Internet cannot be overemphasized given the current world climate. In his testimony before the House Armed Services Committee, the commander of U.S. Cyber Command and the director of the National Security Agency, Navy Admiral Michael S. Rogers, stated that cyberspace "is now part of virtually everything we in the U.S. military do in all domains of the battlespace and each of our lines of effort. There is hardly any meaningful distinction to be made now between events in cyberspace and events in the physical world, as they are so tightly linked."[62] Additionally, Rogers also "believe[s] potential adversaries might be leaving cyberfingerprints on our critical infrastructure, partly to convey a message that our homeland is at risk if tensions ever escalate toward military conflict,"[63] while noting four trends occurring during cyberhostilities:

- autocratic governments that view the open Internet as a lethal threat to their regimes;
- ongoing campaigns to steal intellectual property;
- disruptions by a range of actors that range from denial-of-service attacks and network traffic manipulation to the use of destructive malware; and
- states that develop capabilities and attain system access for potential hostilities, perhaps with the idea of enhancing deterrence or as a beachhead for future cybersabotage.[64]

[62] Cheryl Pellerin, "Cybercom Chief: Cyber Threats Blur Roles, Relationships," Defense Media Activity, 6 March 2015, http://www.defense.gov/news/newsarticle.aspx?id=128305.

[63] Ibid.

[64] Ibid. These trends are important in Latin American-U.S. relations due to the rise of the "pink tide" in Latin America. The "pink tide" is a group of radical, leftist politicians that came to power in the 1990s who are diametrically opposed to U.S. foreign policy. The rise of the "pink tide" in Latin America occurred between 1998 and 2009 when leftist leaders won elections in the following states: Venezuela (1998), Chile (2000), Brazil (2002), Argentina (2003), Uruguay (2004), Bolivia (2005), Nicaragua (2006), Peru (2006), Ecuador (2007), Honduras (2007), Paraguay (2008), and El Salvador (2009). This ideological bloc is also known as the Bolivarian Alliance for the Peoples of Our America (ALBA). For more on the sociopolitical aspects of the pink tide, see William I. Robinson, "Latin America's Left at the Crossroads," *Al Jazeera*, 14 September 2011, http://www.aljazeera.com/indepth/opinion/2011/09/2011913141540508756.html.

Recommendations for a Safer Cyberspace

In comparison to Europe and North America, Latin America's weak countermeasures and low risk of punishment combine with the technology's affordability to make the continent "fertile ground" for cybercrime. More than half of Latin American and Caribbean businesses reported cyberattacks during 2012.[65] Late that year, PiceBOT, a particularly malicious malware capable of gathering financial information, originated somewhere within Latin America.[66] Pharming, deflecting user access from legitimate Web sites to gather sensitive information, costs Mexican banks approximately $93 million annually.[67] Although "over 90 percent of countries that responded to the [Comprehensive Study on Cybercrime] questionnaire have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence,"[68] many Latin American states are still not sufficiently equipped to effectively build up cyberdefense capabilities.[69]

To make Latin America a safer cyberspace environment, the following actions should be taken. First, Latin American governments need to develop a clear legal framework outlining the various types of cybercrimes. Establishing a "comprehensive and consensus-based framework for legislating on cybercrime"[70] will enable seamless investigation of cybercrimes and stronger prosecution of cybercriminals. This standardization, in conjunction with consistent legal language across Latin America, would resolve the "patchwork of re-

[65] Wharton School of the University of Pennsylvania, "Latin America Reaches a Crossroads for Guarding against Cybercrime," *Knowledge@Wharton* (blog), 24 July 2013, http://knowledge.wharton.upenn.edu/article/latin-america-reaches-a-crossroads-for-guarding-against-cybercrime/.

[66] Ibid.

[67] Ibid. For more on pharming, see the antivirus company Norton's explanation of the cybercrime concern at "Online Fraud: Pharming," Symantec Corporation, 2015, http://securityresponse.symantec.com/norton/cybercrime/pharming.jsp.

[68] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime: Draft–February 2013* (New York: United Nations Office on Drugs and Crime, 2013), xxiii, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[69] Wharton School, "Latin America Reaches a Crossroads."

[70] Diniz and Muggah, *A Fine Balance*, 4.

sponses and loopholes open to exploitation."[71] The importance of cybersecurity efforts becomes a state imperative with the growing frequency of high-scale incidents throughout the world and the general Latin American population's increasing awareness of the implications of cybercrime as identified by the Stop.Think.Connect. movement.[72]

In fact, ordinary citizens typically bear the brunt of malicious Internet scams and hacking techniques. This is especially true in such cities as Rio de Janeiro that are "undergoing major technical and social transformations," necessitating a policy change to decrease the "distance—spatial, social, and psychological—between citizens and the state."[73]

As a response to public cyberconcerns, institutions of higher learning "should also provide tracks specifically for the study of cybersecurity."[74] However, for those who cannot afford to take such courses, awareness campaigns can go a long way in promoting safe Internet practices. With "2 billion Internet users worldwide . . . under protected from cybercrime,"[75] a more informed Internet population can help improve cybersecurity. Encouraging multilateralism and citizen empowerment through safe Internet use can only add to the success of a more structured and extensive international response system, legislation, and cyber-response units. In Mexico, concerned citizens use social media platforms, such as Twitter and Facebook, to compensate for the lack of media reports on cartel abuses.[76] This ability to share information bypasses corrupt law enforcement and the cartels to allow neighborhood protection from illicit activity.

[71] Ibid.

[72] OAS and Symantec, *Latin American + Caribbean Cybersecurity Trends*, 4–7.

[73] Graham Denyer Willis, Robert Muggah, Justin Kossyln, and Felipe Leusin, *The Changing Face of Technology Use in Pacified Communities*, Strategic Note 13 (Rio de Jeneiro: Igarapé Institute, February 2014), 2, http://igarape.org.br/wp-content/uploads/2014/01/NE-13-Changing-face-of-techology-29jan.pdf.

[74] Wharton School, "Latin America Reaches a Crossroads."

[75] Diniz and Muggah, *A Fine Balance*, 4.

[76] Igarapé Institute and SecDev Foundation, *Cyberspace & Open Empowerment in Latin America*, Strategic Note: The Open Empowerment Initiative (Rio de Janeiro: Igarapé Institute/SecDev Foundation, June 2013), 5, http://www.cto.int/media/k-r/Open%20Empowerment%20in%20Latin%20America.pdf.

Additionally, a multilateral agreement should be established to foster increased information flow and freedom of Internet use within Latin America. However, public outcry regarding privacy infringement by Latin American governments illustrates the precarious balance of increasing state responses to cyberconcerns while maintaining a status of public empowerment and freedom.[77] Despite the state's best efforts, the intense public scrutiny creates a disadvantage to combatting cybercrime.

Latin American nations in partnership with the United States should establish cyberfusion centers to analyze data in which "'fusion' refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and the private sector."[78] Fusion centers could warehouse and disseminate information and knowledge on the latest investigation and cyberforensic techniques. In this role, the centers would not only provide an overview of how computer network systems are affected once a cyberattack has been committed, but also identify courses of action to mitigate damage.

Latin American nation-states and the United States must also work together on cyberattribution, whereby the United States' expertise can help Latin American governments resolve cyberintrusion situations with neighboring states. Since attribution "has a territorial dimension, and therefore turns into a political problem,"[79] cyberintrusions remain one of the "black swans" in cyberspace.[80]

[77] Geers, "Pandemonium," 12.

[78] U.S. Department of Homeland Security and U.S. Department of Justice, *Considerations for Fusion Center and Emergency Operations Center Coordination: Comprehensive Preparedness Guide (CPG) 502* (Washington, DC: U.S. Department of Homeland Security and U.S. Department of Justice, May 2010), 1, http://www.fema.gov/pdf/about/divisions/npd/cpg_502_eoc-fusion_final_7_20_2010.pdf; and David L. Carter and Jeremy G. Carter, "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement," *Criminal Justice and Behavior* 36, no. 12 (2014): 1323–39, doi: 10.1177/0093854809345674.

[79] Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), 141.

[80] "Black swan," coined by Nassim Nicholas Taleb in 2007, refers to highly improbable and unpredictable massive impact events, for example, the 9/11 attacks, the 2008 economic collapse or, in the cyberworld, the hack into Sony Pictures. See Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

Latin American nations claim they cannot afford to attribute a cyberattack that might escalate to physical war without solid evidence. Given the animosity between Latin American nations, falsely attributing cyberattacks could have devastating consequences especially as the political landscape becomes more complicated. Specifically, as more nation-states develop cyberprograms with disruptive intents, cybercriminals have greater access to cybersystems, and ideological actors—such as hackers or extremists—become more involved in cyberpolitical activity.[81]

We highly recommend a strong public-private cyberpartnership in Latin America. As the Igarapé Institute and the SecDev Foundation stated, "In Latin America, private corporations and firms appear to be playing a comparatively marginal role in supporting cybersecurity initiatives and enhancing public safety in cyberspace. Not a single public-private partnership could be identified in the course of the preparation of this strategic paper in Latin America."[82]

It is time for Latin American nations to encourage a broader meaning of cyberthreats and intellectual engagement within academia to facilitate greater communication among social science disciplines traditionally ignored during cyberconversations. Because "cyberthreat[s] cannot be eliminated,"[83] governments should include the expertise from "various subdisciplines of computer science as well as social science, political science, legal studies, and even history"[84] to develop more effective strategies and responses.

Given the proliferation of computers as tools in the commission of crimes, nation-states must embrace the concept of a Cyber-

[81] James R. Clapper, "Opening Statement to the Worldwide Threat Assessment Hearing" (remarks, Senate Armed Services Committee, 26 February 2015), http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee.

[82] Diniz and Muggah, *A Fine Balance*, 19.

[83] Clapper, "Opening Statement."

[84] Rid, *Cyber War*, 164.

Westphalia Treaty.[85] Given the absence of universally accepted and enforceable norms of behavior in cyberspace, a Cyber-Westphalia could bring some normalcy to the current situation of cyberattacks, cyberterrorism, and cyberespionage "in which multiple actors continue to test their adversaries' technical capabilities, political resolve and thresholds."[86] A Cyber-Westphalia Treaty would "[laud] the benefits of order in the virtual space, based on the norms of sovereignty and power concentration in the hands of states, [which] have guided the actions of the international community in the last few years."[87]

A Vision for Cybersecurity

Former Secretary of Defense Leon E. Panetta commented on the possibility of a "cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life, in fact, it would paralyze and shock the nation" at the hands of a state or nonstate aggressor.[88] He contends that many individuals "worry about hackers and cybercriminals who prowl the Internet, steal people's identities, steal sensitive business information, steal even national security secrets," but a concentrated cyberterrorist strike is of greater concern.[89] Panetta cites the 2012 DDoS attacks on American financial institutions as well as the Shamoon virus that infected Saudi Arabia's Aramco oil

[85] Collectively referred to as the Peace or Treaty of Westphalia, the 1648 series of treaties signed in Münster and Osnabrücke ended Europe's Thirty Years' War by establishing stable borders, a system for interstate relations, and rules for political-social organization. See Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf.

[86] Clapper, "Opening Statement."

[87] Myriam Dunn Cavelty, "The Normalization of Cyber-International Relations," in *Strategic Trends 2015: Key Developments in Global Affairs*, ed. Oliver Thranert and Martin Zapfe (Zurich: Center for Security Studies, 2015), 94, http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2015.pdf.

[88] Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (speech, Business Executives for National Security, New York, 11 October 2012), http://www.defense.gov/transcripts/trasncript.aspx?transcriptid=5136.

[89] Ibid.

company as proof that the Internet is the new battlefield.[90] In spite of advances in cybercapabilities, "Potential aggressors are exploiting vulnerabilities in [American] security."[91] However, the sentiment that only large-scale cyberattacks represent a national security threat overshadows the extent of cybercrimes committed in Latin America and the United States, two of the most digitally active regions in the world. And, as these geographical boundaries shrink as a result of "the Internet collaps[ing] space, as users around the world interact without regard for territory, engag[e] in cross-border exchanges and [elicit] state actions that blur the domestic-foreign divide,"[92] it will become more evident that "the state is no longer supreme authority over information"[93] even though their populations are in dire need of an overarching system to counteract the cybercriminals. In recognition of this, countries in Latin America are developing cybercrime strategies that are influenced by regional actors and international organizations, such as the OAS, the Igarapé Institute, and the SecDev Foundation.[94]

By establishing national CSIRTs and cyberlegislation, states and their private sector allies are better equipped to efficiently and quickly respond to, investigate, and prosecute cybercriminals. With increased private and public sector information sharing through this formal national response unit, necessary coordination will be more feasible. By institutionalizing cyberfusion centers, states can be proactive in their fight against cybercriminals. Additionally, collaborative cybersecurity efforts could support accurate attribution and the development of a formal Cyber-Westphalia Treaty. This standardization would reduce the conflict created by inconsistent cyberboundaries and encourage statewide and international coherence to acceptable conventions. To protect Internet users, awareness

[90] Ibid.
[91] Ibid.
[92] Milton L. Mueller and Hans Klein, "Sovereignty, National Security, and Internet Governance: Proceedings of a Workshop," *Internet Governance Project* (workshop, Syracuse, NY: Syracuse University, 12 December 2014), 1, http://www.internetgovernance.org/wordpress/wp-content/uploads/Proceedings-publication.pdf.
[93] Ibid., 10.
[94] Diniz and Muggah, *A Fine Balance*, 9.

campaigns and education courses should be funded to improve personal cybersecurity. With a conservative estimate of approximately 3 billion people having access to the Internet, these measures are vital to the development of the "new frontier" of the twenty-first century.

Sociocultural Intelligence Apparatus: The PSYWAR Campaign against the Viet Cong

by Tal Tovy

The August 1917 essay "The Twenty-Seven Articles" by T. E. Lawrence informed British officers of societal considerations appropriate for working with Arab populations in Transjordan and Syria.[1] Some 90 years later, *Military Review* published a piece by David J. Kilcullen, "The Twenty-Eight Articles," providing Western forces with relational insights appropriate to the Arab–Muslim populace.[2] A review of the two texts brings up a similar conclusion: to reach the hearts and minds of the local population, one must study and understand the complex aspects of their culture. Montgomery McFate promotes the critical value of cultural understanding to current irregular warfare.[3] Notably, in a war against irregular forces, the center of gravity lies with securing or controlling the support of the

Tovy is an associate professor at Bar-Ilan University, Israel. He holds a PhD in history from the University of Haifa. A veteran of the Israel Defense Forces, Dr. Tovy has published extensively on a variety of military history topics, including the influence of counterinsurgency theory on American combat operations. His other fields of interest encompass Western military thought, U.S. foreign policy, and U.S. military history. Tovy has contributed articles to a variety of publications, such as *Armed Forces & Society*, the *Journal of Military and Strategic Studies*, the *European Journal of American Studies*, and *War in History*.
The author would like to thank the Marine Corps Heritage Foundation for its support in writing this piece.

[1] T. E. Lawrence, "The Twenty-Seven Articles," *Arab Bulletin* (20 August 1917): 126–33. See also the Brigham Young University World War I document archive at http://wwi.lib.byu.edu/index.php/The_27_Articles_of_T.E._Lawrence.

[2] LtCol David Kilcullen, "'Twenty-Eight Articles': Fundamentals of Company-level Counterinsurgency," *Military Review* (May–June 2006): 134–39, http://www.au.af.mil/au/awc/awcgate/milreview/kilcullen.pdf.

[3] Montgomery McFate, "Culture," in *Understanding Counterinsurgency: Doctrine, Operations, and Challenges*, ed. Thomas Rid and Thomas Keaney (London: Routledge, 2010), 189–90.

local population, and thus understanding the characteristics of local society and its needs becomes paramount to preventing passive or active insurgent support. More important, respecting sociocultural influences assists counterinsurgent governments in preventing new members from enlisting in insurgencies and even encourages current members to desert. Kilcullen's and McFate's influential works became more than academic discussions; the U.S. Army and Marine Corps incorporated their precepts into official counterinsurgency (COIN) doctrine.[4]

This article begins by examining the role of anthropological studies as a prime methodological tool for shaping Vietnam War era propaganda aimed at driving Viet Cong fighters to desertion. The analysis that follows frames the promulgation of American researchers' views of rural Vietnamese society in the resulting propaganda. Lastly, the scope of anthropological theory illustrates the significance of its role within psychological warfare (PSYWAR).

Anthropological studies written during the Vietnam conflict serve as primary sources under the precept that this research generated intelligence used during the development of the U.S.–South Vietnamese Chieu Hoi Program, which encouraged Viet Cong fighters' desertion. Essentially, these resources demonstrate the development of a more efficient military strategy as theoretical and practical researchers engaged in cross-disciplinary understanding of the cultural characteristics of the Vietnamese peasantry, the enemy, and the conflict. Although these anthropological studies serve as historical sources for understanding American learning and thinking patterns shaping COIN mechanisms during the Vietnam War, this work does not strive for anthropological rigor. Likewise, this article does not assess the success of U.S. PSYWAR operations during the Vietnam conflict, but instead considers the contribution of anthropology to the development of propaganda content.

[4] *Counterinsurgency,* FM 3-24/MCWP 33.3-5 (Washington, DC: Department of the Army and Headquarters Marine Corps, 2006). McFate cowrote the third chapter, "Intelligence in Counterinsurgency," and Appendix A is an expansion of Kilcullen's *Military Review* piece.

Vietnam-Era Sociocultural Research

Although the Viet Cong began organizing in the mid-1950s, little was known about the movement until the mid-1960s. During the second half of 1964, the war in South Vietnam escalated as the Viet Cong used Vietnam's instability to expand military actions and extend political impact in rural areas.[5] During that year, U.S. Secretary of Defense Robert S. McNamara—though some attribute it to Army General Paul D. Harkins—asked the following questions:[6] Who are the Viet Cong? What drives their fighters to display such great combat efficiency? What is the source of their motivation?[7]

Compelled by this progressive interest, Douglas E. Pike produced an oft-quoted monograph[8] that stands out as one of the most comprehensive and elementary publications about the Viet Cong. Gerald C. Hickey articulated an excellent anthropological examination of the Vietnamese village.[9] And the Rand Corporation provided an organizational response to these questions as well as insight into the sociological and organizational structure of the Viet Cong and the forces driving villagers to enlist.

Established by the U.S. Air Force after World War II, Rand researched various strategic fields[10] and partnered with the U.S. Army Advanced Research Projects Agency (ARPA) in the early 1960s to

[5] For a short overview of the escalation of the war in 1964, see Spencer C. Tucker, *Vietnam* (Lexington: Kentucky University Press, 1999), 103–5.

[6] Seymour J. Deitchman, *The Best-Laid Schemes: A Tale of Social Research and Bureaucracy*, rev. ed. (Quantico, VA: Marine Corps University Press, 2014), 161. See also Robert S. McNamara, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York: Random House, 1995), 32. Gen Harkins was the commander of Military Assistance Command–Vietnam from 1962 to 1964.

[7] Mai Elliott, *RAND in Southeast Asia: A History of the Vietnam War Era* (Santa Monica, CA: Rand, 2010), 49, 53.

[8] Douglas Pike, *Viet Cong: The Organization and Technique of the National Liberation Front of South Vietnam* (Cambridge, MA: MIT Press, 1966).

[9] Gerald Cannon Hickey, *Village in Vietnam* (New Haven, CT: Yale University Press, 1964). In the 1960s, Hickey was a researcher at Rand.

[10] One of the most comprehensive studies on academia as an advisory system to the military is that of Fred Kaplan, *The Wizards of Armageddon* (Stanford, CA: Stanford University Press, 1991). It showcases several theoreticians who worked at Rand during the 1950s and the significance of their ideas on developing the U.S. nuclear strategy. Kaplan states that the ideas posed by this group of researchers shaped American nuclear strategy.

study COIN. This transition served as a step in Rand's quest for relevance under the John F. Kennedy administration's new strategic perceptions, which claimed that insurgency in underdeveloped countries, specifically Southeast Asia, was Communism's main threat.[11]

Throughout the 1960s, Rand published a series written by social studies researchers, including several anthropologists, as part of the Viet Cong Motivation and Morale (M&M) Project.[12] More than 30 papers were published based on thousands of interviews with Viet Cong captives and deserters as well as interviews with refugees.[13] The M&M Project had two main goals: understand and define what prompted South Vietnamese villagers to join the Viet Cong and identify factors that would motivate soldiers to desert. The second objective, a subset of the first, developed as American involvement in Vietnam expanded to augment the South Vietnamese Chieu Hoi psychological warfare program.[14] The combined work of the M&M Project and Chieu Hoi program became the most massive and intensive PSYWAR campaign in military history.[15]

M&M Study Methodology

The Rand research on Viet Cong fighter motivation combined two schools of thought. The first extended 1940s military-sociologist

[11] For a general summary of Rand researchers in social studies, see Ron Robin, *The Making of the Cold War Enemy: Culture and Politics in the Military–Intellectual Complex* (Princeton, NJ: Princeton University Press, 2001), 19–56. For information on the move to insurgency studies, see Elliott, *RAND in Southeast Asia*, 7–44.

[12] After World War II, various social studies disciplines were incorporated into the discussion of strategies in the Cold War in general and in Vietnam in particular. See William M. Hartness, "Social and Behavioral Sciences in Counterinsurgency," *Military Review* 46, no. 1 (January 1966): 3–10; and Austin Long, *On "Other War": Lessons from Five Decades of RAND Counterinsurgency Research* (Santa Monica, CA: Rand, 2006), 5–6.

[13] For a detailed discussion of M&M, see Elliott, *RAND in Southeast Asia*, 45–90. See also Robin, *The Making of the Cold War Enemy*, 190–93.

[14] For a general summary, see Spencer C. Tucker, ed., *The Encyclopedia of the Vietnam War: A Political, Social, and Military History* (Oxford: Oxford University Press, 2000), 69–70.

[15] On the use of propaganda throughout American military history, see Arthur E. Meyerhoff, *The Strategy of Persuasion: The Use of Advertising Skills in Fighting the Cold War* (New York: Coward–McCann, 1965), 77–94. This article presents several examples of American propaganda pamphlets used to introduce the Chieu campaign from Robert W. Chandler, *War of Ideas: The U.S. Propaganda Campaign in Vietnam* (Boulder, CO: Westview Press, 1981).

methodology, and the second transitioned to studying the insurgency. The new trend for the institute relied on well-grounded research and experience dealing with the Communist threat in the Third World during the 1950s. Several studies examined achieving political stability and preventing the spread of Communism to Southeast Asia from a mainly economic standpoint. However, the organizational and social structure of Communist guerrilla groups continued gaining focus as researchers conducted more interviews with captives and deserters.

Recently criticized, the techniques used by sociologists Edward Shils and Morris Janowitz to interview German prisoners of war (POWs) about the unifying factors of the Wehrmacht[16] established sociology research methods for the military during the time of the M&M studies. Several Rand researchers based their interviews of Viet Cong captives and deserters during the Vietnam War on these same practices. Notably, Alexander L. George published a book in 1967 on the operational capabilities of the Chinese Communist Army based on interviews with Chinese prisoners captured by American forces during the Korean War.[17] Likewise, Lucian W. Pye and George K. Tanham interviewed POWs to determine the political and sociological structure of Communist guerilla movements. Pye focused his work in Malaya,[18] while Tanham researched Viet Minh[19] strategies and tactics more relevant to American forces fighting against them in Vietnam.[20]

[16] Edward A. Shils and Morris Janowitz, "Cohesion and Disintegration in the Wehrmacht in World War II," *Public Opinion Quarterly* 12, no. 2 (1948): 280–315.

[17] Alexander L. George, *The Chinese Communist Army in Action: The Korean War and Its Aftermath* (New York: Columbia University Press, 1967).

[18] Lucian W. Pye, *Guerrilla Communism in Malaya: Its Social and Political Meaning* (Princeton, NJ: Princeton University Press, 1956).

[19] Formed in China in 1941, the Viet Nam Doc Lap Dong Minh Hoi (League for the Independence of Vietnam), commonly known as the Viet Minh, were originally led by Communists yet open to those from all political parties. The organization's aim was to free Vietnam from French rule, but of course there were Vietnamese nationalists in the south who joined the Viet Cong, supporting the Viet Minh's efforts for a united and free Vietnam.

[20] See George K. Tanham, *Communist Revolutionary Warfare: From the Vietminh to the Viet Cong* (New York: Frederick A. Praeger, 1967). This book is a nonclassified version of the original study, incorporating relevant chapters on the Viet Cong.

Tanham posited that, although the Viet Minh became a regular army to combat the French, they should not be treated as a regular army due to lingering core principles of Mao Tse-tung's revolutionary warfare. As part of Project Sierra, Rand dispatched Tanham to Paris in 1955 to research the Viet Minh and compose a guidebook that would enable a better evaluation of the organization's strength.[21] Rand published the classified study, but the project was scrapped until the newly appointed Kennedy administration recognized the value of the study to finding solutions for Vietnam's revolutionary war.[22]

Why Anthropology?

Cultural anthropology explains human behavior as an outcome of cultural behavior and the existential experience shared by social groups, which is similar to John Keegan's proclamation that the characteristics of war are an explicit cultural manifestation of battling societies.[23] War conduct—past, present, and most likely future—is a direct outcome of a society's cultural makeup. War, says Keegan, is indeed the continuation of *Politik* by other means, as Clausewitz famously stated, but only if the societies in question are Western ones, products of Greco–Roman heritage. However, the Clausewitzian paradigm is irrelevant and untrue when applied to non-Western societies. As Mao states, even though guerrilla warfare historically shares worldwide characteristics, it still varies according to time, peoples, and conditions.[24] Therefore, cultural influence is most pronounced in irregular warfare. Essentially, Keegan and Mao believed that a Western military engaging a non-Western society must study the latter's cultural characteristics, not to change Western forces but rather to identify the best course of action to generate battlefield success—the ultimate mission for any army. In this manner, intelligence-

[21] Between 1954 and 1958, Rand led a series of wargame scenarios dubbed Project Sierra that demonstrated a limited war in Asia using the Korean War and the French war in Indochina as models.

[22] See Elliott, *RAND in Southeast Asia*, 9.

[23] John Keegan, *A History of Warfare* (New York: Alfred A. Knopf, 1993), 3–60.

[24] Mao Tse-tung, *On Guerrilla Warfare,* trans. Samuel B. Griffith (Mineola, NY: Dover Publications, 2005), 49.

gathering in preparation for, and during war, requires understanding the enemy's cultural essence.[25]

Just as cultural anthropology explains a sort of cultural evolution that occurs as societal standards are acquired through a long process of learning and adapting to physical realities, modern conflict research recognizes that, indeed, Western societies must understand the cultural essence of insurgencies. McFate emphasizes the crucial role anthropology plays in creating strategically, operationally, and tactically efficient systems valuable to political and social realities in Iraq and Afghanistan[26] and unequivocally posits that, before one understands the enemy, one must first understand the enemy's culture. Even more resolute, David Kilcullen claims that the culture of the extreme Islamist insurgency must be thoroughly studied. Specifically, al-Qaeda should be defined as a global Islamic insurgency attempting to spread its philosophical perceptions and interpretations of heresy (*kufr*)[27] across the Muslim world.[28] Therefore, Kilcullen's belief that COIN theories developed in the 1960s must be updated in light of the political and martial challenges and actions promoted by radical Islamic culture[29] complements the process of learning and

[25] See Geoffrey G. Gray, "Managing the Impact of War: Australian Anthropology and the South West Pacific," in *Science and the Pacific War: Science and Survival in the Pacific, 1939–1945*, ed. Roy M. MacLeod (Dordrecht, Netherlands: Kluwer Academic Publishers, 2000), 190–96. This title provides an analysis of the ways in which anthropology helped the Australian Army recruit the native population of Papua New Guinea for the war effort, specifically in cleansing areas with a Japanese presence.

[26] Montgomery McFate, "Anthropology and Counterinsurgency: The Strange Story of Their Curious Relationship," *Military Review* 85, no. 2 (March–April 2005): 24–38, http://www.au.af.mil/au/awc/awcgate/milreview/mcfate.pdf; McFate, "The Military Utility of Understanding Adversary Culture," *Joint Force Quarterly* 38, no. 3 (2005): 42–48; and McFate, "Culture," 189–201.

[27] *Kufr* means not believing in Islam whereas *takfiri* refers to the unbeliever and *takfir* refers to the accusation excommunicating a person from Islam. See Trevor Stanley, "Kufr–Kaffir–Takfir–Takfiri," Perspectives on World History and Current Events, http://www.pwhce.org/takfiri.html; and Sheikh Muhammed Salih Al-Munajjid, "21249: Kufr and Its Various Kinds," Islam Question and Answer, http://islamqa.info/en/21249.

[28] On al-Qaeda as a global organization, see Jason Burke, *Al-Qaeda: Casting a Shadow of Terror* (London: I. B. Tauris, 2003), 179–97.

[29] Kilcullen illustrates his philosophy in two essays: "Counterinsurgency Redux," *Survival* 48, no. 4 (2006–7): 111–30, http://www.au.af.mil/au/awc/awcgate/uscoin/counterinsurgency_redux.pdf and "Countering Global Insurgency," *Journal of Strategic Studies* 28, no. 4 (August 2005): 597–617. He further elaborates on his views in the full-length monograph, *Counterinsurgency* (Oxford: Oxford University Press, 2010), 165–226.

adapting to physical realities indicative of cultural anthropology as opposed to latent biological heredity.

Richard H. Shultz and Andrea J. Dew came to a similar conclusion as they examined changes in military conduct following the Cold War; after removing the Soviet threat, the United States faced new enemies independent of formal nation-states.[30] Terrorist organizations, tribal militias, drug cartels, and organized crime syndicates necessitate understanding culture in the modern sense of a set of rules or values that, when realized, produce behavior considered normal and accepted by society.[31] Governments who authenticate culture as the set of ideals, values, and beliefs through which humans interpret their experience and select their behaviors will be able to prepare COIN forces to construct conflict response strategies appropriate to the philosophical perspective of the enemy. Cumulatively, these anthropological theories and Vietnamese dynamics identified in the previously mentioned literature engender a model to understand the components of sociocultural intelligence apparatus.

From a military standpoint, anthropology is part qualitative and part abstract intelligence gathering, or cultural intelligence as Patrick Porter puts it.[32] Visual intelligence devices can reveal the quantity and location of enemy tanks but cannot disclose enemy intents. With COIN, the problem grows more severe; in an insurgency, it is difficult to even estimate the enemy's physical strength. Consequently, various COIN theories stress the population as the gueril-la force's center of gravity. It is therefore necessary to convince the populace to cease support of guerrilla organizations and, better still, support the government opposing the insurgents. Likewise, military strategists must move beyond British anthropologist Edward B. Tylor's definition of culture as a whole comprised of opinions, beliefs, artwork, laws, values, and other habits acquired by people of a certain

[30] Richard H. Shultz and Andrea J. Dew, *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat* (New York: Columbia University Press, 2006), 1–54.

[31] These definitions are basic for any discussion of culture in social anthropology. See, for instance, David Hicks and Margaret Anderson Gwynne, *Cultural Anthropology* (New York: Harper Collins, 1996), 24–25; and John H. Bodley, *Cultural Anthropology: Tribes, States, and the Global System* (Mountain View, CA: Mayfield, 1997), 8–9.

[32] Patrick Porter, *Military Orientalism: Eastern War through Western Eyes* (London: Hurst, 2009), 55–57.

society,[33] and use the characteristics of the affected society to create an understanding upon which operational patterns can be built.

For example, the Special Operations Research Office organized a 1962 symposium at the urging of the U.S. Army chief of research and development. American academics and senior military officers called attention to the need to understand the cultural, social, and economic constructs of Third World agrarian societies. The symposium focused on COIN doctrines and their relation to Vietnam as well as efforts to formulate an effective plan to counter Communist guerrilla warfare. Deputy Army Chief of Staff General Clyde D. Eddleman claimed that underdeveloped areas, such as Asia, Africa, and Latin America, formed the main front of the Cold War. He also stated the most effective mechanism in the war against the revolutionary Communist guerilla was a stable economic system acting on the primary needs and social structure of the population.[34]

Additionally, U.S. Army Office of the Chief of Civil Affairs Plans and Doctrine Division Deputy Chief Colonel Robert H. Slover presented military civic actions as a weapon against guerrilla forces, concurring that rural societies in underdeveloped countries create a critical battlefield vulnerability. To build local cooperation with COIN forces and to deprive guerilla fighters of public support, Slover recommended that the military reinforce ties with rural societies and support central governments by developing effective military civic actions. He also emphasized that these efforts should be based on a thorough understanding of the target population's lifestyle, customs, social structure, and needs as well as improving villagers' standard of living. Slover posited that this strategy to win over the local population would overpower the guerilla's infrastructure and limit their political success.[35]

[33] Edward Burnett Tylor, *Primitive Culture: Researches into the Development of Mythology, Philosophy, Religion, Art, and Custom*, 2 vols. (London: John Murray, 1871), 1.
[34] Gen Clyde D. Eddleman, "Limited War and International Conflict," in *Symposium Proceedings: The U.S. Army's Limited-War Mission and Social Science Research*, ed. William A. Lybrand (Washington, DC: American University, 26–28 March 1962), 27, 30–31.
[35] Col Robert H. Slover, "Civic Action in Developing Nations," in *Symposium Proceedings*, 70–72. See also D. Michael Shafer, *Deadly Paradigms: The Failure of U.S. Counterinsurgency Policy* (Princeton, NJ: Princeton University Press, 1988), 116–18.

Eddleman and Slover both based their lectures on Franklin A. Lindsay's 1962 essay claiming that control over the civilian population is the key to success in an unconventional war.[36] Lindsay analyzed the factors leading to the Viet Minh victory over the French in Indochina by describing the strategy to gradually gain command of the rural areas by drawing out the French. The countryside offered shelter, supplies, and personnel helpful to establishing and training a regular army.[37] Lindsay's work concluded that the French defeat in Vietnam occurred because the locals gradually sided with the Viet Minh.[38]

From this perspective, Lindsay argued that the foundation for any antiguerrilla warfare strategy and policy must be complete government control over rural areas.[39] The government must invest ample resources in civilian facets such as building schools and clinics and improving agricultural infrastructure while simultaneously performing military actions against Viet Cong strongholds. Military efforts must force guerrilla fighters to be constantly on the move; rout the enemy's control of the countryside; and deprive irregulars of food, shelter, medical attention, and munitions.[40] Lindsay made several recommendations to American Special Forces advisors arriving in the area: be well versed in local customs and cultures, know the language, and understand specific issues in each village. Essentially, the boots on the ground must be experts in guerrilla warfare from both a military and civilian perspective.[41]

A Brief Anthropological Analysis of Vietnamese Society

Learning from the Viet Minh, the U.S. Army invested in efforts to adapt their military strategies to persuade villagers to participate in the revolution. Exemplifying Lawrence's and Kilcullen's respective

[36] Franklin A. Lindsay, "Unconventional Warfare," *Foreign Affairs* 40, no. 2 (1962): 264–66, https://www.foreignaffairs.com/articles/asia/1962-01-01/unconventional-warfare.

[37] See Tucker, *Vietnam*, 62–63.

[38] Lindsay, "Unconventional Warfare," 266.

[39] Ibid., 269–71.

[40] Ibid., 267–68.

[41] Ibid., 274.

observations that cultural understanding supports military success[42] and that "counterinsurgency is armed social work, an attempt to redress basic social and political problems while being shot at,"[43] U.S. and South Vietnamese government agencies began gathering sociocultural intelligence to counter the Viet Cong. Specifically, the United States applied the anthropological concept that culture creates a holistic essence into which extraneous influences gradually permeate to understand the effects of political instability on the integrity of South Vietnamese rural society.

Still true today, war-era studies defined Vietnam as a multiethnic nation home to more than 50 ethnic groups with unique cultural characteristics.[44] Eighty-five percent of the population is still of Viet or Kinh ethnicity, lives in villages, and practices Buddhism. Other "major" ethnic groups make up a meager 1–2 percent of the population. Essentially, rural societies throughout Vietnam are nearly indistinguishable, appearing more as one homogenous culture, both ethnically and religiously.

Three spheres of influence dominate rural Vietnamese society: family, village, and religion. Vietnamese family and village structures follow the Confucian model, namely that society is hierarchic, unequal, yet harmonic, with the family representing the smallest unit.[45] This rigid hierarchy remains strictly based on gender and age. Women are subordinate to men; the young must acquiesce to their elders, whose role is to sustain the family. The nuclear family is the primary economic, social, and religious base to which one owes utter devotion and loyalty—more specifically, one is loyal to the head of the household. Concepts of patriotism are therefore foreign to the Vietnamese peasant.[46] Concluding that the family unit is of utmost importance in Vietnamese society, these people would do any-

[42] Lawrence, "The Twenty-Seven Articles."

[43] Kilcullen, " 'Twenty-Eight Articles'," 107.

[44] Today, 54 ethnic groups are recognized by the Vietnamese government.

[45] Pike, *Viet Cong*, 2–3.

[46] Simulmatics and U.S. Advanced Research Projects Agency [ARPA], "Improving Effectiveness of the Chieu Hoi Program," in *The Viet Cong: Organizational, Political, and Psychological Strengths and Weaknesses*, vol. 2 (Cambridge, MA: Simulmatics and ARPA, 1967), 82, 84–85.

thing to defend their family, maintain its economic stability, and also improve it, although they will almost never fight one another. The Vietnamese religion mixes Buddhism and ancestral veneration,[47] manifesting as family shrines that accompany those for the gods in central locations of the home.[48]

Viet Cong and U.S.–South Vietnamese recruiting strategies acknowledged these dynamics. The Viet Cong presented itself as defending villagers from the pressures of the central government and espoused economic improvement via agrarian reform, which would seize control over land from private entities with government ties and transfer them to the villagers. However, the Viet Cong had trouble gaining villagers' complete loyalty since some of their family members also served in the South Vietnamese army.

The U.S.–South Vietnamese PSYWAR efforts identified family as the innermost, and therefore most important, sphere of Vietnamese society. The United States estimated that at least a third of South Vietnamese villagers had relatives in the Viet Cong and would never furnish any information that might harm them.[49] Thus, U.S. efforts based on these dynamics achieved higher Viet Cong desertion rates as American involvement in South Vietnam increased.

Enlistment and Desertion: Anthropological Aspects from an American Standpoint

One of the most basic claims of cultural anthropology establishes that culture embodies a holistic system while simultaneously being open to changes resulting from the influence of external developments on the cultural group's inner dynamic. Furthermore, the pressure of these processes often damages the cultural fabric, and efforts to resolve tension generate political protest. These precepts explain the rural South Vietnamese adoption of ideological preferences

[47] Evidence of the traditions making up rural Vietnamese society can be found in a book of poems by unknown poets. These folk songs describe the Vietnamese life cycle and the flora and fauna crucial to the villager as well as family structure, marriage, and religion. See Nguyen Ngoc Bich, trans., *A Thousand Years of Vietnamese Poetry,* with contributions by Burton Raffel and W. S. Merwin (New York: Random House, 1975), 40–64.

[48] Hickey, *Village in Vietnam*, 120.

[49] Ibid., 84.

based on changing environmental factors[50] and practical needs[51] as opposed to the maintenance of a stable, culturally specific political ideology defined by typical Western terminology. Viet Cong enlistment should therefore be considered in the broader perspective that Vietnamese political orientation was never binding, and the organization used strategic social and economic protests to induce villagers' responses that shifted the balance of military or political power.

Studies beginning in the 1960s confirmed that, like other Third World agrarian protests, many factors led to the revolution in Vietnam and that the villagers' desire to improve their lifestyles served as the primary motivator to enlist in the Viet Cong movement.[52] Richard K. Horner explained that peasants revolt during times of political unrest, or when strong leadership guarantees an improvement in their status. Vietnam presented both.[53] Viet Cong propaganda encouraged political unrest by attacking the South Vietnamese government with accusations of opposition to the traditional unity of the Vietnamese people[54] and activated the populace with opportunities to pursue personal and economic interests[55] as well as promises of land ownership. Thus, the Viet Cong adopted traditional ideas and operated within the established cultural framework despite the secular, political nature of their revolutionary movement.[56]

Eric K. Wolf added to the anthropological framework, positing that when the villager can no longer trust traditional establishments, and alternative government institutions are simultaneously going through political or economic upheaval or limiting villagers'

[50] Pike, *Viet Cong*, 10.

[51] Richard K. Horner, "Agrarian Movements and Their Historical Conditions," *Peasant Studies* 8, no. 1 (Winter 1979): 9.

[52] For more on protests in general and in agrarian society in particular, see Teodor Shanin, "The Peasantry as a Political Factor," *Sociological Review* 14, no. 1 (1966): 5–10; and Eric R. Wolf, *Peasant Wars of the Twentieth Century* (New York: Harper & Row, 1969).

[53] Horner, "Agrarian Movements and Their Historical Conditions," 8, 11. According to Wolf, peasant revolts succeeded where there was a political void. See Wolf, *Peasant Wars of the Twentieth Century*, 290, 293.

[54] John C. Donnell, Guy J. Pauker, and Joseph J. Zasloff, *Viet Cong Motivation and Morale in 1964: A Preliminary Report* (Santa Monica, CA: Rand, 1965), 20–22.

[55] Pike, *Viet Cong*, 166.

[56] Donnell, Pauker, and Zasloff, *Viet Cong Motivation and Morale*, 20–22. See also Simulmatics and ARPA, "Improving Effectiveness of the Chieu Hoi Program," 81.

participation in them, the psychological, economic, social, and political groundwork is set for a revolutionary movement.[57] Under these conditions, villagers will adopt any political or economic ideology that promises the desired change by using external, and usually urban, factors to internalize the ideology. Ergo, a peasant rarely joined the Viet Cong for purely ideological reasons (i.e., belief in Communism).[58]

The Viet Cong, much like other revolutionary guerilla movements, depended on the rural surroundings and good graces of the villagers.[59] Following guerilla accession in the village, political cadres, often locals, spread Communism's ideological concepts by incorporating accepted Vietnamese traditions into previously ineffective political–philosophic messages. Villagers were told, quite simply, that adopting Communism would bring about the end of imperialism, and the resulting puppet-state would annihilate the large landlord class and set agrarian reform in motion. Using the traditional concept of the holy bond between man and land (*xa*) to explain the essence of socialist thought (*xa hoi hoa*),[60] the Viet Cong promised to return traditional political autonomy to the villages and make every farmer a landowner. Thus, for the villager, supporting the Viet Cong meant support for the organization's call for complete agrarian reform.[61]

Russell H. Betts also noted that the Viet Cong adopted traditional values. He recognized four action patterns among villagers:

[57] Wolf, *Peasant Wars of the Twentieth Century*, xiv.

[58] Simulmatics and ARPA, "Improving Effectiveness of the Chieu Hoi Program," 107.

[59] Raj Desai and Harry Eckstein, "Insurgency: The Transformation of Peasant Rebellion," *World Politics* 42, no. 4 (July 1990): 442–43.

[60] The verb *hoa* designates divine authority over land via man. The meaning of the word *hoi* is union. Thus, the concept of Socialism is perceived as a union between man and land, both bound and blessed by divine authority. See Christine White, "The Peasant and the Party in the Vietnamese Revolution," in *Peasant and Politics: Grass Roots Reaction to Change in Asia,* ed. Donald. B. Miller (New York: St. Martin's Press, 1979), 26; and Wolf, *Peasant Wars of the Twentieth Century*, 189.

[61] The Farmers' Liberation Association (FLA) was established according to Mao's legacy, which stated that villagers make up the prime force for the Communist revolution. Because villagers were ignorant as far as Communist theory was concerned, an organization with clear discipline was needed. For further information on the FLA, see Pike, *Viet Cong*, 167–72.

spontaneous, unorganized political activity; independent action; intentional political activity; and passive action.[62] Betts identified intentional political activity as the model for East Asian revolutions following WWII, which necessitated using an external police force to recruit villagers, unlike the revolutionary model in which leadership stems from within the group.[63] Although the magnitude of terror accompanying the police force employed by the Viet Cong cannot be overstated, it appears that personal interest and agrarian reforms remained important motives for enlistment[64] as villagers attempted to preserve their traditions; protect their land and family from social, economic, and cultural change; and improve their families' lifestyles.[65]

Just as male villagers aligned with the ideology promising the greatest likelihood of safety and economic security, Sandra C. Taylor identified similar personal reasons that motivated female enlistment in the Viet Cong among women as young as 15–17 years old.[66] Diverging from the Western concept of patriotism, villagers would pledge support to either the Viet Cong or the United States–South Vietnam based on the expected personal impact on the family's lifestyle from the evolving military and political conditions. For example, service in the South Vietnamese army meant being far from the village, and frequent military losses prior to U.S. involvement increased the likelihood that family members would experience physical or economic harm, thereby coercing villagers to side with the Viet Cong.[67]

[62] Russell H. Betts, *Viet Cong Village Control: Some Observations on the Origin and Dynamics of Modern Revolutionary War* (Cambridge: Massachusetts Institute of Technology, Center for International Studies, 1969), 1–15. The first part of this study attempts to create a general theory that would explain why villagers joined revolutionary movements. The second part offers a case study of a single village in South Vietnam.
[63] Ibid., 2–3. See also Shanin, "The Peasantry as a Political Factor," 19–21.
[64] Nathan Constantin Leites and Charles Wolf Jr., *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts* (Chicago: Markham, 1970), 41–45.
[65] Betts, *Viet Cong Village Control*, 7.
[66] Sandra C. Taylor, *Vietnamese Women at War: Fighting for Ho Chi Minh and the Revolution* (Lawrence: University Press of Kansas, 1999), 75.
[67] Richard C. Kriegel, *Vietnamese Attitudes and Behavior Related to Management Problems of the Revolutionary Development Program* (Washington, DC: Industrial College of the Armed Forces, 1969), 111, 113–15.

Beyond these reasons for enlistment, an ARPA study concluded young Vietnamese did not understand the essence of Communism, capitalism, or class warfare,[68] but Communist propaganda succeeded by translating the ideology into terms villagers could understand. As a result, many young Vietnamese realized the villages offered few opportunities for self-growth, and the Viet Cong promised development and economic security beyond rural life as well as a chance for self-fulfillment.[69] A 1964 Rand study affirmed that draftees largely misunderstood Communism and claimed to accept the political cadres out of Confucian tradition; even educated deserters professed that they could not elaborate on the meaning of Communism.[70] Kriegel and Pike explained that the Viet Cong counteracted this phenomenon by aggrandizing their commitment to the Vietnamese tradition of north–south unification. Additionally, the Communist movement promoted the singular cultural identity found in the nation's poetry, literature, and song to supersede the importance of a particular political ideology and to inspire the people to rally against the South Vietnamese government as they had against the French.[71]

Historically, the population abhorred the American-backed South Vietnamese government in Saigon due to the perception that it directly descended from the Diem regime that had replaced French colonialism. The ARPA study indicated that this perspective contributed to Viet Cong enlistment as villagers vowed to avenge family members killed and property damaged by government offi-

[68] Simulmatics and ARPA, "Improving Effectiveness of the Chieu Hoi Program." Communism was understood as an improvement in lifestyle and general welfare, mainly as a result of agrarian reform and distribution of land to be owned by the villager; the class war was understood to be a war against the city dwelling landowners associated with the central government. See Donnell, Pauker, and Zasloff, *Viet Cong Motivation and Morale*, 122.

[69] For similar reasons for enlistment among more senior members of the Viet Cong, see Ithiel de Sola Pool, "Political Alternatives to the Viet Cong," *Asian Survey* 7, no. 8 (August 1967): 555–57. These causes included the need for social and economic mobility, for a sense of nationality, to follow the footsteps of other family members who had joined, or for reparation for physical/economic damage brought about by French imperialism and subsequently the Diem government and its predecessors. These conclusions were also reached in other studies, making them unanimously accepted.

[70] Donnell, Pauker, and Zasloff, *Viet Cong Motivation and Morale*, 35–38.

[71] Kriegel, *Vietnamese Attitudes and Behavior*, 14–15; and Pike, *Viet Cong*, 2, 100.

cials and the military during South Vietnam's ascension to power.[72] Similar losses from U.S. air raids and personal problems within the family or with village institutions,[73] as well as previously mentioned economic and safety concerns, also motivated villagers to join the Viet Cong.

Despite these motivators and the years spent defending the nation from outside enemies, the nonmilitaristic nature of Vietnamese society placed professional soldiers on the bottom of the social ladder.[74] However, the traditional Vietnamese society's value of the family role explains why the villager, whose world revolved around the family and the rice field, would risk everything to join the Viet Cong.[75] An analysis of Chieu Hoi interviews of Viet Cong deserters shows that many Vietnamese joined the movement or government-led militias out of loyalty to a family elder or an authoritarian figure. In this manner, consistent with Confucian philosophy, political loyalty materialized from family loyalty; adversely, the possible dissolution of the previously mentioned Viet Cong threats against the family was also incentive to pledge political loyalty.[76]

One fact must be noted above all: the gravity of the causes for Viet Cong enlistment lies not with their accuracy, but with the PSYWAR components founded in them. In his study of PSYWAR, Barry Zorthian raised two important issues that architects of psychological warfare must address: attractive content convincing villagers of government responsibility for all aspects of economy, infrastructure, education, health, and security and corresponding field action.[77] A gap cannot exist between the two. Propaganda and information about hundreds of Viet Cong deserters disclosed during interviews

[72] Simulmatics and ARPA, "Improving Effectiveness of the Chieu Hoi Program," 115–20, also shares the stories of Viet Cong deserters who explained their affiliation with the organization as a response to their hatred of French rule and of the South Vietnamese and American governments who were seen as a direct continuance of the French regime.

[73] Ibid.

[74] Kriegel, *Vietnamese Attitudes and Behavior*, 13, 16.

[75] Simulmatics and ARPA, "Improving Effectiveness of the Chieu Hoi Program," 107.

[76] Leites and Wolf, *Rebellion and Authority*, 41–45.

[77] Barry Zorthian, "The Use of Psychological Operations in Combatting 'Wars of National Liberation' " (paper presented at the National Strategy Information Center Conference, 11–14 March 1971), 44–45.

illustrate Chieu Hoi's application of anthropological studies to meet these requirements and use the full force of PSYWAR.

As PSYWAR efforts explored ways to sabotage Viet Cong recruitment, military-sponsored studies named fear of death (as a result of American action), family concern (homesickness or economic loss),[78] harsh conditions, and loneliness as the main causes of desertion. Society's traditional value of family repeatedly emerged as the greatest Vietnamese justification for military allegiance. The U.S. Army found that most Viet Cong intending to desert the movement learned about the Chieu Hoi program from their families.[79] In essence, U.S. research clearly established that severing Viet Cong ties to the population required using the very means the organization used to persuade villagers to join them. From this perspective, a strategy to form a personal bond between families with members serving in the Viet Cong and government forces became the foundation for U.S.–South Vietnamese propaganda. Beyond the Vietnamese government's recognition of the importance of family ties in Vietnamese culture, efforts were made to expand communication channels between the government, family authoritarians, and potential Viet Cong supporters. As a result of the government filling the propaganda-action gap Zorthian introduced, Viet Cong loyalty decreased as most fighters turned to their families to prove or disprove PSYWAR information.[80]

Reviewing American propaganda pamphlets also pulled on the heartstrings of the Viet Cong fighter by showcasing American military superiority and introducing an alternative. One pamphlet displays an image of a B–52 bomber unloading its deadly cargo,[81] clearly conveying a Viet Cong fighter's sense of hopelessness and the message that he would be better off deserting. Another series of pamphlets displayed the economic distress of a fighter's family and their worry for their son fighting a losing battle.[82] The pamphlets

[78] Chandler, *War of Ideas*, 53, 54, 126, 132.

[79] See, for example, Leon Goure, *Inducement and Deterrents to Defection: An Analysis of the Motives of 125 Defectors* (Santa Monica, CA: Rand, 1968), 21, 30–31.

[80] J. M. Carrier and C. A. H. Thomson, *Viet Cong Motivation and Morale: The Special Case of Chieu Hoi* (Santa Monica, CA: Rand, 1966), 71–74.

[81] Chandler, *War of Ideas*, 47, 49.

[82] Ibid., 55, 63.

introducing the alternative, the Chieu Hoi Program, opposed the depictions of battle duress, homesickness, and American triumph with details emphasizing the improved conditions guaranteed to the deserter and his family.

The risk of relying exclusively on a person's family loyalty as the sole motivator for Viet Cong participation becomes apparent when considering desertion rates, which increased as American involvement grew and as a result of the Tet Offensive, when the Viet Cong desperately needed manpower.[83] The number of deserters joining local and rural militias as well as the U.S. Army Kit Carson Scout Program made this point even more pronounced.[84]

Sociolcultural Implications for Geopolitical Actions

Some critics of the conflict may say that since the United States lost the war in Vietnam, its wartime efforts were made in vain, which would be an overly simplistic and a misguided claim. Although North Vietnam dominated through the summer of 1968, U.S. forces significantly damaged Viet Cong political and military capabilities later that year. Research during the conflict provides examples of how the relationship between anthropological factors and Viet Cong culture affected military action. Likewise, studies during this period indicated that family served as the primary focus of Vietnamese society with individuals committed to psychosocial, physical, and economic defense of their relatives. Villagers commonly decided to join a military-political organization, not for ideological reasons but to protect the family from threats and improve their quality of life.

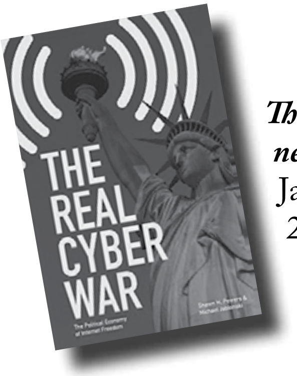
[83] In 1969, approximately 47,000 fighters deserted the Viet Cong, more than any other year of the program. For desertion data by year, see Chieu Hoi returnee figures by month, military region, and province in the National Archives, Record Group 472, Military Assistance Command–Vietnam, Civil Operations for Rural Development Support, Chieu Hoi Division files. Many declared themselves deserters to reap monetary benefits when, in fact, they were not. Still, the numbers are impressive. Generally, research on the Chieu Hoi Program claims that more than 159,000 Vietnamese deserted between 1963 and 1973.

[84] Named for famous American frontiersman BGen Christopher "Kit" Carson, these scouts were Viet Cong or North Vietnamese Army deserters hired by the U.S. Army. For more information on the program, see http://www.globalsecurity.org/military/world/vietnam/rvn-af-kit-carson.htm.

The Viet Cong used this knowledge as a means to wage war. Conversely, the U.S.–South Vietnamese Chieu Hoi Program realized that specific aspects of Vietnamese culture were a complicated, yet crucial part of their PSYWAR strategy. Thus, the anthropological perspective of intelligence gathering enabled both Viet Cong and U.S.–South Vietnam efforts to apply cultural perceptions to explain why and how the military conflict would progress as well as to develop systems of psychological warfare.

As governments around the world continue to learn from the cultures they interact with, a complete and thorough understanding of the enemy is impossible, but research can identify complex characteristics that prompt fighting patterns unique to each society. Leaders will come to realize that not only military prowess and economic power but also sociocultural aspects alter warfare. Therefore, the value of Lawrence's observations becomes evident in conjunction with Keegan's admonition that the essence of conflict cannot be understood via political considerations alone. Even operating according to the Clausewitzian paradigm, there is no doubt about the reciprocal influence of societal culture and military force on irregular warfare.

Book Reviews


THE REAL CYBER WAR
The Political Economy of Internet Freedom
Shawn M. Powers & Michael Jablonski

The Real Cyber War: The Political Economy of Internet Freedom. By Shawn M. Powers and Michael Jablonski. (Urbana: University of Illinois Press, 2015. Pp. 288. $95.00 cloth; $25.00 paper.)

The Real Cyber War says many things that need to be said. It is not, however, a book about war in the context of the use of force or armed attack. This title looks at the larger geopolitical competition between nation-states seeking to control the Internet and the information it carries as a resource. Authors Shawn Powers and Michael Jablonski closely examine concepts that guide American policy, such as Internet freedom and multistakeholderism. Rightly noted, the authors question if these ideas are based on outdated assumptions and cherished notions of politicos and technorati alike. This hypothesis will likely irritate some while providing a valuable discussion for all.

Political leaders understand the value of information and use it as a tool to advance their interests. Companies seek business models that extend economic control and market share. We do not want to presume that the frequent pronouncements about Internet freedom actually disguise a larger, conscious strategy of geopolitical control. Americans may believe what they say about the Internet even if foreign audiences do not, but consideration should be given to the possibility of actions driven by a simple incentive to maintain current advantages without being guided by a larger strategy. The United States may respond in a consistent manner to stimuli and incentives based on elite assumptions

JAMES LEWIS investigates the Internet and security at the Center for Strategic and International Studies. He previously worked on political-military and technology issues as a diplomat and a member of the Senior Executive Service.

about how the world and the Internet should work without necessarily pursuing a conscious strategy for geopolitical dominance. America's last "grand strategy" was articulated 60 years ago, and although future strategies have been a recurring quest for think tanks, efforts to develop a successor have been more comedic than useful.

In contrast, some foreign governments have explicit strategies to exert control over information resources. Challenges to America's global dominance emerged over the last decade, and the Internet is a key battleground. Specifically, Russia contests American dominance of the "information space" by creating global news outlets like RT and allegedly seeking to purchase the favors of European journalists. Although focused on controlling domestic information, China has also tried to create alternative structures by setting up organizations like the Confucius Institute to bring a Chinese point of view to foreign affairs. Similarly, the Al Jazeera Media Network challenges the monopoly of Western news outlets by promoting a Middle East perspective.

The limitation on these efforts is that, while it is easy to criticize U.S. motives, it is hard for an authoritarian regime with a taste for xenophobia to offer alternatives. Few people are going to sign up for the Chinese version of information access. The success of the authoritarian informational challenges comes from their ability to exploit the immense penchant for conspiracy theories that the Internet has unleashed.

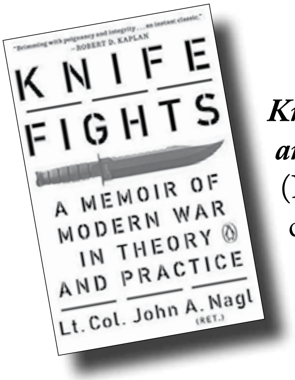
American interests have been damaged in this contest, but some of this is self-inflicted due to continually invoking ideas that no longer have much credence in the international community. The authors' examination of the multistakeholder model in chapter 5 is invaluable by positing the U.S. presentation of the multistakeholder model as a more representative and consensual approach to Internet governance. The authors identify a central flaw leading them to question American intent—the great majority of representatives are self-selecting, usually American, Westerners who use multistakeholderism to justify the status quo.

Having observed the creation of Internet governance, it struck this reviewer at the time as a blend of low self-interest and lofty millennial political goals—a kind of Northern California dream of becoming rich while doing good. Of course, this is nonsense as illustrated by the examination of Google provided in chapter 3. As the rest of the world has come to realize its dependence on the Internet and the control of American companies over this crucial infrastructure, they have begun a process of what the authors call "renationalization," rejecting an American dominated multistakeholder model for a more traditional approach to the collective governance of global resources based on state sovereignty and the United Nations.

Other chapters are less persuasive, shaped by dark concerns over U.S. National Security Agency surveillance and Googlenomics. Calling the giants of Silicon Valley an "Information Industrial Complex" where "government investment was critical to the industry's growth, and the industry's expertise was considered essential for the government's survival" is debatable (p. 72). Alternative explanations fit the data better; it is more likely that the government invested in information technology to preserve military superiority and companies took advantage of this investment to gain wealth. The authors recognize this conclusion in chapter 4, noting that economic motives rather than geopolitical strategy drive American policy.

America has become the land where secrets are not long preserved. If there was a strategy to create an ominous "industrial complex," we should be able to find primary evidence to confirm this, not a collection of remarks formed into a supportive aggregation. This methodological weakness becomes a problem in general for political science. Similarly, valuable observations are somewhat disfigured by being crammed into the structure and language of international relations theory.

These are criticisms of the field within which the authors labor, however, and not criticisms of the book. *The Real Cyber War* presents a new and valuable discussion of what can truly be called a geopolitical struggle and perhaps the most important war of our time.


"Brimming with poignancy and integrity . . . an instant classic."
—ROBERT D. KAPLAN
KNIFE FIGHTS
A MEMOIR OF MODERN WAR IN THEORY AND PRACTICE
Lt. Col. John A. Nagl (RET.)

Knife Fights: A Memoir of Modern War in Theory and Practice. By LtCol John A. Nagl, USA (Ret). (New York: Penguin Press, 2014. Pp. 288. $16.81 cloth; $13.46 paper; $11.99 e-book.)

In *Knife Fights*, the author of *Learning to Eat Soup with a Knife* creates an intimate description of the education, experience, and practice that contributed to his emergence as one of the premier voices advocating counterinsurgency (COIN) doctrine during the last decade. Nagl provides a warning to not forget the lessons we have learned at great cost. This book is for anyone curious about how military leaders assimilate experience, combine it with theory, and write about it to help leaders anticipate challenges. Readers should be warned that portions of this book are irreverent to the point of offending some, particularly senior leaders. After all, this memoir offers an unvarnished account from a warrior-scholar describing what it is like to advocate doctrinal change to a nation at war. Regardless of whether readers advocate COIN doctrine, *Knife Fights* provides an example of advocating for change while engaged in a close fight.

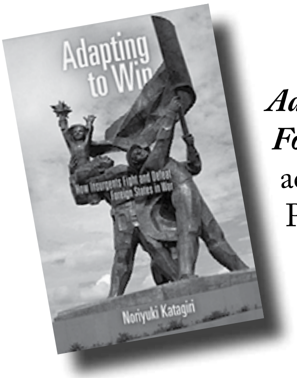
Engaging accounts in the first part of Nagl's book describe his early experiences at West Point, his first combat experience during Operation Desert Storm, and his studies at Oxford. These accounts depict that journey intertwined with the scholarship that laid the foundation for *Learning to Eat Soup with a Knife*. Although the author experienced classic conventional conflict during Desert Storm, he ultimately became interested in the ambiguous pursuits of COIN operations. At Oxford, Nagl came to believe that U.S. military leaders had walked away from counterinsurgency doctrine after Vietnam. In the author's view, this resistance to COIN operations constituted a hole in U.S. military doctrine waiting to be exploited by our enemies.

Nagl describes witnessing enemy exploitation of U.S. COIN ignorance during his second deployment to Iraq in 2004–5. The author found himself in the unenviable position of attempting to practice the theories he studied at Oxford against a thinking and adaptive enemy in Anbar Province. He also presents the difficulties military leaders faced because of the lack of planning for post-invasion operations. Namely, the demobilization of the Iraqi Army combined with senior leaders' refusal to recognize a developing insurgency created opportunities that insurgents exploited. These poignant descriptions will likely sound familiar to readers who experienced similar challenges and ambiguity while deployed in Iraq or Afghanistan.

Nagl provides a detailed analysis of the last 13 years of COIN theory and practice in the chapter titled "COIN Revisited," one of the most engaging portions of this book. Readers interested in understanding the positions of COIN advocates will find this section illuminating. The author provides detailed discussions of the importance of combat advisors in COIN and the necessity of language and cultural training to successfully accomplish these missions. Nagl asserts that, since most opponents cannot compete with conventional U.S. warfighting capabilities, future enemy offensives will rely on COIN strategies to engage U.S. forces. Therefore, American leaders who do not prepare for such a possibility do so at the peril of themselves and their country.

RICHARD A. McCONNELL, lieutenant colonel, USMC (Ret), is an assistant professor at the Department of Army Tactics, Command and General Staff College, Fort Leavenworth, Kansas. McConnell earned his bachelor's degree in history from the University of Wisconsin and his master's degree from Webster University. His most recent work on critical thinking in professional military education earned a Silver Pen Award from the U.S. Army Command and General Staff College.

Knife Fights provides a window into the education, experiences, and leader development of a warrior scholar through two different conflicts over as many decades. Few senior American leaders predicted the challenges resulting from the events commencing with the 11 September 2001 terrorist attacks and transpiring over the last 13 years; however, according to Nagl, the United States should have anticipated the challenges associated with combating an insurgency and prepared for them by maintaining COIN doctrine, training, and leader development after Vietnam. Since U.S. forces assumed they would never engage in COIN operations after that conflict, the events resulting from 9/11 were not anticipated. Likewise, U.S. leaders can ill afford to repeat this mistake by discarding the COIN lessons bought with the sweat and blood of America's military. Should U.S. leaders abandon these teachings again, Nagl's book could serve as a great primer for relearning and rewriting COIN lessons. Whether an advocate or opponent of COIN doctrine, *Knife Fights* is definitely worth the read for military and civilians alike.



Adapting to Win: How Insurgents Fight and Defeat Foreign States in War. By Noriyuki Katagiri. (Philadelphia: University of Pennsylvania Press, 2014. Pp. 312. $69.95 cloth and e-book.)

Noriyuki Katagiri is well published in the field of insurgency studies, having written about cases involving the Philippines, Vietnam, Malaysia, Britain, France, and Portugal. He teaches at the U.S. Air Force's Air War College in the Department of International Security.

Katagiri's *Adapting to Win* addresses an intriguing and enduring conflict studies issue: how does a substantially weaker power defeat a militarily dominant foe? It defies logic that small insurgencies have the capacity to survive losses on the battlefield, lack of funding, and basic materiel support to overcome stronger powers. Before 1945, the insurgents usually lost such struggles with only a 15 percent chance of success, but since that time the insurgents' odds of being victorious improved to 61 percent (p. 9). Katagiri's research investigates why this is the case. Military planners increasingly accept that such conflicts as Operation Restore Hope (Somalia) and Operation Iraqi Freedom are norms in the post–Cold War order and not aberrations. If so, how can the United States mitigate the growing success of insurgencies they are likely to encounter in the near future?

MATTHEW R. SLATER, PhD, is a plans and policy analyst for Marine Corps University's Center for Advanced Operational Culture Learning.

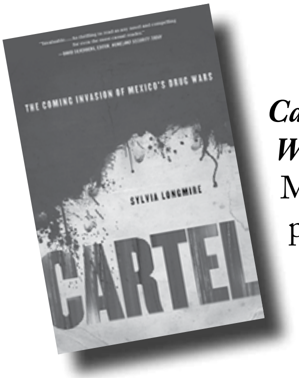
The author begins with a well-documented literature review on the potential reasons for weaker-power battlefield success. Several theories are reviewed, including the impact of mechanization, the duration of conflicts, and external democratic influence. One theory posits that increased mechanization divorces stronger opponents from knowledge about local populations, contributing to an inability to win hearts and minds (p. 16). Given that an average conflict lasts 2.7 years and, since 1945, they increased to 7 years (pp. 10–11), influential author David Galula argues that the greater the duration of an insurgency, the more likely the insurgence will be a success. Other research focuses on the negative domestic influences of democracies to end wars before stronger powers subdue weaker opponents (p. 15).

Katagiri then applies his own unique methodology by using sequencing theory to explain weak power success. He articulates sequencing theory as a combination of Darwin's concept of natural selection with Jean-Baptiste Lamarck's ideas about the inheritance of acquired characteristics. Katagari asserts that insurgent groups successfully fight more powerful adversaries through variation, selection, and replication (p. 25). Lesser powers are forced to innovate for survival (variation), where initially only the strongest survive (selection), and after extended fighting the remaining elite insurgents apply their hard-won experience of learning and innovation to the battlefield (replication). These qualities are expressed over three phases: guerilla warfare, state building, and conventional warfare. If the weaker power is able to properly sequence the conflict to avoid conventional fighting until it has built sufficient strength, then it dramatically increases its odds of winning.

In the application of sequencing theory, the author identifies and labels six patterns that insurgencies seem to follow: conventional, primitive, degenerative, premature, Maoist, and progressive (p. 49). The bulk of *Adapting to Win* addresses one model per chapter while categorizing 148 insurgencies dating back to 1816 that follow these six models. The conventional model explains 63 percent of insurgencies according to Katagiri, and over time insurgents only won 19 percent of the conventional model conflicts (p. 61) because they made the mistake of going "toe-to-toe" with the larger power rather than adjusting their strategy to their relatively weaker position. When insurgents use the Maoist or progressive models, their chances of success increase to 80 and 100 percent, respectively. The sequencing is different for historical case studies, but the conventional war phase must always follow state building if the insurgents want to be triumphant. The author points out the logic of this fact by stressing that a conventional war requires significant economic, political, and social resources.

The framework provided by Katagiri to assess insurgencies helps the reader break down a very complex topic. In some ways, his hypothesis is very similar to the three phases of Maoist guerilla warfare philosophy: strategic defense, strategic stalemate, and strategic offense that target elites, security forces, and the entire nation, respectively. However, Katagiri's sequencing is dynamic, while Maoist doctrine suggests just one method for success. In reality, the goals of each approach are different. Katagiri attempts to assess the relatively recent success of weak powers as opposed to prescribing a template for insurgent success.

The author provides the reader with a well-researched and unique perspective on how weaker opponents are increasingly likely to win conflicts in the modern era. *Adapting to Win* provides a thought-provoking thesis that should be read by both warfighters and U.S. policy makers to better understand how current and future adversaries are "adapting to win."



Cartel: The Coming Invasion of Mexico's Drug Wars. By Sylvia Longmire. (New York: Palgrave Macmillan, 2011. Pp. 248. $26.00 cloth; $17.00 paper; $9.99 e-book.)

Sylvia Longmire's *Cartel* offers an overview of Mexican organized crime modus operandi and explains why the cartels are the current major threat to the national security of the United States. The book is relevant to all Americans who want to understand the complexity of illegal drug consumption in the United States, the violence of the Mexican drug war, and how these combined challenges pose serious risks for the entire country, not only to the Southwest border states.

The author has followed Mexico's cartels for years as a senior intelligence analyst on drug trafficking and border violence for the state of California. In *Cartel*, her vast national security experience is presented in a well-thought-out blend of real-life examples, relevant background information, important facts and hard data, insightful analysis, and suggestions for policy makers.

Longmire's main goal with *Cartel* appears twofold. First, she brings awareness to the general public of the dangers of what she calls "cartel infestation" in the United States. Second, she provides real policy recommendations to those in charge of leading border security and other agencies involved in keeping the public safe.

The author successfully draws readers' attention to key topics by bringing the human factor to the main stage through both real events and hypothetical situations involving victims, criminals, or law enforcement agents. From a single realistic scenario, Longmire effectively makes the connection to the broader issue covered in a chapter, bringing a vivid image that stays with the reader. For instance, in chapter 8 the author describes in detail a nearly fatal encounter between a border patrol agent and human traffickers.

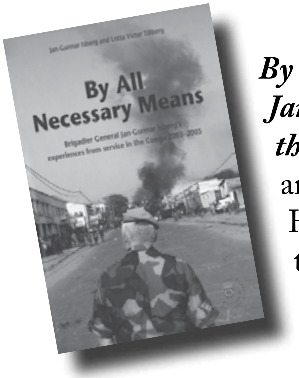
Longmire makes the point that most of the hundreds of methamphetamine labs in the United States are run by Mexican cartels. She calls special attention to the fact that most of these labs are located in states hundreds of miles away from the Southwest border. Similarly, the author describes how the Mexican cartels grow millions of dollars' worth of marijuana in U.S. parks and forests nowhere near the border with Mexico. In both cases, the author explains the risks to the general public as a result of these illegal activities, the violence associated with them, and the strain on already limited resources. U.S. Forest Service and National Park Service agents are particularly ill prepared to deal with heavily armed Mexican marijuana growers on U.S. soil.

Longmire provides a detailed analysis of the highly polarized debate on firearms and gun control laws intermingled with drug trafficking and cartel violence south of the border. She points out that as much as 80–90 percent of firearms used by the Mexican cartels are bought legally in the United States by straw buyers and subsequently smuggled illegally across the border into Mexico by the cartels. The author provides fuel for the debate by citing such data as "2005 ATF [U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives] inspectors documented 113,642 missing guns from only 3,847 inspections" (pp. 196–97). Considering that there are 115,000 firearms dealers due for inspection by only 600 inspectors, the actual average is 1 inspection per dealer every 10 years (p. 197). The author offers several policy recommendations on this issue, such as "don't saddle the ATF alone with prevention of southbound weapons trafficking" (p. 198).

DENISE U. SLATER is a researcher and Latin America subject matter expert for the Regional, Culture, and Language Familiarization Program within Marine Corps University's Center for Advanced Operational Culture Learning.

Finally, the author defines drug decriminalization and drug legalization, and she reviews the pros and cons influencing her opinion. This heated political debate is currently occurring across the entire Western Hemisphere. The contradictions remain as more than 20 U.S. states have legalized medical marijuana, and 3 states have legalized its recreational use, even as the drug war remains a central priority of U.S. policy in Latin America.

Cartel is an important title that brings clarity to a serious issue often mistakenly considered relevant only to the states along the border with Mexico. The author successfully exposes the risks that the Mexican drug cartels pose to U.S. national security.



By All Necessary Means: Brigadier General Jan-Gunnar Isberg's Experiences from Service in the Congo 2003–2005. By Jan-Gunnar Isberg and Lotta Victor Tillberg. Translated by Stephen Henly. (Skurup, Sweden: Swedish Military History Library, 2012, Pp. 240. Cloth.)

In 2000, the United Nations Organization Stabilization Mission in the Democratic Republic of Congo (MONUSCO) began deploying military forces to the Congo to oversee the implementation of the Lusaka Ceasefire Agreement and the end of the Second Congo War. By 2003, low-level ethnic fighting between Lendu and Hema militias was still taking place in the Congo's newly created Ituri Province, stoking fears of another genocide similar to that which occurred in nearby Rwanda. That June, the United Nations (UN) launched Operation Artemis, a European Union–led military mission into the province to provide short-term stabilization. Operation Artemis ended in September 2003 and handed responsibility for security in Ituri Province over to MONUSCO. MONUSCO established a multinational Ituri Brigade in Bunia, the capital city of Ituri, with forces from Uruguayan, Bangladeshi, Nepalese, and Pakistani infantry battalions. Brigadier General Jan-Gunnar Isberg of the Swedish armed forces was given command of the Ituri Brigade. General Isberg had extensive command experience in UN-sponsored peacekeeping operations in Cyprus, Lebanon, the Balkans, and Afghanistan prior to his deployment to the Congo.

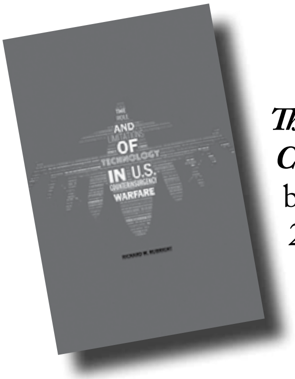
PAUL WESTERMEYER is a historian with Marine Corps History Division at Marine Corps University in Quantico, Virginia. He is the coeditor of *Desert Voices: An Oral History Anthology of Marines in the Gulf War, 1990–1991* (forthcoming) and author of *U.S. Marines in the Gulf War, 1990–1991: Liberating Kuwait* (2014) and *U.S. Marines in Battle: Al-Khafji, 28 January–1 February 1991* (2008).

Written originally in Swedish as a textbook for the Swedish National Defense College, *By All Necessary Means* creates interest not only by its structure and style, but also through the unique perspective presented as part memoir, history, and political science case study. The first four chapters cover Isberg's experience in the Congo, how he was chosen to command the Ituri Brigade, and the operations he conducted during the Bakavu crisis and in Goma and Kivu. Occasionally, first person transcripts of interviews between Isberg and his coauthor, Lotta Tillberg, appear to break up the narrative chapters. Of particular interest in the narrative, Isberg describes working with various nationalities, seeing some of his command accused of war crimes, disarming child soldiers, and interacting with local rebel and military commanders, including some that shifted sides in the midst of the crisis.

Forming the penultimate chapter of the work, a compilation of essays and study guides extracts lessons from the narrative and explains how those lessons apply to the strategic and tactical levels of war. This chapter also includes an essay detailing Isberg's final reflection on his time in the Congo. Tillberg presents a case study as the final chapter to "highlight military professionalism from an epistemological perspective" (p. 195). She examines specific problems Isberg encountered during his tour and delineates the situations according to her theory of military professionalism, supporting her arguments with snippets of interviews conducted with Isberg and breakout descriptions from the previous narrative. The book concludes with appendices describing the history of the Congolese conflict as well as defining abbreviations and terms employed throughout the text.

Isberg's narrative is well written and clear, although the work's structure can be confusing. The topic and author are unique; many Americans have experience working with indigenous groups and multinational military forces, but very few have held command over a large UN force. The blue-helmeted peacekeeper perspective certainly needs better study in the United States. Tillberg's contributions are interesting and provide a window into the advanced military education of Sweden. Unfortunately, this purpose also seems to be the primary cause for the confusing structure. While primarily a memoir, the work nonetheless includes significant citations to relevant documentation, both as footnotes and in the text.

The Second Congo War and its aftershocks have ravaged central Africa for nearly three decades, millions have died, and yet this "African World War," as many term it, is little known in the United States. The causes and course of the massive conflict are exceedingly complex, and Isberg's memoir can only explain a small portion from his few years in one province. Nevertheless, an in-depth look at one small portion of a massive conflict is extremely useful as details and complexity become blurred when one tries to understand the war as a whole. Although fairly rare in English, Isberg's book serves as an excellent resource for anyone trying to better understand the crisis in modern Africa.



The Role and Limitations of Technology in U.S. Counterinsurgency Warfare. By Richard W. Rubright. (Lincoln, NE: Potomac Books, 2015. Pp. 296. $36.95 cloth.)

In *The Role and Limitations of Technology in U.S. Counterinsurgency Warfare*, Richard Rubright presents a carefully researched and insightful consideration of how technology can enhance U.S. counterinsurgency success. His observations, while upholding his stated purpose to address a historiographical gap, also stand as authoritative recommendations for the improvement of American counterinsurgency strategy. A compelling combination of evidentiary interviews and personal experience support Rubright's claim that the U.S. military "must consider technology in both strategic and tactical counterinsurgency terms" to successfully participate in future counterinsurgency operations. Rubright also asserts that professional political leaders should be more familiar with "strategic considerations," while military officials should appraise conflicts honestly (p. 232).

Rubright reiterates these essential facts by generating a persuasive, authoritative, and thought-provoking treatise. He begins by introducing relevant concepts, including a valuable definition of technology as an "enabler of capability" (p. 20). He describes the historiographical setting of his work and illustrates that, while useful, the literature rarely presents a viable solution to strategic counterinsurgency problems. In this context, Rubright highlights the gap that his work is designed to fill—combining a scholarly discussion of counterinsurgency strategy with the kind of technological dimension that the literature has heretofore been lacking (pp. 12–24). A firm discussion of theory follows, where Rubright occasionally risks repeating himself to the point of redundancy, but the result is a solid explanation of his rationale and a clear introduction of important concepts. Subsequently, the author emphasizes a distinction between technology and strategy, arguing that technology itself cannot be thought of as a strategy or an acceptable substitute for one. Instead, the capabilities that technology provides must be balanced with elements of the contextual environment, such as the political situation. As a result, the application of technology can only enhance strategic advantage not create it, and strategy must be "made responsive to political objectives at all times" (p. 17).

Key to Rubright's argument is the concept discussed in chapter 7 of an "operationally offensive, tactically defensive" counterinsurgency strategy. This strategy "blends the audacity and initiative of an offensive operation" with the "inherent strengths of a defensive mode of modern warfare" (p. 25). However, the author makes the case that, while "technical capability allows for enhanced defense," it is not always effective. He illustrates a number of historical situations where superior technological capability did not provide an overwhelming advantage to even more numerous forces and where reliable strategies were not effectively fused with the capabilities available (pp. 28–60).

PHILIP SHACKELFORD is a graduate teaching assistant in the Department of History at Kent State University. He recently presented a paper titled "Flying High: The U.S. Air Force Security Service and Its Rise to Prominence in the U.S. Intelligence Community" at the 82d Annual Meeting of the Society for Military History. He is currently researching the U.S. Air Force Security Service in connection with Cold War intelligence and national security.

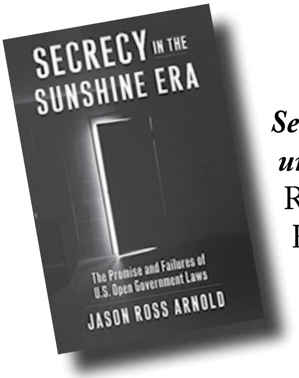
As a result, Rubright illustrates that if the U.S. military applies "proper advantage of the technical capabilities of existing force structure" and the potential of emerging technologies to the operationally offensive, tactically defensive concept, they would provide the "tools at the strategic level for policy makers to feel more comfortable" with counterinsurgency warfare (pp. 60–61). He believes the failure of the military to anticipate and prepare for a tenacious insurgent reaction to conflict is one of the primary downfalls of U.S. counterinsurgency strategy thus far. Using a potentially overdeveloped discussion of counterinsurgency in Iraq to illustrate this point (pp.

67–101), Rubright clearly explains the consequences of failing to adapt quickly, implementing poor policy decisions, hesitating in the application of political leadership, and failing to effectively protect the center of gravity—the civilian population (pp. 90–96).

Pointing out the "limits of politically correct doctrine" in counterinsurgency, the author argues that the political environment is crucial. When faced with an overwhelming insurgency, the options available to the U.S. military, according to Rubright, are withdraw, redefine political objectives, or pursue unrestricted tactics that will result in heavy casualties and a pressurized political environment. Of these, he stressed that only the first two are acceptable since the "only effective end state will be achieved through political considerations with the help of military capabilities" (pp. 103–31).

These contextual recourses affect the implementation of a successful counterinsurgency strategy, but Rubright points out that the U.S. military should be prepared to fight any type of conflict. His subsequent discussion of coalition partners, domestic support, and third-party intervention notwithstanding, Rubright arrives at a point in chapter 4 that effectively summarizes his entire argument—"integration of technology, solid civilian guidance, and a break with rigidity in force structure are required to leverage technology appropriately to apply an operationally offensive, tactically defensive concept to counterinsurgency warfare" (p. 172). This statement would have been well suited for his conclusion in light of the slight digression of contextual influences presented in chapter 5.

Overall, the book's effective organization supports a significant and timely evaluation of technology and counterinsurgency applications relevant to current debates and trends. Rubright's thoughtful consideration of the role of technology in adding a competitive edge to counterinsurgency warfare identifies what will be necessary to reinforce the U.S. military.



Secrecy in the Sunshine Era: The Promise and Failures of U.S. Open Government Laws. By Jason Ross Arnold. (Lawrence: University Press of Kansas, 2014. Pp. 560. $39.95 cloth.)

It appears that the era of sunshine never arrived. Author Jason Ross Arnold does a great job of demonstrating that, despite the groundswell of support in the 1970s toward making government more open and transparent, the ideal environment has not arrived. Over the last 45 years, many presidential administrations have made big commitments to greater transparency by promising the wonders of life in a world full of sunshine when in reality it was no more than lip service.

Why do Sunshine Laws that protect public rights to attend meetings and access government information even matter? *Well, in a world without government disclosure and transparency, accountability is dead.* In the absence of information about what happened, we *the people* can make no judgments about whether the government did well or poorly; there is, therefore, no opportunity for accountability to occur.

MAURICE P. McTIGUE of the Queen's Service Order is currently vice president for outreach at the Mercatus Center at George Mason University. He was director of the Government Accountability Project for 10 years. Prior to joining Mercatus, McTigue was a member of the New Zealand Parliament for nine years and held eight different positions in the New Zealand cabinet. After leaving Parliament in 1993, he was appointed New Zealand's ambassador to Canada and ambassador to the Caribbean. He joined the Mercatus Center in 1997, where he still works on improving the quality of governance in the United States.

Arnold efficiently organizes vast quantities of information into digestible chunks of information so that, concept-by-concept, we develop an informed view of the causes of transparency failure. As the author fairly and comprehensively builds the argument for governments to keep some information secret, we can follow that logic. But then, as he dives more deeply into classified information, we get feelings of disquiet about whether the spirit of the law is being followed. For example, it is a little hard to accept that the Defense Department still insists on retaining secrecy classifications for documents generated in 1917.

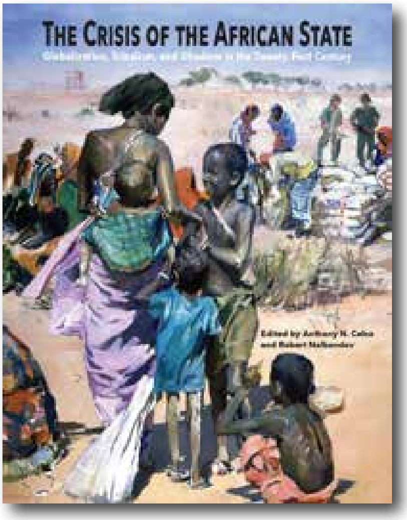
As the author moves into freedom of information issues for materials that do not have a security link, it becomes even more difficult to pretend that the spirit of the Sunshine Laws is supported by U.S. government culture. It appears that the motive for secrecy in many cases is to protect the administration or its officers from critique should the information be made public. Surely, the intention of Sunshine Laws was to do exactly that—make governments and individuals accountable for their performance. This reader can only hope that the exposé this book provides will shame those in authority into providing much more robust mechanisms for prosecuting breeches of these important transparency laws.

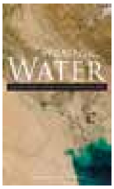
Through Arnold's narrative, it also becomes apparent that a great expansion of secrecy may occur in this era of terrorism and heightened security. Of particular concern, the author contends that those in public office who favor a more Delphic government seize opportunities to frighten the public into accepting increased secrecy as the price for greater personal safety. However, as the author points out, additional secrecy may not improve our safety. In fact, we may indeed be further endangered if the information demonstrating that the government is not doing enough to maintain public safety remains hidden.

Of equal concern, Arnold discloses the level of secrecy surrounding the scientific community. While we can accept that some scientific discovery may have strategic implications and needs to remain secret, we can also accept that other scientific information could cause public panic. The government's practices that limit information become increasingly difficult to accept in light of the quantity of mundane information shrouded in secrecy. After all, knowledge is the device that we use to protect ourselves from danger, but in some cases, delayed access to that knowledge increases the danger. For example, belated access to new drugs and information on dangerous products or services prevents *the people* from making informed choices for self-protection. An issue this reviewer had not considered prior to reading this book is that the government may freeze patents and deny people access to improved products or processes that would enhance personal well-being or would cause detrimental effects on economic growth.

While the author does a good job quantifying the breadth of the secrecy problem, the inability to subjectively identify best- and worst-case scenarios becomes evident when one considers that retaining a large amount of information in one case may not lead to harm, whereas retaining a small number of pages in another case could lead to significant danger. As an example, if President Richard M. Nixon had been able to suppress Watergate information, great harm would have occurred. Likewise, Arnold posits that no administration since 1970 has fulfilled their many promises.

The author devotes considerable space to potential solutions for sustained government secrecy—and there have been an abundance of inquiries for information to be made public over the last 45 years—but by no stretch of the imagination could we claim that the United States has an open and transparent government. It seems to this reader that government culture contributes to the issue of limited access to information and, until the culture of all those working in government changes to a belief that all information should be public—unless there is a compelling reason for it to remain confidential—the progress of transparency will be slow or nonexistent. *Secrecy in the Sunshine Era* is a must read for policy makers and aspiring politicians, but it remains to be seen if they will take the time to become better informed because they understand that the absence of transparency prevents *accountability*.


THE CRISIS OF THE AFRICAN STATE
Globalization, Tribalism, and Jihadism in the Twenty-First Century
Edited by Anthony N. Celso and Robert Nalbandov


WATER

CHINA'S EMERGING NATIONAL SECURITY INTERESTS

JOURNAL

MCUP
MARINE CORPS UNIVERSITY PRESS

www.mcu.usmc.mil/mcu-press