CTX

From the Editor

Happy New Year, everyone. As I write this, we're a few weeks into 2021 and there are sparkles of hope here and there that this year may be an improvement over the seemingly endless disasters of the last one. Vaccines are finally being deployed against the coronavirus, although how fast and for whom remain big sticky questions. The United States seems to have survived a political crisis that brought its system of democratic government to the edge of chaos. The endless conflicts in Syria, Libya, Yemen, Iraq, and Afghanistan aren't over by any means, but they have evolved—devolved?—once again into chronic civil agony instead of multinational warfare.

2021 is also the tenth anniversary of the Arab Spring, a moment when the world held its breath while citizens of countries across North Africa and the Arab Middle East rose up against corrupt authoritarian governments in a bid to end chronic poverty, oppression, and inequality. However, despite the initial burst of change and hope that swept so many countries, we still see entrenched strong-arm rule, calcified political structures, and stagnant stratified economies.

And where have all the terrorists gone? Not far, that's for sure, even if the pandemic has kept many of them off the streets lately. Closed borders and city-wide curfews may have helped limit the operational scope of ISIS, Lashkar-e-Taiba, al-Qaeda, and the like for the time being, but we know the teeming refugee camps of Syria are busy producing the next generation of violent ideological extremists. Meanwhile, other groups such as al Shabaab and Boko Haram have continued their depredations, and random bomb attacks by the Taliban—in the midst of "peace negotiations"—are making life in the city of Kabul increasingly perilous for residents and visitors alike.

So, the endless work of trying to make the world a better place amid hope and fear continues.

This issue of *CTX* begins with an analysis by Command Sergeant Major Thomas Myers. He tackles Irregular War theory and the confusion that can arise when we misuse terminology to describe and understand the kinds of conflicts that are being fought today. His contention is that a common frame of reference is

required for military theory to be useful to the operator, and that this frame of reference needs to be grounded in doctrine.

Next is a look at how SOF can use its unique skillsets to support both defensive and offensive cyber operations in contemporary hybrid conflict and counterterrorism operations. Using the Netherlands' efforts to create a SOF-cyber unit as his example, Major Jonas van Hooren describes three possible configurations at the organizational level, and also warns about some of the obstacles and pitfalls that might cause such efforts to fail.

Our third feature is an unusual study of radicalization as it has unfolded in recent years in Pakistan. In a series of interviews conducted by a Pakistani national over about a year's time, a broad selection of respondents from throughout Pakistani society discuss what they believe to be the foundations of radical sectarianism and "jihadi culture" in their country. With just a few light analytical touches, Dr. David Belt lets the interviewees speak for themselves. Both the interviewees and the interviewer remain anonymous to protect them from possible repercussions.

For the Ethics and Insights column, George Lober continues his ruminations "On Truth, Lies, and Loyalty," which he began in the previous issue of *CTX* (vol. 10, no. 2, Summer 2020). Lober first distinguishes between ethical and moral choices; then, using the 2015 Danish film *A War* as the basis for his discussion, shows how difficult it can be to make moral and ethical judgements about decisions taken in battle. When a choice has to be made, whose lives will matter the most?

We have two book reviews for you in this issue. First, Chief Warrant Officer Rick Manley reviews *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* by Audrey Kurth Cronin. Cronin uses a framework of actors and interests to evaluate contemporary approaches to counterterrorism and, as Manley points out, makes a compelling case that strategies of compellence rather than leverage are doomed to fail over the long run. Then, Major George W. Bailey reviews *Blood in the Fields: Ten Years Inside California's Nuestra Familia Gang* by Julia Reynolds. Bailey recommends the book for its descriptions of prison gang culture, recruitment, and indoctrination, which he feels will help CT professionals better understand the internal dynamics of terrorist organizations.

Check out the new book by Dr. Glenn Robinson, *Global Jihad: A Brief History*, on our publications page. You can also read an article based on a chapter of the book in the Summer 2020 issue of *CTX* (vol. 10, no. 2).

Stay in touch with Global ECCO on Facebook. Send your article ideas and drafts to CTXSubmit@GlobalECCO.org. You, the professionals of the global CT community, are what make *CTX* unique and valuable, and we rely on you to let us know how we're doing. Meanwhile, stay healthy, and may we all enjoy a peaceful, happier spring.

Elizabeth Skinner
Editor, *CTX*

Inside

ABOUT THE CONTRIBUTORS

Major George W. Bailey is a US Army Civil Affairs officer who has served in Afghanistan and deployed throughout the Middle East. He recently earned his master's degree in Defense Analysis (Irregular Warfare) and a Certificate in Middle Eastern Regional Security Studies from the US Naval Postgraduate School (NPS), Monterey, California. He is currently pursuing a master's degree in computer science at Johns Hopkins University.

Dr. David D. Belt is a professor at National Intelligence University, Washington, DC, where he specializes in the social analysis of strategic-level security issues emerging from global Islamist movements worldwide. Previously, Dr. Belt was an assistant professor of National Security Studies at National Defense University, where he developed and taught the university's first national security professional certified course on countering violent extremism. He served 26 years in the US Navy's Special Operations Officer community (non-SEAL) before retiring with the rank of captain.

George Lober retired as a senior lecturer from the Defense Analysis department of NPS in 2016. Prior to his retirement, he initiated and instructed a course in Critical Thinking and Ethical Decision Making.

Major Jonas van Hooren began his military career in 1998. After completing the Royal Marine Mountain Leader course in the UK and officer training in the Netherlands, he conducted combat tours in Iraq, Afghanistan, and Pakistan between 2003 and 2006. MAJ van Hooren was in charge of the Centre of Excellence Military Operations for extreme conditions; he later commanded the international squadron of Maritime Special Operations Forces (MARSOF) and led a Combined Joint Special Operations Maritime Task Group. Currently, he is head of future plans at the MARSOF HQ in the Netherlands. He holds a BS degree in economics and an MS in Defense Analysis (Irregular Warfare) from NPS.

Chief Warrant Officer 3 Rick Manley is a 16-year member of the US Army Special Forces Regiment. He has had numerous operational deployments to the CENTCOM theater in support of contingency operations, as well as significant operational time spent in or focused on the USINDOPACOM region. He is currently pursuing a master of science degree in Defense Analysis (Irregular Warfare) at NPS.

Command Sergeant Major Thomas Myers currently serves as the Senior Enlisted Leader for the US Army's International Special Training Center, Pfullendorf, Germany. He has served more than 20 years in the US Army Special Forces. CSM Myers holds a master's degree in intelligence studies and a certificate in ancient and classical history from American Military University.

COVER PHOTO

Ukrainian and Polish people protest against Russian military actions on the Crimean Peninsula during a pro-peace demonstration in front of the Russian Embassy, Warsaw, 2 March 2014.
WOJTEK RADWANSKI/AFP via Getty Images

DISCLAIMER

TERMS OF COPYRIGHT

Irregular War Is Revolutionary

CSM Thomas Myers, US Army

"Liiberté Guidant le Peuple" ("Liberty Leading the People"), by Eugène Delacroix, 1830.

Anyone setting out to study or discuss rebellions of this sort at once runs into semantic difficulties, for many terms are used which, while largely synonymous, have come to mean different things to different men.

James Elliot Cross, *Conflict in the Shadows*[1]

IN 2010, AFTER DECADES SERVING IN SPECIAL OPERATIONS forces deployed throughout Africa and from the Balkans to the Middle East, I wrote a paper about the use of terrorism as a tactic in revolutionary change.[2] The paper predicted that the next phase of unrest in the Middle East would be mass civil uprisings, revolution, and civil war; fittingly, the paper was published in February 2011, at the height of the Arab Spring. USSOCOM's priority at the time was combating terrorism. But terrorism is a tactic, and the issues presented by instability in that region require a response that counters the strategic problem of widespread revolution. I have also noticed a great deal of misunderstanding among my SOF students about how to apply doctrine to current conflicts. US irregular war (IW) doctrine is inadequate because it fails to adequately address revolutions. By merging revolution theory with US doctrine, I have developed a logical and straightforward process to understand IW that may provide clarity not only for US SOF planners but also for US allies and partners.

In his article, "Do We Really Understand Unconventional Warfare?," David Maxwell wrote, "In the twenty-first century we are more likely to experience kinds of warfare for which scholars have been hard-pressed to find a name."[3] Due to either discontent with or the misunderstanding of doctrinal terms, theorists and practitioners continually invent new names for old ideas or reinterpret old names in new ways. In this era of integrated campaigning, it is crucial for military staff personnel, particularly those working in the combatant commands and

theater special operations commands, to understand the concepts associated with IW. It is equally important that, as often as possible, the academic community construct theoretical work in a manner that is useful to the practitioner. This paper attempts to bridge theory and practice to create a shared understanding between multinational operational staffs and the academic community about how to define IW and the conditions that lead to it.

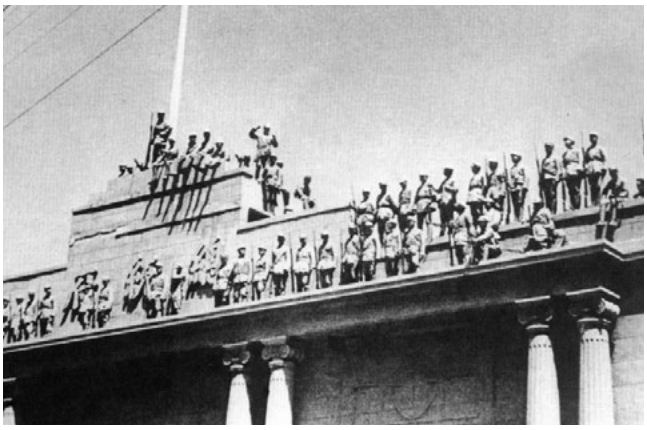
Doctrine, an often-reviled word in the military lexicon, "establishes a common frame of reference."[4] Non-doctrinal terms such as "gray zone," "asymmetric warfare," and "hybrid warfare," if not associated with such a standard frame of reference, add unnecessary confusion. Such non-doctrinal terms may serve to expand and explain concepts, and thus help to create a shared understanding with allies and interagency partners who are not tied to the same lexicon. However, using terms in the proper framework will differentiate doctrinal from non-doctrinal terms, placing each in the appropriate context.

"Revolutionary War is a Political War"[5]

The term "political warfare" was coined by George Kennan, a foreign service officer who worked in the US Embassy in Moscow during WWII and later served as US ambassador to Yugoslavia. Kennan defined political warfare as "the logical application of Clausewitz's doctrine [war is the continuation of policy with other means] in time of peace."[6] He proposed conducting political warfare "to maintain contact with, sustain, and influence underground movements in the soviet world resisting Kremlin domination," and "to strengthen indigenous forces combatting communism in countries where soviet political warfare is a threat to our national security."[7] Many military professionals, however, dislike the word "political" because it insinuates interference and restrictions on operations; the word "warfare" is oftentimes offensive to diplomats and politicians because it represents the failure of diplomacy or other means of conflict resolution. Perhaps the most salient objection to the term political warfare is that all wars have political objectives; warfare itself, therefore, is political.

> **All wars have political objectives; warfare itself, therefore, is political.**

This article uses the term political warfare as described by Kennan for four reasons. First, there is not yet a better term to describe these types of conflict. Proposed replacements such as "unconventional statecraft" or "effective statecraft," have not taken hold and attract equal amounts



In April 1949, near the end of the Chinese Civil War, the People's Liberation Army forces captured Nanjing and the Presidential Palace.

of disagreement.[8] "Great power competition" is not sufficient because it leaves out both smaller powers and non-state actors, and because the term "competition" does not necessarily involve violence. Second, "political" refers to both leadership and objective. If it is not directly led by civilian agencies, political conflict should be at least closely coordinated with them. The term also reminds the military that there are considerations in war beyond kill/capture. Third, "warfare" reminds diplomats and politicians that involvement of the military generally equates to militarily decisive tasks such as destroy, neutralize, and so on. If combat ensues, someone is at war. While the protagonists may not be Americans (it may be an ally or partner doing the fighting and dying), warfare nevertheless is underway. Finally, this type of conflict, by necessity, involves political legitimacy. The defender is fighting to maintain legitimacy and, thus its hold on power; the attacker seeks to undermine the defender's legitimacy while building its own.

For the United States, the application of violence in pursuit of national policy objectives is the responsibility of the Department of Defense, which applies power through two types of war that doctrine refers to as "traditional war" and "irregular war."[9] Traditional war fits closely with what Russell Weigley calls "the American way of war" and equates to the term "conventional war": a conflict between nation-states, using a strategy of annihilation and attrition.[10] Because the non-doctrinal term conventional war is used interchangeably with traditional war, it logically follows that the other type of war is "unconventional war." That logic is incorrect. Doctrinally, unconventional war is

a subset of IW, which precludes its use as an antonym for traditional war.

Perhaps there is a more useful or more logical term than IW for all the kinds of conflict that are not the traditional state-on-state kind. William Sevenson, Marshall Ecklund, Hun Soo Kim, and Robert Billings, for instance, argue for a return to the use of the term "low-intensity conflict."[11] Be that as it may, the current doctrinal term is IW, described as: "A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will."[12]

The 2010 Irregular Warfare Joint Operating Concept states:

> There are principally five activities or operations that are undertaken in sequence, in parallel, or in blended form in a coherent campaign to address irregular threats: counterterrorism (CT), unconventional warfare (UW), foreign internal defense (FID), counterinsurgency (COIN), and stability operations (SO). In addition to these five core activities, there are a host of key related activities including strategic communications, information operations of all kinds, psychological operations, civil-military operations, and support to law enforcement, intelligence, and counterintelligence operations in which the joint force may engage to counter irregular threats.[13]

The Concept further notes: "Security force assistance (SFA), a term that overlaps with foreign internal defense, is defined as: activities that directly support the development of the capacity and capability of foreign security forces and

Mao Zedong, Chinese Communist revolutionary and leader, c. 1960

their sustaining institutions."[14] It also includes this clarification: "These five activities and operations are not listed in an effort to suggest sequence or a linear phasing model. This concept advocates the execution of these five activities in concert with one another to achieve the desired ends."[15]

In "Making Sense of Irregular Warfare," Joe Brown wrote, "[Irregular warfare] is often conflated and used interchangeably with unconventional, revolutionary, asymmetric, guerrilla, insurgent, civil, hybrid, and even terroristic war."[16] While there are endless variations, irregular wars are "wars of governance. . . . [The] contestation arises when another group challenges the incumbent government's legitimacy and seeks to supplant it."[17] In other words, IW involves revolution.

The term "ideology" is yet another contentious word relevant to this discussion. The Assessing Revolutionary and Insurgent Strategies (ARIS) series defines ideology as:

> a set of beliefs that constitute one's goals, expectations, values, and actions and form a comprehensive worldview. In insurgencies, a well-developed ideology serves the purpose of unifying disparate members of a movement, organizing actions around goals and shared values, and justifying actions that may include violence against countrymen.[18]

Ideology is expressed as a strategic narrative, and serves as the glue that holds a revolutionary coalition together and motivates insurgents to take up arms.

Ideology is expressed as a strategic narrative, and serves as the glue that holds a revolutionary coalition together and motivates insurgents to take up arms. An ideology must present both the case against the existing social or political order and the need for fundamental change.[19] Revolutionary ideology and its supporting narratives must be grounded in three elements. First, ideology must demonstrate why it is essential to reform or overthrow the current regime, highlighting the root grievance(s) that the government cannot or will not solve. Second, the ideology must provide a vision of how society, including a political and economic system, should be restructured. Third, the ideology should provide both the motivation to resist the existing political order and the justification to use violence if necessary.[20] Ideology expresses the "why" and should not be confused with "how" strategy is carried out.

The Revolutionary Context: Wars of Governance

In 2035, the Joint Force will confront Violent Ideological Competition focused on the subversion or overthrow of established governments.

Joint Operating Environment 2035[21]

Whether confronting Russian and Chinese interference in the affairs of our allies and partners, or ongoing violent jihadist movements, the United States struggles for legitimacy and influence over relevant populations.[22] As many US SOF operators have experienced in the Middle East and Africa, a government that meets the needs of the people and is fulfilling its side of the social contract has little to fear from internal unrest. Conversely, poor governance incites rebellion.[23] In confronting civil unrest, a government has a binary choice: reform or repress. Reform requires addressing the grievances that are causing the instability; repression occurs when the government resorts to force to stop the unrest. The former can ameliorate the conditions that led to the unrest, while the latter addresses only the symptom of the disorder, not the cause, thus allowing the root cause to fester and foment additional unrest.

Civil unrest, under some circumstances, can develop into an insurgency and eventually lead to a revolution. Jack Goldstone defines revolution as "the forcible overthrow of a government followed by the reconsolidation of authority by new groups, ruling through new political (and sometimes social) institutions."[24] Working from earlier models developed by notable political scientists such as Crane Brinton and Theda Skocpol, Goldstone created a comprehensive model for the analysis of revolutions. He proposed three phases of revolution: state breakdown, struggle for

Mensheviks Pavel Axelrod, Julius Martov, and Alexander Martinov at Norra Bantorget ("Northern Railway Square") in Stockholm, Sweden, May 1917.

power, and state reconstruction.[25] It is during the struggle for power that unrest may transform into armed confrontation involving military forces. This phase is of most interest to our discussion because it is the essence of IW. Before discussing IW's place in revolution, a quick explanation of the beginning and end of revolutions, according to Goldstone's model, is in order.

Goldstone's first phase, state breakdown, occurs when three preconditions are present: a national-level crisis, elite alienation, and a high potential for mobilization of the populace.[26] A crisis that the government cannot overcome precipitates a loss of state legitimacy and control; such crises are often fiscal. A portion of the elite class turns against the state, eventually becoming leaders within the revolt. Widespread protests against the state and governmental repression of these protests by security forces may increase popular resistance, potentially leading to the second phase, armed insurgency (discussed in greater depth below). During this delicate period within the state breakdown phase, external actors can provide support, either to the government to help it surmount its crisis or to the resistance to undermine the government.

Goldstone's third phase, assuming successful revolution, is state reconstruction. The nature of a revolutionary government depends on the pre-revolutionary experiences of the new leaders, the international environment, and the pre-revolutionary economic structures. When a regime is toppled, the opposition/nascent government must be well organized and prepared to exercise good governance, which includes everything from policing to trash removal. Most importantly, the new government must address the original grievances. History has shown that a new government's failure to address the underlying social objections to its predecessor creates a situation that often devolves into a radical phase.[27] The failure of the Girondins in France, the Mensheviks in Russia, and the provisional government of Shahpour Bakhtiar in Iran each led to the seizure of power by brutal radicals.

> **A new government's failure to address the underlying social objections to its predecessor creates a situation that often devolves into a radical phase.**

During the first and third phases, the elements of national power—diplomacy, information, military, economy, finance, intelligence, and law enforcement—are leveraged to achieve desired end states.[28] For example, during the state breakdown phase, diplomacy is used by the government to

"Run on the Tuileries," by Jean Duplessis-Bertauxon, 1792.

US Marines and Afghan National Army soldiers patrol through a residential area of the city of Marjah to carry out counterinsurgency operations as part of Operation Moshtarak.

gain support for itself and to isolate potential insurgents; information operations are conducted to enhance or undermine the legitimacy of the various actors; and economic actions are taken that can reduce or exacerbate the crisis. Likewise, elements of national power can support or undermine the revolutionary regime in the state reconstruction phase. This can also include elements of national power supplied by allied or partner nations. The military, for the most part, and especially in the case of supporting nations, is in a secondary role in both the beginning and the ending phases.

Of primary significance for this article is the second phase, the struggle for power. During this phase, revolutionary movements can employ whichever violent or nonviolent tactics they have determined are the best means for meeting their strategic goal of replacing the existing system. Insurgency/counterinsurgency and terrorism/counterterrorism describe "how" a revolution may be conducted or thwarted. The question of "why" can be answered by looking at political objectives to address the strategic problem, as seen by the revolutionaries.

An organic, grassroots social movement that has an organization and leadership can provide a viable alternative to the existing regime. Only a population motivated by a shared sense of purpose and identity can provide a sufficient recruiting pool of reliable men and women willing to risk their lives for their cause. Past experience of US SOF indicates that it is difficult, if not impossible, to manufacture a viable partner force during a revolution if an organized group does not already exist. The effectiveness of partnering with the pre-existing Kurdish forces during the Syrian civil war, as compared to the attempt to cobble together the Free Syrian Army, is a case in point.

Although a civil war like the one in Syria is not necessarily a part of all revolutions, it is worth noting that the French, Russian, and Chinese Revolutions, among others, all involved extensive civil wars. Nicholas Sambanis wrote that it is "difficult, if not impossible, to develop an operational definition of civil war without adopting some ad hoc coding rules to distinguish civil wars from other forms of political violence."[29]

Drawing on Sambanis's work and Mao Zedong's theory of protracted war, I propose that the genesis of civil war

in a revolution depends on several factors, including the strength of the regime, the extent of fragmentation amongst the revolutionaries, and the ability of counterrevolutionary elements to continue fighting should the regime collapse.[30] Mao's theory of protracted war was adapted by the US Army in Field Manual 100-20, *Military Operations in Low Intensity Conflict*, which expressed the theory in three phases: latent and incipient, guerrilla war, and war of movement.[31] During the war of movement phase, the revolutionaries field an army capable of meeting government forces in conventional battle. Civil war may result if the revolution does not have sufficient power to defeat and overthrow the government, which is itself unable to suppress the rebellion. Such was the case in Syria, where ISIS was able to match the capabilities of the Syrian Army.

Revolutionary movements unable to match the strength of the government may use "confidential, violent terroristic activity" to achieve their goals.[32] Terrorism is the calculated use of violence outside of internationally accepted bounds of civil law and conventional military conduct in the pursuit of political or social objectives.[33] The emphasis on the terms "terror," "terrorism," and "terrorist" can distract from the "why" by focusing attention on "how." Groups and states use terror as a means to achieve an end rather than as the end itself. Groups that utilize terror may, in reality, be movements evolving in capability as they grow with success, expanding from small cells to guerrilla units to revolutionary armies, and ultimately replacing the existing power structure. Terror is a tactic of adversaries, both state and non-state, as part of a broader IW strategy.[34]

Arguably, USSOCOM has been overly focused on terrorism and counterterrorism activities, treating a tactical symptom as a strategic problem.

Arguably, USSOCOM has been overly focused on terrorism and counterterrorism activities, treating a tactical symptom as a strategic problem. Counterterrorism must serve as a component to support a broader strategy with political objectives. The primary aim of such an approach must be the neutralization of the enemy's ideology and the promotion of governmental legitimacy. Deprived of popular support, the insurgent group becomes isolated and forced to flee or face destruction by state security forces. Without the justification and popular support provided by ideology, the group is likely to remain an illegitimate criminal organization in the eyes of the population and the international community. In such a case, the population is more likely to side with the state as the legitimate pillar of security and governance.

Should the government overreact to rising unrest with violence and repression while failing to implement reforms, it may push the population into the arms of the opposition. Once the rebels have won widespread support, the recruiting base of the revolution increases, and the movement becomes an armed insurrection. Rebellions sometimes begin with small-scale guerrilla warfare and

Figure 1: IW in Support of a Partner Nation[35]

	COMPETITOR	ALLIED NATION		USA
NATIONAL POLICY	Political Warfare Supports Partner Opposition	Offensive Opposition Attempting Overthrow	Defensive Government Resisting Overthrow	Political Warfare Supports Allied Government
STRATEGIC	Irregular Warfare (IW) Strategic Messaging	Revolution	Counterrevolution Good Governance	IW Strategic Messaging
OPERATIONAL	Unconventional Warfare (UW) Psyops	Insurgency Resistance	Counterinsurgency (COIN) Resilience	Foreign Internal Defense (FID) Security Force Assistance (SFA) Psyops
TACTICAL	Nonviolent Resistance, Guerrilla Warfare, Subversion, Sabotage, Terrorism		Counterterrorism, Law Enforcement, Direct Action, Civil-Military Operations, Military Information Support Operations	

Figure 2: IW in Support of an Opposition Movement[36]

LEVELS OF WAR	COMPETITOR	INDIGENOUS ENTITY (Nation occupied by or allied with the Competitor)		USA
NATIONAL POLICY	Political Warfare Supports Indigenous Government	Defensive Government backed by competitor	Offensive Opposition seeks to overthrow government or occupying power	Political Warfare Supports opposition to indigenous government or occupying power
STRATEGIC	IW	Counterrevolution	Revolution	IW
OPERATIONAL	FID SFA	COIN	Resistance/Insurgency	UW
TACTICAL	Law Enforcement, Direct Action, Civil-Military Operations		Nonviolent Resistance, Guerrilla Warfare, Subversion, Sabotage	

build toward a more conventional capability. When this occurs, civil war erupts. This progression was proposed by Mao and is the apparent experience in the US-led coalition's struggle against al-Qaeda and ISIS.

Piecing it all Together: A New Doctrinal Model for SOCOM and Allies and Partners

In light of the above discussion, it is incorrect to speak of a counterinsurgency (COIN) strategy. While this statement may appear controversial to many in the US and NATO context, it can clearly be seen that neither counterterrorism nor unconventional warfare (UW) equates to anything more than the proper doctrinal missions of foreign internal defense and stability operations. The United States and our allies and partners conduct an IW *strategy*, which includes, among other things, COIN *operations*. The same is true of UW. We do UW operations as part of a broader IW strategy. In the same vein, doctrinally, the United States cannot have a strategy pertaining to guerrilla warfare,

Figure 3. Strategic Level Support to Partner Nation or Opposition[37]

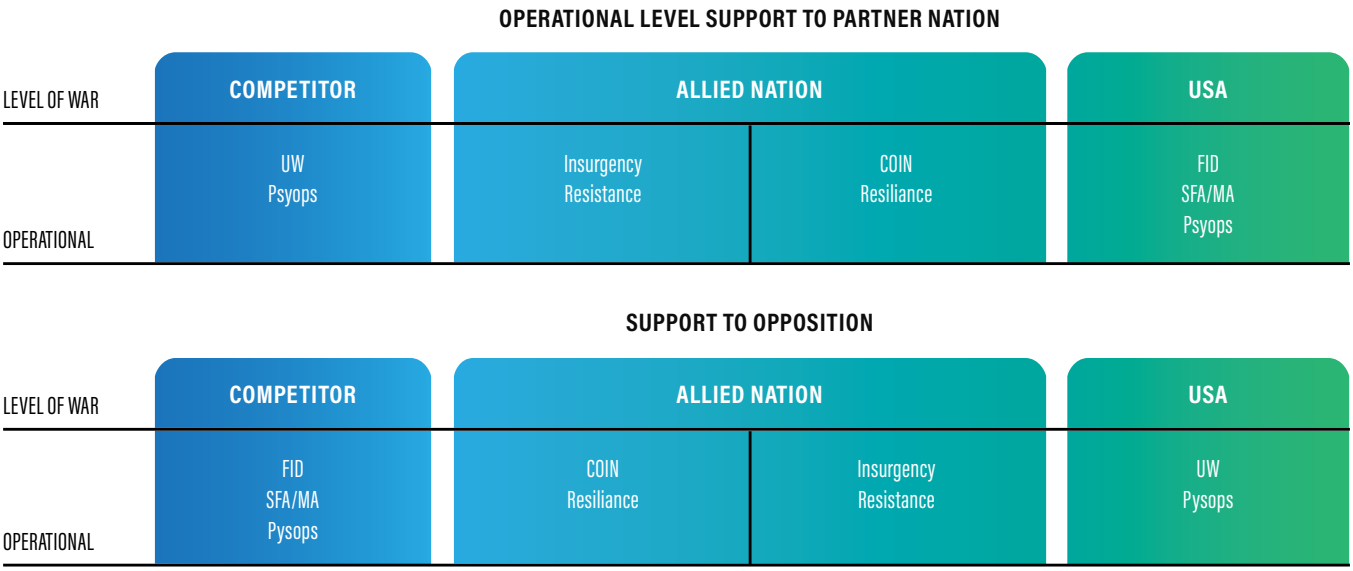
STRATEGIC LEVEL SUPPORT TO PARTNER NATION

LEVEL OF WAR	COMPETITOR	ALLIED NATION		USA
STRATEGIC	IW Strategic Messaging	Revolution	Counterrevolution Good Governance	IW Strategic Messaging

SUPPORT TO OPPOSITION

LEVEL OF WAR	COMPETITOR	ALLIED NATION		USA
STRATEGIC	IW Strategic Messaging	Counterrevolution Good Governance	Revolution	IW Strategic Messaging

Figure 4. Operational Level Support to Partner Nation or Opposition[39]



nor can there be a counterterror strategy. As highlighted above, guerrillas and terrorists engage *tactically* during UW operations. Under an IW strategy, UW aids a revolutionary movement at the operational level and foreign internal defense is operational-level support to a government countering a revolutionary movement. The political leaders of the United States and their UW experts within USSOCOM must ensure that all of our tactical and operational activities are linked to a broader holistic IW strategy.

Figure 1 places military activities in the proper context. In the scenario depicted, the United States is an external actor supporting an allied nation. The competitor is attempting to undermine the allied nation. The government of the allied nation is defending itself from attack by internal opponents supported by the competitor. The United States leverages all elements of national power in pursuit of national policy; in this case, great power competition requires a policy of political warfare toward a competitor.

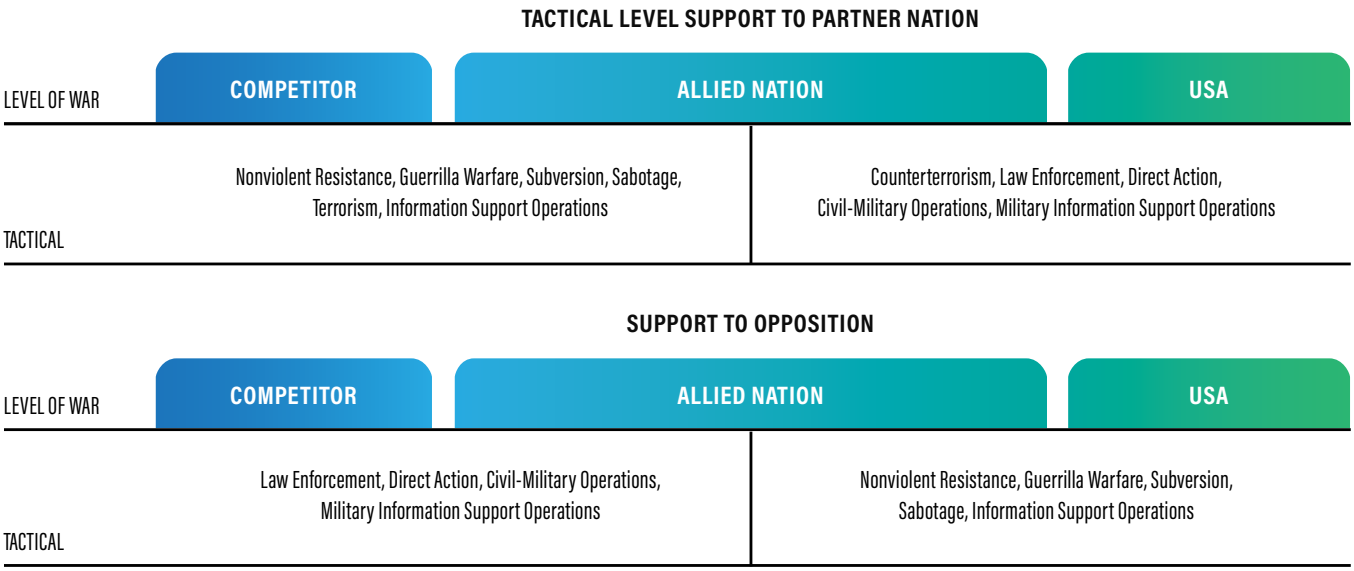
The United States and its allies must return to a national strategy of IW, when warranted, that includes national policy that is comprehensive and global in scope. When a nation decides on a policy of political warfare, that nation employs *all* the elements of national power. The government exerts diplomatic pressure, conducts information campaigns, and imposes economic sanctions. The military contribution is IW. Coordination with other elements of national power and with partners and allies is integral to IW. Within a contested nation, policies of defense and offense are adopted by the government and its internal opponents, respectively. The government seeks to defend its position while the opponent attempts to replace or reform the government. Figure 2 depicts a scenario in which the United States supports the opposition to a foreign government or occupying power.

At the strategic level, depicted in figure 3, the indigenous entities are conducting either revolutionary or counter-revolutionary activities. The best counter to revolution is good governance, because it provides legitimacy to the government and undermines the revolutionary narrative.

At the operational level, the military conducts UW in support of an indigenous resistance movement or insurgency. It performs foreign internal defense and security force assistance in support of a partner or ally, building resilience or conducting COIN (see figure 4). The United States does not act in a vacuum; therefore, "resilience," while not doctrinal, is included here because many European allies use the term.[38] Resilience is a preparation-of-the-environment activity conducted by a nation in danger of invasion and occupation by a hostile force. The term refers to a people's ability to recover the will and ability to resist following the trauma of occupation. Based on the above, it follows that the United States, generally, should not conduct COIN in other countries but should, instead, support partners'/allies' COIN efforts. If US COIN operations become necessary, such operations should be undertaken only to gain time and space to allow our partner/ally to build its own organic COIN capability.

As figure 5 shows, at the tactical level, US forces conduct sabotage, subversion, guerrilla warfare, and preparation of

Figure 5. Tactical Level Support to Partner Nation or Opposition[40]



the environment, among other activities. These activities can be done directly and unilaterally, directly *with* indigenous partners, or indirectly *through* indigenous partners. At the tactical level, such operations merge most noticeably with those of partners.

Closing Thoughts

No one starts a war—or rather, no one in his senses ought to do so without first being clear in his mind what he intends to achieve by that war and how he intends to achieve it.

Carl von Clausewitz, *On War*[41]

Before embarking on an IW strategy, two principle questions must be addressed: whom are we seeking to defeat, and what is the desired end state? These questions apply to partners and allies as well. If actors' goals are incompatible, IW is best not pursued. The United States will never be successful if its deeds do not follow its ideals. Thus, the partners it chooses should share both the desired end-state it seeks and its values.

Irregular wars are wars of government legitimacy and influence over populations; therefore, revolution theory is essential to understanding IW doctrine.

Non-doctrinal terms such as "gray zone" and "hybrid warfare" can be useful to describe an environment and activities in greater depth. But these terms should be used in support of rather than instead of doctrinal terms. Until a change is made to existing doctrine, proper terminology must be used in the proper context to avoid confusion and missteps. This article presented a doctrinal and theoretical framework for understanding IW. The strategic, operational, and tactical levels of war, paired with revolution theory, provide needed context for understanding doctrinal and non-doctrinal terminology. When the United States engages in political warfare, the US military conducts strategic IW in support of partners conducting either revolution or counterrevolution. Operations performed during IW include unconventional war or foreign internal defense and security force assistance, while partners engage in insurgency or resistance, or counter-insurgency and resilience. In support of the operational level, the US military performs counterterrorism, guerrilla warfare, joint combined exchange training, civil-military operations, information support operations, and other tactical operations. Irregular wars are wars of government legitimacy and influence over populations; therefore, revolution theory is essential to understanding IW doctrine. Irregular war is revolutionary.

ABOUT THE AUTHOR

CSM Thomas Myers currently serves as the Senior Enlisted Leader for the International Special Training Center, Pfullendorf, Germany.

NOTES

1. James Eliot Cross, *Conflict in the Shadows: The Nature and Politics of Guerrilla War* (Garden City, NY: Doubleday, 1963), 4.
2. Thomas Myers, "Terrorist to Tyrant," *Homeland Security Affairs* 7 (February 2011): https://www.hsaj.org/articles/57
3. David S. Maxwell, "Do We Really Understand Unconventional Warfare?" *Small Wars Journal* (23 October 2014): https://smallwarsjournal.com/jrnl/art/do-we-really-understand-unconventional-warfare
4. John Spencer, "What Is Army Doctrine?" Modern War Institute, 21 March 2016: https://mwi.usma.edu/what-is-army-doctrine/
5. David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Fredrick Praeger, 1964), 6–7.
6. George F. Kennan, "George F. Kennan on Organizing Political Warfare," Wilson Center, 30 April 1948, 1: https://digitalarchive.wilsoncenter.org/document/114320 ; Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton; Princeton University Press, 1984), 87.
7. Kennan, "George F. Kennan," 4, 5.
8. Michael N. Schmitt and Andru E. Wall, "The International Law of Unconventional Statecraft," *Harvard National Security Journal* 5, no. 2 (2014): https://harvardnsj.org/wp-content/uploads/sites/13/2014/01/Schmitt-Wall-International-Law-of-Unconventional-Statecraft.pdf ; Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND Corporation, 2018): https://www.rand.org/pubs/research_reports/RR1772.html
9. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, JP1 (Washington DC: Joint Chiefs of Staff, 2017): x.
10. Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington, IN: Indiana University Press, 1991).
11. William Stevenson, Marshall Ecklund, Hun Soo Kim, and Robert Billings, "Irregular Warfare: Everything Yet Nothing," *Small Wars Journal*, 16 December 2008: https://smallwarsjournal.com/jrnl/art/irregular-warfare-everything-yet-nothing
12. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington, DC: Office of the Secretary of Defense, 2013): 149.
13. Department of Defense, *Irregular Warfare Joint Operating Concept, Version 2.0*, (Washington, DC: Office of the Secretary of Defense, 2010): 4.
14. Ibid., footnote 7.
15. Ibid., footnote 8.
16. Joe Brown, "Making Sense of Irregular War," *Over The Horizon Journal* (19 April 2017): https://othjournal.com/2017/04/19/making-sense-of-irregular-war/
17. Ibid.
18. US Army Special Operations Command, Assessing Revolutionary and Insurgent Strategies, *Human Considerations of Undergrounds in Insurgencies*, (Fort Bragg, NC; USASOC, 2013), 368.
19. Myers, "Terrorist to Tyrant," 2.
20. Ibid.
21. Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: Joint Chiefs of Staff, 2016): https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf
22. US Department of State and US Agency for International Development, *Joint Strategic Plan* FY *2018 – 2022* (Washington, DC: Department of State, 2018), 23–31: https://www.state.gov/wp-content/uploads/2018/12/Joint-Strategic-Plan-FY-2018-2022.pdf
23. USASOC, Assessing Revolutionary and Insurgent Strategies, 13–21.
24. Jack A. Goldstone, "An Analytical Framework," in *Revolutions of the Late Twentieth Century*, eds. Jack A. Goldstone, Ted Robert Gurr, and Farrokh Moshiri (Boulder, CO: Westview Press, 1991), 37.
25. Ibid.
26. Ibid., 37–40.
27. Jack A. Goldstone, *Revolutions: Theoretical, Comparative, and Historical Studies* (Belmont, CA: Wadsworth/Cengage Learning, 2003), 4.
28. Joint Chiefs of Staff, *The National Military Strategic Plan for the War on Terrorism*, (Washington, DC: Joint Chiefs of Staff, 2006), iii: https://www.files.ethz.ch/isn/15230/2005-01-25-Strategic-Plan22.pdf
29. Nicholas Sambanis, "What Is Civil War? Conceptual and Empirical Complexities of an Operational Definition," *Journal of Conflict Resolution* 48, no. 6 (2004): 816: http://www.jstor.org/stable/4149797
30. Ibid., 814–858; Mao Tse-tung (Zedong), "On Protracted War," The Marxists Internet Archive: https://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm.
31. Department of the Army, *Military Operations in Low Intensity Conflict*, FM 100-20 (Washington, DC: Department of the Army, 1990): https://www.globalsecurity.org/military/library/policy/army/fm/100-20/index.html
32. Eitan Azani, *Hezbollah: The Story of the Party of God: From Revolution to Institutionalization* (New York: Palgrave Macmillian USA, 2009), x.
33. Myers, "Terrorist to Tyrant"; Mark Burgess, "Terrorism: The Problems of Definition," Center for Defense Information, 1 August 2003: https://aldeilis.net/english/terrorism-the-problems-of-definition/
34. State use of terrorism against rebellious and insurgent populations is an important and large topic which exceeds the scope of the present discussion.

35. Created by the author.
36. Created by the author.
37. Created by the author.
38. Kevin D. Stringer and Glennis F. Napier, eds., *Resistance Views: Essays on Unconventional Warfare and Small State Resistance* (MacDill Air Force Base, FL.: JSOU Press, 2018).; Otto C. Fiala, *Resistance Operating Concept (*ROC*)*, (MacDill Air Force Base, FL: JSOU Press, 2020), 3–72.
39. Created by the author.
40. Created by the author.
41. Clausewitz, *On War*, 579.

How Dutch Special Operations Forces Can Support Cyber Operations: A Symbiotic Relationship

MAJ Jonas van Hooren, Netherlands Marine Corps

ON THE SUNNY MORNING OF 11 APRIL 2018, Russian cyber operator Aleksej Sergejvitsj Morenets left the Moscow headquarters of the GRU, Russia's main military intelligence directorate, to take a taxi to the airport. At the airport, he joined his cyber colleague Yevgeni Michajlovitsj Serebrakov and two support agents—Oleg Miajlovitsj Sotnikov and Alexej Valerjevitsj Minin—from the GRU intelligence cyber warfare team, also known as ATP 28 or Unit 26165. Using diplomatic passports, they traveled together on a direct flight from Moscow to Amsterdam with one mission: to hack the world's top chemical weapons watchdog in The Hague, the Organization for the Prohibition of Chemical Weapons (OPCW).[1]

After the nerve agent poisoning of Russian ex-spy Sergei Skripal and his daughter in the British city of Salisbury in March 2018, and the chemical attack a month later by Syria's Russian-backed military on the town of Douma, the OPCW had launched extensive investigations. It blamed Russia for both attacks, citing evidence that implicated the GRU.[2] Russia protested that the OPCW was going far beyond its mandate. Instead of waiting for the results of the full investigation, Russia sent the GRU hackers to the Netherlands to compromise and disrupt OPCW computers.

After arriving in the Netherlands, the GRU cyber warfare team hired a car and scouted the OPCW building and its surroundings to prepare for a closed access hack on the OPCW's wi-fi network. On 14 April, the team left a rental car fully packed with state-of-the-art hacking equipment in the parking lot of the Marriott hotel, as close as possible to the neighboring OPCW building where they were attempting their attack. From the moment the GRU team set foot on Dutch ground, however, they had been closely monitored by the Dutch military intelligence and security services (MISS). Before the Russians could carry out the actual hack, they were intercepted and detained by Dutch authorities, who were fully prepared to prevent the cyber-attack against the OPCW. When they realized what was happening, the GRU team tried to destroy one of their Russian cellphones, which showed their heightened awareness of security. After having all of their technical equipment, laptops, antennas, cameras, and mobile telephones confiscated, they were escorted to Schiphol Airport and deported to Moscow.[3]

This attempted hacking operation shows that the Netherland's knowledge, innovation, network, and technology services are possibly vulnerable to virtual and physical (hybrid) threats instigated by foreign organizations and institutions.[4] This vulnerability is by no means limited to the Netherlands, as shown by the discovery in late 2020 of widespread cyber infiltration of US government agencies and private corporations by Russian intelligence operatives.[5] At the time of this writing, the extent of that operation and its possible consequences are still unknown.

This article investigates the relationship and avenues for coordination between the physical environment, where SOF operates, and the more abstract virtual environment, the cyber domain, in the context of the Netherlands.[6] If these two environments are effectively connected, this combination could provide the Ministry of Defense (MoD) with better insights into more efficient and effective capabilities to defend against both national and international hybrid threats that the Netherlands may face.

The problems and solutions proposed in this article are written from the perspective of a wealthy European nation with advanced military capabilities and strong international alliances. As developing countries increase both their integration into the modern global economy and their reliance on cyberspace to conduct domestic and international business, however, they will inevitably increase their vulnerability to disruptions and threats in the cyber domain. The ideas and options presented in this

Cyber warfare operators monitor cyber attacks.

article can be a useful starting point for all governments to discuss the ways in which military forces—and particularly special operations assets—can defend and support their growing cyber sectors.

Dutch strategic military leaders see the importance of improving cyber defenses, but struggle to find the right approach.

Background to the Problem

Like other knowledge-based globalized economies, the Netherlands is vulnerable to hybrid cyber threats from state and non-state actors. Dutch strategic military leaders see the importance of improving cyber defenses, but struggle to find the right approach. This article explores the question of how Dutch SOF can enhance national cyber capabilities to counter the hybrid threats that the Netherlands currently faces.[7] It finds that SOF's unique capabilities offer three possible options: 1) to gain access to hard targets for cyber operations; 2) to provide the means to get people, hardware, and software in or out of the operation area; and 3) to understand, deceive, and influence the cultural environment to enhance cyber operations. The article also proposes three potential structural options for integrating SOF and cyber capabilities: 1) develop and train cyber-SOF teams and delegate them to the operational commands; 2) embed SOF and cyber personnel in each other's organizations; or 3) create a new cyber-enabled special operations unit. The Netherlands defense ministry has recently established some organizations, including a new Special Operations Command (NLD SOCOM), a Defense Cyber Command, and a Joint SIGINT (signals intelligence) Cyber Unit, that can support one or more of these options.

The Netherlands is in many ways a very safe country, but the world's security situation is changing rapidly. The current Dutch threat level is "substantial"—that is, level 4 on a scale of 1 (minimal) to 5 (critical)—meaning that a terrorist attack against the Netherlands is considered to be highly likely.[8] The threats posed by terrorist attacks, cyber attacks, unwanted foreign interference and compromised elections, military pressure, and attacks on critical economic processes are urgent and require an effective ministry-wide security policy. The weakening of the international security situation, combined with intensifying geopolitical conflicts of interest, makes the Dutch MoD's involvement in cyber security critical. It not only must prepare for "advanced digital threats in the event of an unforeseen (military) conflict,"[9] but also has a responsibility to assume that this could happen (or has already happened) throughout government, and on the international level through the country's membership in NATO and other international organizations.

Salafism and Wahhabism

The traditional operational environments (land, maritime, air, and space) have been enriched and, at the same time, imperiled by a new environment: the cyber, or "fifth," domain, which encompasses all forms of "digital warfare." The cyber domain, however, differs from the other domains in that it is a human-made, partly non-physical domain that integrates human activity across the other domains' physically delineated boundaries. Cyberspace can be considered to be interconnected and "autonomous physical or virtual networks, software-controlled systems or devices, software, and data," including systems that are not connected to the internet and physical components such as computers, servers, routers, satellites, and cables on land and in the sea, air, and space.[10] Consequently, the five domains are dynamically interlinked; a change in one usually has implications for the others. According to the 2015 US National Security Strategy, "the world is connected by shared spaces . . . and access is at risk due to increased competition and provocative behaviors."[11]

Cyber war, or the less inflammatory terms *cyber conflict* or *cyber competition*, can trigger a reaction in one or more of the physical domains, and vice versa. For example, in 2004, the Siberian gas pipeline infrastructure was manipulated virtually to raise the pressure in some pipelines, which resulted in an explosion. More famously, the digital worm called Stuxnet, deployed in 2005 but not discovered until 2010, damaged an Iranian nuclear enrichment facility by manipulating its control program to sabotage the spinning frequency of the nuclear enrichment centrifuges.[12]

Royal Netherlands Army SOF Korps Commando Troepen (KCT)

The Stuxnet attack may have been the first offensive cyber weapon to be deployed, and its effects delayed Iranian nuclear development for years.[13] Russia has become particularly adept at weaponizing international cyberspace in innovative ways. A Kremlin-directed massive directed-denial-of-service attack on the highly digitized Estonian public and commercial infrastructures in 2007 temporarily shut down ministries, parliament, banks, news organizations, and businesses.[14] In 2008, before the Russian army launched a physical military invasion of a Georgian province, the battlefield was well-prepared by Russian online influence operations that primed the ethnic Russian population to support the invasion.[15] Russian cyber intelligence assets used a similar playbook to pave the way for the annexation of Crimea in 2014.[16] Evidence from several investigations shows that the 2016 US presidential election was at least influenced by online trolls working for the Russian Internet Research Agency, who spread misinformation through fake social media accounts.[17] These are only a few of the more notable incidents that took place in the past two decades.

Cyberspace will influence the future of the military, especially SOF, because both worlds are rapidly coming closer together.

In similar ways, cyberspace will influence the future of the military, especially SOF, because both worlds are rapidly coming closer together. The difference between soldiers using real guns and hackers pulling the trigger online will become less clear.[18] Hacking one enemy to drive it to attack another enemy, while the instigator avoids both attribution and the costs of physical conflict, is now a real threat. The physical role that SOF plays in hybrid warfare will necessarily evolve when future hybrid warfare takes place primarily online.

The Roles of SOF and Cyber in Each Other's Domains

NATO delineates SOF's primary roles as special reconnaissance (SR), military assistance (MA), and direct action (DA). These three main tasks, or derivatives of them, are typically executed in the physical landscape. The cyber domain gives nation-states the opportunity to counter aggression "under the radar"—that is, using covert, non-attributable means—and SOF could be a proficient capability to support these cyber activities against national threats. Currently, 95 percent of warfighting is traditional, consisting of tanks, planes, and ships, while only 5 percent is taking place in the cyber-domain; however, some experts expect that by 2035, the ratio will have shifted to 50–50.[19] Being physically on the ground gives SOF opportunities to establish relations and connections with local stakeholders,

from which cyber operations could benefit. Patrick M. Duggan, a retired Special Forces colonel, put it in another way:

> SOF are the key to cyber warfare and deception, and manipulation. SOF can exploit their abiding understanding of psychological, cultural, and societal factors that drive human behavior and for providing unrealized opportunities in persuasion and compulsion to shape the calculations, decision-making, and behavior of relevant actors. Adopting a discreet push-approach for cyberwarfare, SOF can channel the steady accumulation of small human and technical acts into an eventual psychological tipping point that changes the adversary's behavior.[20]

The operational SOF environment and cyberspace share many similarities. For instance, both involve overt, covert, and clandestine activities that are executed by anonymous individual actors, groups, nation-states, or even transnational organizations, in a global and complex environment.[21] The clandestine activities of SOF are comparable to stealthy cyber operations: the purpose of both is to assist in gaining military, political, economic, ideological, social, or religious dominance, as well as an information advantage.[22] Both have relatively short preparation and recovery times, are relatively cheap, and have an opaque and stealthy character. The intent of SOF actions like DA and SR is similar to offensive cyber operations. Likewise, the intent of an MA operation could match the purpose of defensive cyber operations: to strengthen a foreign state and thus safeguard its national political- military interests without large-scale military involvement. Both can also have a deterrent effect by serving as a warning of a country's capabilities.[23]

There are nevertheless some significant differences between SOF and cyber operations. For instance, the SOF operator in the field behind enemy lines accepts high personal risk compared with the relatively safe and secure desk jobs of the cyber experts in their home country or Forward Operating Base. The cyber expert can operate from almost anywhere in the connected world regardless of geographic proximity to the target, while the SOF operator must be physically in the area of operation near or at the target, sometimes in conflict zones with poor infrastructure and living conditions. Furthermore, cyber combatants are not limited by personal physical condition or physical handicaps, whereas SOF personnel need to be physically fit, well trained, and always ready to operate in harsh conditions.

State-sponsored cyber operations rarely occur in isolation; they are usually coordinated with other diplomatic and military means at the same time and in the same place.

However, given their respective strengths and abilities, there is growing interest in having SOF and cyber capabilities integrate and coordinate. In some situations, it may no longer be necessary for SOF to conduct a physical SR to prepare for a DA operation, when the required information is already prepared, documented, and exploited online. On the other hand, the insertion of malware into an enemy air-gapped network may require boots on the ground, and those boots usually belong to SOF. State-sponsored cyber operations rarely occur in isolation; they are usually coordinated with other diplomatic and military means at the same time and in the same place.[24]

SOF's Possible Roles to Fill the Cyber Gaps

Dutch SOF, like those in many NATO countries, characterizes itself as a joint strategic asset that can "conduct special operations in uncertain, hostile, or politically sensitive environments to create effects that support the achievement of strategic-operational comprehensive objectives. These operations may be conducted using clandestine or covert capabilities/techniques and require mature and highly-trained operators."[25] Obviously, SOF is not a silver bullet for all cyber problems and capability gaps, and some of its traditional roles will not be useful in all (digital) operational environments; however, its unique capabilities should be considered when planning certain kinds of cyber operations.

The three main ways in which SOF can support and execute cyber operations are to: 1) gain access to hard targets for cyber operations; 2) provide the means to get people, hardware, and software into or out of the operations area; and 3) understand, manipulate, and influence the cultural environment. Although these three roles differ significantly, they are not mutually exclusive. For example, before a cyber technician can be extracted out of a hostile locality (role two), SOF needs first to understand, manipulate, and perhaps influence the cultural environment (role three) to set the right conditions for the extraction. As it is, each role could be used as an umbrella for numerous kinds of cyber-SOF operations with various tactics, techniques, and procedures.

Gain Access to Hard Targets for Cyber Operations

The planning, execution, and command and control of a cyber operation could, theoretically, be orchestrated from a desk at any connected platform anywhere (land, air, sea, or space) in the world. There are, however, classified examples of cyber operations that could not have been carried out without putting physical boots on the ground to create points of entry and provide access to so-called "hard targets" of interest to cyber intelligence. Such targets are often remote, isolated, and difficult-to-access physical objects.[26] SOF's character as an under-the-radar operating force, capable of blending in with the local inhabitants and equipped with the proper reconnaissance, sabotage, breach, and fighting tools, makes it a valuable initial entry force to physically exploit tactical sites and/or to create the conditions for cyber operators to break into computers, networks, and information systems in or around hard targets.

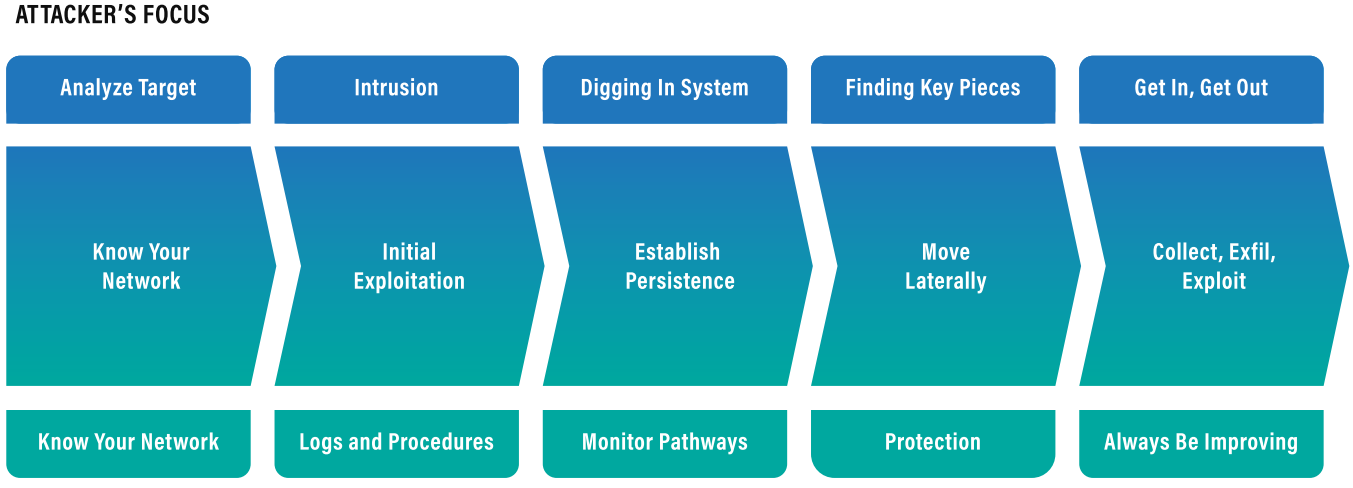
> **There are classified examples of cyber operations that could not have been carried out without putting physical boots on the ground to create points of entry.**

Hacking into computers through active cyber operations is often done via an intrusion model. Figure 1 depicts such an intrusion model and the stages of this multifaceted process. The model is not technically or tactically focused, but could be used as an operational concept for intruders to reach their strategic objective in a cyber operation.[27] Each stage (reconnaissance, initial exploitation, establishment of persistence, lateral moves, and collection-exfiltration-exploitation) in this model presents an opportunity to get deeper in someone's system to spy, influence, sabotage, collect, or even attack. Alternatively, the defender's method seen in this model illustrates the measures necessary to counter or defend the cyber system.

Especially in the first stages of the intrusion model, SOF present on the ground could conduct SR to collect information on the target (target acquisition) or be the initial entry force to bridge the "air gap" between the physical and virtual environments. With such proximity, SOF could collect intelligence about the target and use radio-frequency technology to establish a connection with objects of interest, even when those objects are isolated from the internet.[29] Once this has been accomplished, the cyber experts "back home" could exploit the gathered intelligence and focus on the next stage in the intrusion model.

A good proof-of-concept is the formerly secret operation code-named "Olympic Games," but better known as the Stuxnet attack.[30] During this combined NSA-CIA-Mossad operation, which was first discovered in 2010, NSA-developed malware was infiltrated into a nuclear enrichment facility in Natanz, Iran, with the goal of sabotaging the centrifuges and stopping the enrichment process. Although the enrichment facility was heavily protected and therefore

Figure 1: The Intrusion Model[28]



Members of the Netherlands Maritime Special Operations Force (NLMARSOF)

not connected to a network, the CIA and Mossad used human assets to bridge the air gap and infect the Iranian system.[31] In denied and hostile circumstances, in particular, SOF can be used as the human tool to resiliently bridge air gaps with technical equipment in various environments and climates during low visibility operations.

Another hypothetical example is the placement of technical devices to intercept, assemble, influence, disaggregate, disseminate, jam, or disturb data and systems in foreign countries. Such a device could be covertly placed by SOF personnel close to the target of interest in a hostile environment.[32] This technique was probably also used in the Stuxnet operation. New York Times journalists David Sanger and Thom Shanker describe a different incident:

> What seemed to be an ordinary rock near a nuclear facility was in fact filled with electronic equipment that may have been relaying pilfered info or transmitting command and control instruction. . . . In 2012, a unit of the Iranian Islamic Revolutionary Guards Corps moved a rock near the country's underground Fordo nuclear enrichment plant. The rock exploded and spewed broken circuit boards that the Iranian news media described as the remains of a device capable of intercepting data from computers at the plant.[33]

SOF has the ability to give cyber operators access to hard, difficult, and isolated physical targets by placing electronic or digital devices in extreme, rough, and dangerous terrain; cyber personnel can use the data and information they gain for follow-on operations in the next step of the intrusion model.

Move People, Hardware, and Software into or out of the Operation Area

SOF has various land, air, and maritime capabilities in its operational toolbox to get humans, hardware, and software into or out of the operations area. Dutch SOF can function as an SR element, quick reaction force (QRF), counterterrorism (CT) unit, or force protector (FP) to support cyber operations. With these capabilities, SOF is able to get technical cyber experts or support agents, for example, into and out of a hostile environment. What is more, SOF can catch and arrest malicious hackers, hacktivists, cyber criminals, and cyber-terrorists from where they sit behind their computers or mobile devices and extract such individuals, along with their software and hardware for processing by the authorities.

It is also possible for SOF personnel to insert technical equipment or software into a foreign country by infiltrating it into the area of interest or giving it to cyber experts who need it to carry out cyber operations. This could be something as small as a USB stick, or it could be larger technical support equipment. Besides infiltration, it is also possible for SOF to remove and exfiltrate important information devices to a safe location for further technical investigation. Both infiltration and exfiltration operations of software and hardware could be executed by SOF in all kinds of extreme environments and conditions in the air, land, and maritime domains. As Patrick Duggan notes, SOF could support cyber operations by "monitor[ing]

and employ[ing] inconspicuous sensors and unmanned platforms to relay information across mobile deep learning devices equipped with 'neutral networks' capable of processing massive amounts of data, even classified."[34] Technically trained SOF operators could integrate so-called FRINGE (photo, robo, info, nano, geno, and electro) technologies to help bridge the cyber gap between the men and the machines.[35]

Technically trained SOF operators could integrate so-called FRINGE (photo, robo, info, nano, geno, and electro) technologies to help bridge the cyber gap.

The 2007 Israeli raid against a suspected nuclear facility in Syria is a good example of the use of FRINGE technologies to bridge the cyber gap between men and machines. In July 2007, Israeli *Shaldag* commandos moved electronic warfare, cyber, and laser equipment into the Syria desert in preparation for a special operations mission code-named "Orchard." Electronic warfare and cyber warfare specialists used the equipment to set up a false-sky picture and jam Syria's air defenses. This deception operation allowed Israel to send F-15s and F-16s into Syrian airspace, where they dropped laser-guided bombs on the suspected nuclear reactor site at al-Kibar, without being detected by the radar station in Tall al-Abyad. As soon as the Israeli aircraft were in the vicinity of the Syrian site, the *Shaldag* commandos directed their lasers onto the reactor to guide the aircraft to their target. The nuclear reactor site in al-Kibar was completely destroyed.[36]

Understand, Deceive, and Influence the Cultural Environment

SOF can facilitate cyber operations by building relationships, establishing human networks, and creating local trust through key leader engagements.[37] By being physically present in the theater of operations, SOF has the opportunity to understand the local environment, recognize future opportunities, and exploit vulnerabilities to create entry points for possible cyber operations. In other words, SOF can draw a picture and set the conditions for the cyber experts in the initial stages of the intrusion model. Whether the human network of an adversary is using

Ukrainian Navy at port in Sevastopol, 2007.

People protesting Russian invasion of Ukrainian territory, 2014.

social media or other digital communications, the network itself remains physical, and is therefore susceptible and vulnerable to interception and influences.[38] The adversary's strategic goals can be manipulated, deceived, or influenced via physical or virtual entry points in the overlapping area between human and digital interaction. SOF can exploit both entry points using its traditional land, sea and air capabilities, cyber assets, or a combination of these.

This article began with a discussion of the Russian close-attack-hack—that is, hacking from a close distance—that was used to bridge the air gap on the OPCW in The Hague. That attack provides a clear example of the overlapping area between human and digital interaction, and clarifies the third way in which SOF can support cyber operations. To prepare for the attack, the GRU operators blended into the Dutch cityscape by posing as tourists. In this guise, they were free to wander around exploring weak spots in the security of the OPCW building. They then used the wi-fi network as a vulnerable physical entry point to get inside.

In another example, Russian SOF influenced the cultural environment in Crimea to prepare for cyber operations, setting the conditions to paralyze any opposition before the cyber-attack was launched. Using the pro-Russian population in Crimea to understand, deceive, and influence the Ukrainians, Russia gained a decisive advantage at an early stage of the hybrid conflict. By using pro-Russian Crimeans as proxies, Russian SOF was able to influence the regional culture and set the conditions for the next stage in the annexation: a digital sabotage of three Ukrainian electricity distribution companies, which left more than 200,000 consumers without power.[39] No power meant no communications, which made it childishly simple for the Russians to take over all of the Ukrainian military installations on the peninsula.

Using the pro-Russian population in Crimea to understand, deceive, and influence the Ukrainians, Russia gained a decisive advantage at an early stage of the hybrid conflict.

Whether connected to the internet or not, SOF could set the conditions, directly or indirectly, to take discrete human and technical actions and create entry points in the regional cultural environment via proxies, allied partners, the indigenous population, and key leaders. These physical and virtual entry points could be exploited by cyber experts back in the home country to counter digital hybrid threats.

Ways to Integrate SOF and Cyber Assets

The discussion in this section uses existing agencies of the Dutch Ministry of Defense (MoD) to illustrate ways in which SOF and cyber capabilities can be integrated and prepared for joint operations. Although these examples are based on specific existing Dutch entities, the three possible options identified here can be extrapolated to other defense ministries, depending on their existing and potential future resources. The three primary options to integrate SOF with cyber activities to support special cyber operations are to: 1) delegate cyber-SOF teams to the operational commands; 2) embed SOF and cyber personnel in each other's organizations; and 3) create a new cyber-enabled special operations unit. Each option is described in detail below, followed by a vignette that illustrates how units organized according to that option might actually operate.

Option One: Delegate Hybrid Cyber-SOF Teams to the Operational Commands

The Dutch MoD, with SOCOM in the coordinating role, could instruct the Army and Navy, which are the only two operational commands with SOF capabilities, to set up hybrid cyber-SOF teams. These cyber-SOF teams would integrate with the Army SOF *Korps Commando Troepen* (KCT) and the Netherlands Maritime Special Operations Forces (NLMARSOF), giving both operational commands control over the hybrid units at the tactical and operational levels. Both KCT and NLMARSOF are already tailored for the units' anticipated needs, according to their available resources and budgets. These hybrid cyber-SOF teams would enhance the traditional SOF MA, SR, and DA roles with cyber expertise.

The hybrid teams would require personnel to have a deep specialization in both SOF operations and cyber techniques. The operators on these teams should know how to infiltrate a denied or hostile environment, execute various SOF taskings, and at the same time, code, encrypt, or manipulate digital media by using advanced tools, such as FRINGE technologies.[40] The recruitment, training, and maintenance of these highly skilled and developed personnel will be challenging, so it would be best for both KCT and NLMARSOF to experiment with SOF-cyber integration on a small scale.

> **If the proper mandate, legal framework, and infrastructure are in place, these hybrid tactical-operational cyber-SOF capabilities can achieve significant results.**

If the proper mandate, legal framework, and infrastructure are in place, these hybrid tactical-operational cyber-SOF capabilities can achieve significant results. Military intelligence cyber operations already have access to a range of activities and techniques, which could also be used for offensive cyber operations. With this in mind, however, it would be a mistake to simply try to transform a hacker into a SOF operator or vice versa.

Vignette for Integration Option 1

The Special Operations Maritime Task Group (SOMTG) Trident is fully operation-capable at its maritime platform outside the exclusive economic zone somewhere off the coast of East Africa and waiting for further instructions from the Allied Maritime Command in Northwood, United Kingdom. When Trident receives its NATO-SOF mission set, to infiltrate and collect intelligence on a local pirate network at one of the larger illegal camps near the beach, the staff start their planning. They conclude that the only option to covertly insert personnel is by swimming or diving. All other options using boats, helicopters, or even parachute drops are too risky and could alert the security-conscious pirates. In preparation for such a contingency, SOMTG Trident has integrated technical experts who are fully trained to swim and dive.

The next night, two buddy teams, each consisting of one MARSOF operator and one technical cyber operator, launch from the Navy vessel and proceed toward the coastal pirate camp in a small rubber boat. When they reach the designated position offshore, the first team of two gets into the pitch-dark water; both are connected with a snag line and equipped with radios, weapons, and technical equipment. After 20 minutes, the boat driver receives a call that the first team missed its target due to a strong current. The second team is inserted from a different angle and, within two hours, they manage to swim to the beach and infiltrate the hostile pirate camp. Here, they covertly install a digital interception device that makes it possible to intercept and decrypt all local radio traffic, including the encrypted signals that enable the pirates' mother ship to interdict commercial vessels. With this information, SOMTG Trident is able to track and intercept all of the pirates' local communications, which leads to the

arrest of many pirates caught in action outside the East African country's territorial waters.

Option Two: Embed SOF and Cyber Personnel in the Other Organization

At the staff level, some Dutch SOF and cyber security personnel are already working in one another's organizations. On the strategic level, SOCOM has a cyber officer liaising with the Defense Cyber Command (DCC) and the Joint SIGINT Cyber Unit (JSCU).[41] On the operational and tactical levels, both KCT and NLMARSOF also have cyber liaisons in staff positions. Despite these steps, however, there are almost no SOF planners or even operators working in the DCC or JSCU and, other than the liaisons, no cyber experts or operators are working in the SOCOM, KCT, or NLMARSOF. Due to the scarcity of technical cyber personnel, the MoD has started a project with reserve cyber experts.[42] Both the SOF and cyber organizations could use this pool of cyber experts when they are planning for operations that require specialized cyber techniques, coding, or encryption.

Embedding specialized personnel in each other's organizations will benefit the cultural understanding and situational awareness of both SOF and cyber personnel, and help bridge the gap in institutional cultures between the communities. To sketch a scenario, both SOF and cyber personnel could start with an internship within each other's organizations to learn and understand the culture, techniques, procedures, and planning processes used by their respective groups. The development of mutual understanding and respect will demand an extended commitment from both cyber and SOF personnel and their organizations and leadership. The specialists need to train, exercise, and educate one another to learn the tactics, techniques, and procedures of SOF and cyber operations. Once there is a basic mutual understanding, SOF and cyber personnel could embed in task-organized teams that fit future taskings. A flexible mentality is vital because every mission to support cyber operations demands a different approach. Sometimes SOF personnel will only stand by physically in a holding area, ready to act as a quick reaction force, and occasionally cyber experts will embed in a SOF team to be inserted into or extracted out of the operation area. Both ways of embedding personnel will demand training, time, commitment, and patience at all levels.

A flexible mentality is vital because every mission to support cyber operations demands a different approach.

Vignette for Integration Option 2

After accomplishing its first NATO-SOF mission in the African pirate camp, SOMTG Trident receives new orders from Northwood to physically install spyware on a secure server in a medium-sized regional city in the target country. The purpose is to intercept the pirates' email traffic, which, it is hoped, will give NATO a better understanding of the pirates' financial networks. The cyber experts have already flown in and, disguised as tourists, are waiting in a hotel in the city for the cyber equipment they need, which they could not bring in via commercial flights. SOMTG Trident should be able to provide a screen during the interception operation, and in case of emergency, react as a QRF to protect and, in the worst case, extract the cyber experts back to the maritime platform.

Due to long and intensive joint education, training, and exercises in their home country, the SOF and cyber teams know each other very well. They speak the same language and understand each other's tactics, techniques, and procedures, which allows a smooth link-up and handover procedure at the hotel with the SOMTG's low-visibility operations (LVO) team. During the actual close-target hack at the data center, the LVO team provides a covert screen, which would act as an early warning system and alert the cyber team in case of a possible compromise. As soon as the hack is completed, the cyber team returns to the hotel and the LVO team exfiltrates via the water back to the maritime platform, safe and secure beyond the horizon. The spyware is successfully installed and the surveillance begins.

Option Three: Create a New Cyber-Enabled Special Operations Unit

The third integration option to enhance SOF support for cyber operations is to create a new centralized, cyber-enabled special operations unit that operates directly under the strategic wing of SOCOM or DCC/JSCU. Under these wings, such a unit could "serve as the single authority to plan, coordinate, and build for global cyber-SOF operations."[43] From this strategic level, both the Army with KCT and the Navy-Marine Corps with NLMARSOF could benefit from this cyber-enabled special operations unit by embedding teams from the cyber-SOF unit in those forces during exercises, training, and, ultimately, operations.

Ultimately, the legal framework would determine what kind of techniques and types of cyber operations are allowed.

This cyber-enabled special operations unit would need a staff element to plan, control, liaise, develop, build, and sustain the new group. Depending on the main effort and legal framework for an operation, this staff element could act as a sub-unified command under the wings of SOCOM or DCC/JSCU in a supported or supporting role; this dual-headed orientation would give the staff flexibility and encourage creativity.[44] A mission set under the umbrella of a cyber-oriented command, such as DCC and JSCU, demands more technical expertise than one under SOCOM, where a more tactical approach is needed. Ultimately, the legal framework would determine what kind of techniques and types of cyber operations are allowed.

To picture a scenario, this cyber-enabled special operations unit could divide its focus and expertise among special warfare roles such as MA, SR, and surgical strikes such as DA. In special warfare, the cyber-enabled special operations unit places more emphasis on the regional background and linguistic skills of its personnel in order to improve its ability to blend into the local environment. Although there is still a need to understand coding, encryption, and the use of FRINGE technologies, the focus in special warfare is more on understanding the local population's habits, routines, and customs. Therefore, special warfare fits most closely with the third SOF support opportunity: to understand, deceive, and influence the cultural environment.

Within surgical strike scenarios such as DA, cyber-enabled special operators should focus more on cyber techniques. These operators should be highly skilled in systems and computer science and understand FRINGE technologies and their specific functions within the denied or sensitive cyber domain. As one information systems and security specialist suggests, "These teams would perform more direct and often unilateral cyber special operations, such as crippling adversaries' [command and control] systems or launching cyber-attacks to disable target defense installations or infrastructural facilities."[45] By understanding the dynamics of MA, SR, and DA operations, the cyber-enabled special operations teams could be used in the whole spectrum of SOF operations and provide support to further cyber operations.

Anti-aircraft guns guarding Natanz Nuclear Facility, Iran

Vignette for Integration Option 3

The installed spyware at the African data center was discovered by the local authorities and the whole data center was temporarily disconnected. The Navy vessel with SOMTG Trident is not in the vicinity anymore. This left Northwood in the dark, with no situational understanding of the pirates' financial network. The next opportunity for NATO to act on this is an upcoming MA exercise with several African partners. Army SOF has already been training with these African partners for several years and has built a reliable network with key local political, military, police, and Islamic leaders to support regional cultural awareness.

During the exercise, a strategic-level cyber-enabled special operations unit has blended into the Army SOF team to learn from their colleagues' cultural awareness. After a couple of weeks, under the umbrella of the MA training and with the help of some of the trusted local leaders, the cyber-SOF unit undertakes a covert campaign against the pirates in their illegal coastal camps. With their local knowledge, the members of the unit understand how to target the pirates digitally, launching social media campaigns that use the pirates' own online identities to blackmail, manipulate, and deceive the pirate leaders. This results in visible chaos and instability among the pirates, which the local authorities benefit from and which also provide NATO with better situational understanding.

Dynamics and Conditions That Will Affect SOF-Cyber Integration

It is not the intent of this section to compare the three integration options for SOF to support cyber operations and draw conclusions. Nevertheless, it is important to understand the dynamics and conditions that will affect both the SOF and cyber organizations and influence the three integration options. All three integration options require, at a minimum, a proper legal framework, dedicated resources, cultural integration, command and control procedures, and coordination at all levels to be viable. There are three critical considerations for assessing the viability of the three integration options: mission impact, feasibility, and the mitigation of possible risks.

Mission impact is defined as the efficiency and effectiveness of each integration option in meeting the goal of enhancing national cyber capabilities. Functional SOF and cyber teams are more independent of each other, whereas horizontal project teams have a very high level of interdependence. To increase their effectiveness, the horizontal SOF and cyber units need the appropriate means or mechanisms for coordinating workflows, such as rules, hierarchy, supervision, mutual accommodation, and horizontal communication.[46] Bringing these two entities, with their disparate backgrounds, types of education, and perhaps even viewpoints, together requires choosing an integration option with the best potential for deconfliction, coordination, and synchronization.

The second condition that will influence the choice of an integration option is based on feasibility, which requires setting up decisive principles for success. By examining the integration, deconfliction, coordination, and synchronization of each option, the success of the combination can be measured. It is relevant to keep the dynamics and conditions in review, however, because they will affect and influence all three integration options. For example, the legal framework will decide whether this is an intelligence exploitation operation under the umbrella of the security intelligence services, or a military operation under the direction of SOCOM or DCC. All frameworks request different juridical approaches to legitimize the type of operations.

> **Excellent leadership from both sides, along with clear lines of command, control, and coordination, will be key aspects of the process.**

As mentioned earlier, differing institutional cultures are another dynamic that will influence the feasibility of integration.[47] Excellent leadership from both sides, along with clear lines of command, control, and coordination, will be key aspects of the process. Whether the type of structure chosen for integration is centralized, decentralized, or pooled-divisionalized, a feasibility assessment should weigh barriers and points of resistance versus facilitators and drivers in the two cultures and evaluate the degree to which cyber and SOF activities are reciprocal.[48]

The third critical consideration is risk mitigation. Lessons from the Netherlands's past show that the Dutch operational commands, in particular, tend to operate in a "stove-piped" manner. Both KCT and NLMARSOF follow their own training pipelines and particular recruiting, selection, and training criteria.[49] This stovepipe approach resulted, for example, in different goals for similar Army and Navy training courses such as sniper, CT, jungle, mountain, and arctic warfare. Decentralizing these structures and delegating functions could be inefficient at this point, especially for cyber capabilities. Fortunately, in recent years, the Chief of Defense of the Netherlands has given more direct guidance to the operational commands and established joint organization components. Nevertheless, the risk of stovepipe thinking within the operational commands still requires strategic guidance and integration cooperation from the MoD. To exploit cyber warfare operations and gain the most significant effect, cyber and SOF personnel, including their capabilities, need a central structure according to the type of operations they will be expected to carry out. USSOCOM and USCYBERCOM in the United States are currently struggling with these same dynamics. Their mitigation approach is to build a Cyber Special Operations Command, as per the third organizational option described above.[50]

Other risks that require mitigation include the lack of reciprocal cultural awareness, such as different professional SOF and cyber jargons and tactical versus technical expertise. SOF and cyber staff personnel use different planning cycles, such as the cyber kill-chain and the intrusion model versus the special decision-making process. Maybe the most important risks to overcome are the biases that already exist. Winning the hearts and minds of all the personnel involved in the reorganization is essential to success.[51]

To begin this process, MoD and its constituents should bring the various stakeholders from SOF and the cyber community to the table to start brainstorming, investigate the pros and cons of the three viable integration options, and examine the effects that would be achieved within

both the SOF and cyber organizations. It will require time, effort, and resources. The MoD should start by selecting personnel and training them in both cyber craft and SOF specialized tactics, techniques, and procedures. These could be skilled cyber professionals from the private or academic sectors who are physically fit and can embrace both SOF and cyber techniques. These cyber operators should conduct sufficient training, exercises, and, ultimately, operations together with SOF personnel to be capable of meeting operational requirements. This integration demands a direct, centralized command and control that can mitigate the risks outlined above and build relations among the various strategic and operational commands.

Conclusion and Recommendations

During research for the thesis from which this article was taken, including discussions with both US and Dutch SOF and cyber professionals, it became clear that all three potential SOF roles supporting cyber operations depend on the will of the MoD to change and restructure its organization. Furthermore, integration requires a clear understanding of the strengths, weaknesses, and cultural gaps between SOF and cyber personnel and their organizations.

The strength of cyber capabilities is that, when connected with the internet, the physical location of those capabilities does not matter, which means cyber operations can stay under the radar with minimal risk for escalation. Cyber capabilities rapidly implement new ideas and technologies. On the downside for integrating with special operations is the slow pace of the decision-making process: zero days are costly and very time consuming, can be used only once, and can backfire. There is also a shortage of qualified and experienced personnel to code, hack, and battle online against the hybrid threats. For these reasons, the MoD should start cyber career paths among the various defense organizations and develop ways to retain experienced cyber experts instead of losing them to much more financially attractive civilian contracts.

> **All three potential SOF roles supporting cyber operations depend on the will of the MoD to change and restructure its organization.**

SOF have agile, adaptable, stealthy, flexible, and resilient personnel who can conduct independent and persistent operations. The SOF operators are culturally aware, speak the languages of the countries in which they work, and understand the environment in which they operate, including the risks and opportunities of that environment. They can be employed across the peace-war continuum in support of tactical, operational, and strategic-level intelligence collection in both permissive and denied areas using a range of available tools and capabilities. The current drawback for SOF personnel is insufficient cyber awareness and digital experience. Due to their physical presence in the area of operations, they are also always at a higher risk than their cyber colleagues who work at a desk back home.

To bridge the gap between the cyber experts and SOF operators, activities such as cross-training, joint exercises, and, ultimately, operations can help to increase mutual cultural understanding. Good command and control, excellent leadership, the proper legal framework, and clear communication are important but not sufficient. Both SOF and cyber personnel should also interact often and learn the basic techniques for both SOF and cyber operations. It is important to keep in mind that all integration options demand an open and unbiased view, mutual respect, clear communication, and the will to start small with simple and inexpensive cyber capabilities. Until the political and legal structures can accommodate offensive cyber operations supported by SOF, the MoD leadership should seek opportunities within the existing legal framework.

Senior MoD leadership should set the conditions that promote better and deeper integration between SOF and cyber capabilities by establishing a clear directive with national guidance. MoD leadership need not search for all the solutions, but rather must create the fertile conditions for honest discussion, and then simply listen to their SOF and cyber specialists. As the need for cyber operations continues to grow, SOF can support the development of online defensive and offensive measures by filling the physical gaps to make these cyber operations more successful.

ABOUT THE AUTHOR

MAJ Jonas van Hooren currently heads the Netherlands Marines Special Forces' future planning group.

NOTES

1. "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW," *BBC News*, 4 October 2018: https://www.bbc.com/news/world-europe-45747472
2. Laura Smith-Spark, and Katie Polglase, "Netherlands Officials Say They Caught Russian Spies Targeting Chemical Weapons Body," CNN, 5 October 2018: https://www.cnn.com/2018/10/04/europe/netherlands-russia-gru-intl/index.html
3. "NRC: Russische ambassade is spionagecentrum, was betrokken bij poging OPCW binnen te dringen," [Russian embassy is espionage center, and was involved in intended penetration of OPCW], *de Volkskrant*, 1 December 2018: https://www.volkskrant.nl/nieuws-achtergrond/nrc-russische-ambassade-is-spionagecentrum-was-betrokken-bij-poging-opcw-binnen-te-dringen~bb9402dc/
4. This article uses the terms "hybrid warfare" and "hybrid threat" in its discussion about the integration of Dutch SOF and cyber means, rather than the ambiguous term "gray zone." The European Union describes hybrid threats thus: "Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives." Frank Bekkers, Rick Meessen, and Deborah Lassche, *Hybrid Conflicts: The New Normal?* (The Hague: The Hague Centre for Strategic Studies and TNO, 2019), 7: https://hcss.nl/report/hybrid-conflicts-new-normal
5. Jaclyn Diaz, "Russia Suspected in Major Cyberattack on U.S. Government Departments," NPR, 14 December 2020: https://www.npr.org/2020/12/14/946163194/russia-suspected-in-months-long-cyber-attack-on-federal-agencies
6. This article was derived from the author's master's thesis: Jonas van Hooren, "The Imperative Symbiotic Relationship Between SOF and Cyber: How Dutch Special Operation Forces can Support Cyber Operations" (master's thesis, Naval Postgraduate School, 2019): https://calhoun.nps.edu/discover?query=van+hooren . Unless otherwise noted, all translations from Dutch to English are by the author.
7. Van Hooren, "The Imperative Symbiotic Relationship Between SOF and Cyber."
8. Wendelmoet Boersema, "Wat we Weten over de Russische Hackaanval tegen de OPCW" [What We Know about the Russian Hack against the OPCW]," *Trouw*, 4 October 2018: https://www.trouw.nl/home/wat-we-weten-over-de-russische-hackaanval-tegen-de-opcw~ad2eb078/.
9. *Special Operations Forces: Schaduwkrijgers in Het Licht van de Toekomst* [Special Operations Forces: Shadow Warriors in The Light of the Future] (The Hague: The Hague Centre for Strategic Studies, 2015): https://hcss.nl/report/special-operations-forces-schaduwkrijgers-het-licht-van-de-toekomst
10. Gorkem Yigit and Dana Cooperson, "From Autonomous to Adaptive: The Next Evolution in Networking," Ciena, January 2018: https://www.ciena.com/insights/white-papers/From-Autonomous-to-Adaptive-The-Next-Evolution-in-Networking.html
11. Department of Homeland Security, *National Security Strategy of the United States of America 2015* (Washington, DC: Department of Homeland Security, 2015), 2: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf
12. Ben Buchanan, T*he Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (New York: Oxford University Press, 2017), 31–33.
13. Lorenzo Franceschi-Bicchierai, "The History of Stuxnet: The World's First True Cyberweapon," Vice News, 9 August 2016: https://www.vice.com/en_us/article/ezp58m/the-history-of-stuxnetthe-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee
14. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), 97–98: https://carnegieendowment.org/2018/01/18/cyber-mercenaries-state- hackers-and-power-pub-75280
15. Ibid., 101–102.
16. Ibid., 98–100.
17. Miles Parks, "FACT CHECK: Russian Interference Went Far Beyond 'Facebook Ads' Kushner Described," NPR, 24 April 2019: https://www.npr.org/2019/04/24/716374421/fact-check-russian-interference-went-far-beyond-facebook-ads-kushner-described
18. "Zero Days: VPRO Tegenlicht," 12 October 2014, YouTube, 49:16: https://www.youtube.com/watch?v=JhkXSg9KQE8
19. *Special Operations Forces: Schaduwkrijgers.*
20. Patrick Duggan, "Why Special Operations Forces in U.S. Cyber-Warfare?," *Cyber Defense Review*, 8 January 2016: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/
21. Frank C. Sanchez, Weilun Lin, and Kent Korunka, "Applying Irregular Warfare Principles to Cyber Warfare," *Joint Force Quarterly* 92 (2019): https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_15-22_Sanchez-Lin-Korunka.pdf
22. Robert Koch and Gabi Rodosek, eds., ECCWS *2016-Proceedings of the 15th European Conference on Cyber Warfare and Security* (Sonning Common, UK: Academic Conferences and Publishing Limited, 2016).
23. Robert M. Gates, "Helping Others Defend Themselves: The Future of US Security Assistance," *Foreign Affairs*, May/June 2010: https://www.foreignaffairs.com/articles/2010-05-01/helping-others-defend-themselves
24. Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK: Oxford University Press, 2018), 90.
25. NATO, Allied Joint Doctrine for Special Operations, AJP 3.5 (Brussels: NATO, 2013).
26. In interviews, the author was given various first- and second-hand examples of classified operations in which SOF was used as the initial entry force to pave the way for cyber operations. These conversations were held in Monterey, California, in August 2019 with personnel from USCYBER Command, and in The Hague, The Netherlands, in September 2019, with personnel from NLDSOCOM, DCC, JSCU, and SOF.
27. Buchanan, *The Cybersecurity Dilemma*, 33.
28. "Cyber Security: Understanding the 5 Phases of Intrusion," Graylog Blog, 27 July 2020: https://www.graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion . The model was distilled from a presentation to the Enigma 2016 conference by National Security Agency (NSA) director Rob Joyce: USENIX *Enigma 2016 -* NSA TAO *Chief on Disrupting Nation State Hackers*, 28 January 2016, YouTube, 34:55: https://www.youtube.com/watch?v=bDJb8WOJYdA
29. Classified documents provided by former NSA employee Edward Snowden and published by the *New York Times* in 2013 prove this technique. See Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, 5 September 2013.

30. *Zero Days*, directed by Alex Gibney, (2016; New York: Magnolia Pictures, 2016): https://www.youtube.com/watch?v=nnKdZyS3CKU
31. This human asset was recruited by the Dutch GISS at the request of the NSA and CIA. Huib Modderkolk, "Het is oorlog maar niemand die het ziet," [It is War but Nobody Sees It] (Amsterdam: Uitgeverij Podium, 2019).
32. Buchanan, *The Cybersecurity Dilemma*, 34.
33. David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway into Computers," *New York Times*, 14 January 2014: https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html
34. Patrick Duggan, "SOF's Cyber FRINGE," *Small Wars Journal*, 10 February 2016: https://smallwarsjournal.com/jrnl/art/sof%E2%80%99s-cyber-fringe
35. Ibid.
36. Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel*, 11 February 2009: https://www.spiegel.de/international/world/the-story-of-operation-orchardhow-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html
37. Donghui Park, Julia Summers, and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," Henry M. Jackson School of International Studies, University of Washington, 11 October 2017: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
38. Patrick M. Duggan, "U.S. Special Operations Forces in Cyberspace," *The Cyber Defense Review* 1, no. 2 (Fall 2016): https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2016.pdf?ver=2017-03-27-130219-357
39. Park, Summers, and Walstrom, "Cyberattack on Critical Infrastructure."
40. Duggan, "SOF's Cyber FRINGE."
41. Interviews with Commanders NLD SOCOM and Dutch DCC, The Hague, The Netherlands, 9–10 September 2019.
42. Interview with Commander Dutch DCC, The Hague, The Netherlands, 10 September 2019.
43. Benjamin Brown, "Expanding the Menu: The Case for CYBERSOC," *Small Wars Journal*, 5 January 2018: https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc
44. In interviews with Commanders NLD SOCOM and Dutch DCC, both commanders stressed the importance of a flexible and creative mindset within SOF-cyber operations, where the command relationship is supporting or supported. The Hague, The Netherlands, 9–10 September 2019.
45. Brown, "Expanding the Menu," 6.
46. Jonathan Murphy, Hugh Willmott, and Richard L. Daft, *Organization Theory and Design* (Mason, OH: Cengage Learning EMEA, 2014), 277.
47. In interviews with Commanders NLD SOCOM and Dutch DCC, both commanders mentioned that culture and mutual understanding between SOF and cyber personnel are the primary foci for sustainable integration. The Hague, The Netherlands, 9–10 September 2019.
48. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory*, 7th ed. (New Brunswick, NJ: Transaction Publishers, 2003).
49. Commander NLMARSOF has no issues with NLMARSOF having its own specialized courses. However, he noted that cyber integration needs to be coordinated from the strategic level for both NLMARSOF and KCT. Conference call with Commander NLMARSOF, 26 September 2019.
50. Brown, "Expanding the Menu," 7.
51. Interview with Commander Dutch DCC, The Hague, The Netherlands, 10 September 2019.

Causes of the Ongoing Mass Radicalization of Islam in Pakistan: An Ethnography

Dr. David D. Belt, National Intelligence University

RELIGIOUS RADICALIZATION IN PAKISTAN, a nuclear-armed, Muslim-majority country of 195 million souls, has been a source of concern to its neighbors and others around the world for a long time.[1] What specific factors are driving this radicalization? This article, the first part of a two-part ethnographic study, addresses this question through digitally-recorded in-person narrative interviews with 25 diverse Pakistanis from all regions of the country.[2] Each of them is well-placed in government, civil society, academia, non-governmental organizations (NGOs), or political and religious movements, and is actively involved in promoting, countering, or researching the more significant Islamic movements. These interviews add value to the literature on radicalization by revealing the interviewees' personal and professional senses of the likely longer-term future of extremism in Pakistan. The running commentary that accompanies the discussion addresses the relevant literature where it may enhance the reader's understanding.

The grounded theory approach to the interviewees' free-flowing unstructured narratives identified a range of factors shaping extremism that can be arranged into a useful conceptual framework.[3] This framework and the causal categories that emerged from the present study might serve as an approach to understanding the emergence of

Mingora City, Swat Valley, Pakistan

extremism or to predict the future of extremism, not only in many Muslim-majority countries but in any country where extremist movements are gaining ground. This conceptual framework will be described at greater length in the second part of this study, which will appear in a subsequent issue of *CTX*.

To gain access to a wide range of subculturally distinct interviewees for this ethnography, and to gain their un-adulterated, non-self-censored perspectives, the interviews for this project were conducted by a Pakistani citizen, "X," who— because of his similar work on the subject—has sufficient cultural and social capital with his subjects. I first met X in 2006, when I was developing the curriculum for the course "Containing al-Qaedaism" at National Defense University, Washington, DC. At that time, X was involved in countering extremism in a key sector of Pakistan that cannot be divulged here. Many years later, I informally partnered with an international NGO, which also must remain anonymous, to conduct a study of religious radicalization across nine global regions,. The project started in Pakistan about five years ago, with X as our country expert and researcher, but before we could expand the research further, the project's funding fell through. My partnering organization and X gave me permission to use these insightful narrative interviews on the condition that I remove all personal identifying information. To preserve the anonymity of the interviewees, which is necessary to prevent retribution and preserve the ethnographic value, they are identified as "Source 001," "Source 002," and so on (see Appendix 1: List of Interviewees on p. 54 for a quick reference to participants' affiliations).[4]

The Radicalization of Pakistan's Religious Landscape

Most of the interviewees described a country that was undergoing what I term "mass-level" radicalization, but this term has to be taken on a relative scale. Interviews with Pakistani-Americans whose families frequently travel between the two countries and analysis by Brookings Institution researcher Madiha Afzal suggest that support for extremism in Pakistan is not all-pervasive.[5] Rather, Pakistan is akin to what Samuel Huntington, in his provocative 1996 book, *Clash of Civilizations*, described as a cleft country, "with sizeable groups of people from different civiliations."[6] Analogizing from Huntington's idea, we can view Pakistan as a country cleft by sizeable groups of people who hold different worldviews: for example, secular society versus Islamists, and the large minority of more extremist Deobandi and Wahhabist Sunnis versus the less fundamentalist majority Sufi Barelvi Sunnis.[7] The term "mass-level," therefore, does not denote a society-wide phenomenon, but rather indicates much greater structural support for extremism than is the case in many other Muslim-majority countries.

> **Pakistan is akin to what Samuel Huntington described as a cleft country, "with sizeable groups of people from different civiliations."**

Source 004, for example, who worked for an organization in northern Punjab that produced a counternarrative to Islamic extremism, described Pakistan as being in a crisis, asserting that "the whole society has become a factory of radicalization." Source 007, a government official in Peshawar, similarly said of religious extremism, "I think this is deeply rooted in our society."

We set out to examine which particular combination of factors is currently driving the radicalization of Pakistan's religious landscape. To organize the answers to this question from the narratives, this ethnography uses a conceptual framework for radicalization developed by the Quilliam Foundation, a London-based think tank composed mainly of former Muslim extremists. In its 2010 briefing paper, *Radicalisation on British University Campuses: A Case Study*, Quilliam approvingly quotes a segment from the British government's Channel program for countering violent extremism,[8] which describes the radicalization of Muslim university students in the UK in terms of four primary contributory factors, in no particular order of importance:

> 1. [E]xposure to an *ideology* that seems to sanction, legitimize or require violence, often by providing a compelling but fabricated narrative of contemporary politics and recent history.
>
> 2. [E]xposure to *people or groups* who can directly and persuasively articulate that ideology and then relate it to aspects of a person's own background and life history.
>
> 3. [A] crisis of *identity* and, often, uncertainty about belonging, which might be triggered by a range of further personal issues, including experiences of racism, discrimination, deprivation and other criminality (as victim or perpetrator); family breakdown or separation.
>
> 4. [A] range of perceived *grievances*, some real and some imagined, to which there may seem to be no credible and effective non-violent response.[9] (Emphasis in the original document.)

With this framework in hand, we can begin to explore each of these factors within the context of radicalization in Pakistan.

Ideology

Within the broad factor of ideology, the interviewees' more specific responses can be divided into the ideologies of Islamism, pan-Islamism, caliphatism, Salafism, jihadism, takfirism (an extreme form of sectarianism that holds the majority of Muslims to be apostate), anti-Westernism or conspiracism, and taqlidism (a doctrine of strict conformity and/or unquestioning obedience to the teachings of one's primary religious authority).

Islamism, Pan-Islamism, and Caliphatism

Islamism—the notion that the political system should be Islamic rather than secular—is hegemonic in Pakistan, with deep cultural roots. Source 025 described Pakistan's current extremism in terms of its Islamist political culture, which is institutionalized in its founding legal structures going back to 1949. Pakistan's pre-constitution "Objectives Resolution," in 025's words, constituted "an open license that this state will be an Islamic state." This notion is well-established in the literature, implicating the religious political movement Jamaat-e-Islami (JI) and its founder, Maulana Abu Ala Maududi, as being instrumental in this minority rejectionist, pre-takfiri trend, and also for bringing clerics—an "Islamic lobby"—into the mainstream

of politics in pre-Partition Punjab.[10] Source 025 added that advocates of the Objectives Resolution, like Liaqat Ali Khan, the nation's first prime minister, were part of the "caliphate movement, pan-Islamism."[11]

> **Pakistan's pre-constitution "Objectives Resolution," constituted "an open license that this state will be an Islamic state."**

Source 012, a Salafist affiliated with the Ahl-e-Hadith movement, members of which are often referred to as Wahhabis,[12] also identifies with caliphatism, or the "one ummah" movement, which seeks to unite all Muslims under one global caliphate. His comments revealed why support for ISIS and for the notion of a caliphate broadly has been so ascendant. "In Islam," 012 said, "there is no concept of geographical boundaries and nation states. Instead, there is only the concept of the ummah. … Even if a Muslim lives in India, America, or Russia, he is still a brother. It is then fine if someone wants to go and help his brother, through jihad in other countries."

Source 022, a government official who writes columns for a Pakistani newspaper, and who was interviewed in Mardan, described revolutionary extremism in Pakistan as a function of a broad and growing subculture of "caliphatism"—a pan-Islamic "one ummah" yearning for a United States of Islam, or one large Muslim country. 022 said, "Our scholars, ulema, say that Islam does not accept the nation state and discourages national boundaries."

All of these pan-Islamic sentiments for a caliphate, however, don't necessarily translate into hostility toward the West or Westerners. In 2009, I spent a week traveling in China with the head of JI's Institute of Policy Studies, during which time we had wide-ranging conversations about religion and politics that lasted for many hours. This staunch pan-Islamist gravitated toward me as an American Christian, and there was not a hint of extremism in his worldview. Yet, his opinions were revolutionary in terms of delegitimizing secular and nation-state government structures for Muslim majority countries.

The political cultures of caliphatism and pan-Islamism provide the platform for the other more violent forms of extremism that Pakistan is now plagued with—namely, Salafism and its two offspring, jihadism and takfirism.

Salafism and Wahhabism

Salafism, along with its antecedent Wahhabism, is a puritanical movement within Sunni Islam that has been spread all around the world by Saudi Arabia. According to Dr. Mubarak Ali, a prominent Pakistani historian, a significant segment of Pakistan's population has undergone Wahhabization, or, in his word, "Arabization."[13] The political influence of this fundamentalist sect has been so significant that some describe Pakistan as the "Wahhabi Republic."[14] According to Iqbal Haider, Pakistan's former law minister, "whether they are the Taliban or the Lashkar-e-Taiba, their ideology is Saudi-Wahhabi without an iota of doubt."[15] This is of strategic concern because Pakistan's population is seven times larger than Saudi Arabia's. Wahhabis and Deobandis together comprise about 20 percent of Pakistan's Muslims, while the Sufi Berelvi community is estimated to comprise about 60 percent.[16] Along with the Shi'a, who make up most of the remaining twenty percent of Pakistan's population,[17] the Berelvi community has traditionally eschewed violence and stood as a counternarrative to Salafism.[18] More recently, however, this "us vs. them" mentality and the spread of violent rhetoric and practices in the society as a whole seem to be gradually stransforming Berelvism, lowering the threshold of violence within the community and its political party, Tehreek-i-Labiak.[19]

> **Fundamentalist politics has become so entrenched in Pakistan that the country has been referred to as the "Wahhabi Republic."**

Source 004 corroborated this problematic trend, describing Pakistan as being in a crisis and asserting that "the whole society has become a factory of radicalization." 004 saw Salafism, rather than non-religious factors such as political grievances, as the basis for much of this extremism.

The problem for Pakistan, said Source 008, a professor and former dean at an Islamic university, began when Salafis from the Wahhabi tradition began to inject their beliefs into the traditional Pakistani Hanafi fiqh, or jurisprudence, mainly through "religious schools and madrassas." Source 008 was talking about the way that Wahhabi Salafism influenced Hanafi ideologues in the late 19th-century to create Deobandism, a South Asian version of Wahhabi Salafism that emerged from the Islamic university in India, the Darul Uloom Deoband.[20] Essentially Salafist in their outlook, the Deobandi ulema (scholars) were also a key part of the problem, according to Source 023.

Source 025 added that the Salafization of Deobandism had "matured," or become suffieciently hegemonic, by 2001, with significant proselytizing by Saudi Arabians. This view is corroborated in the literature, specifically by Arshi Saleem Hashmi, who is on the faculty at National Defence University, Islamabad.[21]

Source 012, a Salafist affiliated with the Ahl-e-Hadith movement, was working to counter the violent sectarianism that plagues Pakistan. Although he was quick to share with a fellow Muslim interviewer that jihad is "about fighting disbelievers, such as Russians, India, America," 012 hinted at a hopeful trend of counter-sectarianism in Wahhabi ideology, adding that jihad is "not a concept of relations between Muslims, or Sunni and Shi'a."

Source 020, an activist within the pro-US Awami National Party (ANP), who has a large social media presence directed at countering violent extremism, characterized Pakistan's violent extremism as having "spread to a large extent" due to the growth of Salafism. For Source 020, it was not religious education that needed reform as much as the religion itself: "Most important, actually, our religion is biased; it needs reinterpretation." "Some verses and hadith," 020 added, "are problematic about religious harmony." Given the Salafization of the religious landscape, 020 painted a bleak future for Pakistan in terms of extremist ideology.

Jihadism

According to the interviewee narratives, Islam in Pakistan has been infused with the ideology that holds violent jihad to be obligatory, a kind of sixth pillar of Islam. Source 006, a highly educated and accomplished resident and activist of Pakistan's Swat district, who leads a civil society organization focused on containing extremism, lamented that the Islamism enshrined in Pakistan's founding has shaded to jihadism; the two are one and the same, at least in the Swat district. In his words, "nowadays, it is general thinking that 'jihad is religion.'"

Defensive Jihadism

At least a third of the interviewees were supporters of what we might call "defensive jihadism," an Islamic just-war doctrine that holds that militancy is mandatory in the defense of any Muslim group that has come under occupation or is

The Eastern Public School & College, District of Mirpur Khas, Pakistan

experiencing other forms of injustice from non-Muslims.[22] For these non-violent interviewees, defensive jihadism is not viewed as a form of extremism. Occupation of Muslim lands is a red line that, according to prominent Islamic jurisprudence, such as Yusuf al-Qaradawi's definitive 2009 *Fiqh of Jihad,* obligates Muslims to repel the occupier.[23] Source 001, a civil society activist working to contain militant extremism, described the Soviet invasion of Afghanistan in 1979 as an initial catalyst for the rise of defensive jihadism in Pakistan: "people got inspiration from Afghanistan as they considered them their religious brothers which were under attack."

Source 003, a Salafi, echoed the mainstream Islamist just-war doctrine that holds the entire global Muslim population as the nationalist or kinship entity to which defensive jihadism applies. "If you live in a Muslim state and the state does not allow for jihad," he said, "then you can migrate to the place where jihad is going on." In this way, a Muslim can fulfill the obligation to defend fellow Muslims under occupation simply by changing citizenship, rather than by receiving religious injunctions from imams or clergy. Source 005, who holds a doctorate degree, similarly saw jihad as absolutely essential for the survival of the community of the faithful, saying that "if Muslims do not engage in jihad, they will be destroyed." Pakistan's government *does* allow for jihad, and it must continue to do this if it is going to maintain legitimacy in the eyes of the country's many Islamist political factions.

> **Source 005 saw jihad as absolutely essential for the survival of the community of the faithful, saying that "if Muslims do not engage in jihad, they will be destroyed."**

Source 010, a well-known Islamic scholar with a YouTube presence who focuses on containing sectarian violence, is a proponent of defensive jihad and made a distinction between it and illegitimate violence. "Where Muslims are oppressed—e.g., Palestine and Kashmir," 010 said, "jihad is obligatory even for Muslims who are not living there." Source 011's worldview also reflected the wider general support for violence in the name of religion in Pakistan. Source 011, who is an imam at a well-known madrassa, the editor of a prominent Islamic journal, and a political representative, criticized the popular media for denigrating the notion of a more militant jihad. 011 advocated Hafiz Muhammad Saeed's vision of jihad, which he claimed is supported by the Pakistani government. Saeed is the chief or amir of the jihadist group Jama'at-ud-Da'wah (JuD), and a co-founder of Lashkar-e-Taiba (LeT).[24] He has advanced the irredentist defensive jihad position that India will be forced to leave Kashmir just as the United States was forced to leave Afghanistan. In 2014, the US State Department banned JuD as a foreign terrorist organization and a front for LeT.[25]

Source 012 agreed that jihad "is obligatory on Muslims" and "is necessary to fight against oppressors in places where Muslims are oppressed by non-Muslims, such as in Kashmir, Afghanistan, and Palestine." Under this doctrine of defensive jihadism, 012 said, "the Kashmiris are in the right to fight for their freedom as they are fighting against kuffar [non-Muslims or infidels]."[26]

Source 021 is a Salafist and also a member of Markazi Jamiat Ahl-e-Hadith (JAH), Pakistan's only Salafist political party, which is part of the broader Salafist or Wahhabist Ahl-e-Hadith movement that began in India in the mid-nineenth century.[27] 021 cited JI founder Maulana Maududi's description of state-led defensive jihad, which is also the position of the Pakistani government: "jihad is only legitimate if it is endorsed by the state, and it must be conducted to protect Islamic countries," and "jihad is legitimate if kuffar attack a Muslim state."

Offensive Jihadism

Speaking more on the notion of *offensive* jihad to advance Islam, Source 016, a former Deobandi and deputy amir within the JAH, said that "jihad is an undisputed fact of Islam," but added, "if there is an Islamic revolution through which a purely Islamic state is established, only then, under the orders of the amir, will jihad be legitimate."

Source 012 had sympathies with the principle of offensive jihad that he was quick to share with a fellow Muslim interviewer, believing that jihad is "about fighting disbelievers, such as Russians, India, America." 012 countered the sectarianism that plagues Pakistan, saying that jihad is "not a concept of relations between Muslims, or Sunni and Shia."

Source 021 suggested that the ideology of offensive jihadism benefits the Gulf monarchs and other authoritarian regimes, and that this is why JAH is supported by the Saudis and the Pakistani government. As a kind of regime security strategy, the Saudi and Pakistani governments have promoted jihad against non-Muslims, while simultaneously denigrating the takfiri form of jihadism that tends to view both of these authoritarian and corrupt regimes as illegitimate and insufficiently Islamic. 021 explained, "terrorism conducted against the current political leaders

challenges the writ of government and creates anarchy and chaos, or fitna, which is not allowed in Islam." In this sense, 021 advocates for what might be called a state jihadism, which is staunch support of state-legitimated and directed jihad against the enemies of true Islam. "Jihad is a struggle or 'fighting in the way of God,'" 021 said, adding, "this means fighting against the kuffar, not against other Muslims." In other words, jihad is legitimate if not directed at other Muslims. Pakistan, 021 explained, "is an Islamic state ideologically," and "it is the duty of the government to work through state media to promote the true meaning of jihad, and properly distinguish between jihad and terrorism." Furthermore, 021 said, "It is the responsibility of the current government to promote jihad, and thereby elevate faith/religion."

> **"It is the responsibility of the current government to promote jihad, and thereby elevate faith/religion."**

Takfirism

Violent extremism in Pakistan also flows from the Salafi-inspired sub-doctrine of takfirism, or the takfiri mentality. The term comes from the verb *takfir*, or the religious practice of excommunicating Muslims who are deemed to be heretical or insufficiently Islamic, and who are thus seen as obstructing the unification of Islam into a global caliphate. Typically, the proximate cause of this practice of declaring another Muslim to be apostate is to provide the religious legitimacy to kill that person. There are two forms of takfirism. One is the kind embraced by al- Qaeda ideologue Ayman al-Zawahiri in his fight against Muslim states that were, in his eyes, interfering with the quest for the global caliphate. Like Iran's Supreme Leader Ayatollah Ruhollah Khomeini, al-Qaeda's leadership viewed most of the present governments ruling over Muslim lands, incuding Gulf monarchies like Saudi Arabia, to be illegitimate and apostate; thus, jihad against them was legitimate.[28] Another form of takfirism is an outgrowth of the sectarianism that emerged in Saudi-backed Salafism.[29] It excommunicates from the ummah what Salafis view as heretical forms of Islam, such the Shi'a and Ahmadiyya in Pakistan, in order to bring about a pure, unified Islamic state, or caliphate.

The takfiri trend emerged in Pakistan in force nearly four decades ago, when Maulana Haq Nawaz Jhangvi, heavily influenced by Salafism or Wahhabism, declared Shi'a to be kuffar. He broke away from the main Deobandi Sunni organization Jamiatul Ulema-e-Islam in 1985 to found the Sipah-i-Sahaba Pakistan (SSP), or Guardians of the Prophet's Companions. Banned by President Pervez Musharraf in 2002 as a terrorist organization, the group has survived with Gulf state funding and rebranding that allowed it to avoid the law, changing its name first to Millat-e-Islamia and currently to Ahle Sunnat Wal Jamaat, under which it also functions as a political party.[30] Since then, other Pakistani Salafist groups known for their takfiri-sectarianist and jihadist ideology have emerged, including JuD and SSP offshoots Lashkar-e-Jhangvi (LeJ) and Tehrik-i-Taliban Pakistan, or the Pakistan Taliban.[31]

Source 018, a researcher with a graduate degree who is a member of the JAH, described this takfir trend as "a disease that is eating us up. We are all supposedly Muslims but if you look into each neighborhood, each calling the other kafir. In one masjid [place of prayer], it was written outside that only people of that denomination are welcomed. For other [denominations], there was a fine. In another masjid, someone of a different denomination came and they literally washed the masjid after he left."

Source 020 feared that the spread of takfirism in Pakistan would lead to the genocide of non-Sunni, non-Salafist Muslims. This form of sectarianism, spreading out of the Jhang District in central Punjab, has already engendered a vicious cycle, as both Sunni and Shi'a clerics condemn each other's practices as heretical. Takfirism is so deeply embedded across the Sunni community that many of Pakistan's Deobandis have joined ISIS to kill Shi'a and Alawites in Iraq and Syria.

Source 011 pointed to Muhammad's statement that, "my ummah will be divided into 73 sects but only one will be the right path, the one that leads to me and my companions." Referring to the Sunni-Shi'a conflict in Pakistan's remote Kurram Agency, adjacent to the North Waziristan tribal district, Source 018 declared that some in Waziristan "are non-Muslims and the position of Pakistani scholars is also that they are not Muslims."[32]

Source 010 legitimized both global jihadism and takfirist militancy against the government. "If any country does not wage jihad against the kuffar," he said, "then it is necessary to reform or replace the government." Reinforcing the predominant narrative of takfirism, Source 005 declared, "The current leadership are merely Muslims by name." Source 008 similarly said that Pakistanis "feel that our government … follows American policy," implicating the government as being complicit with or a proxy of what the takfiri narrative calls America's "war on Islam." This anti-government sentiment further fuels takfirism,

008 said, and its adherents "follow a philosophy of the nearest enemy, because attacking this enemy [the Pakistani government] is easier than attacking the distant enemy [the United States]."

> **"Attacking this enemy [the Pakistani government] is easier than attacking the distant enemy [the United States]."**

Anti-Westernism, Antisemitism, and the "War on Islam" Conspiracy

Another set of intervening or contributing factors in the spread of radical views includes antecedent ideologies or mentalities that provide fertile ground for violent extremism. First is the ideology of anti-Westernism, which is tinged with conspiracy-thinking. Source 008 pointed to a deep societal master narrative that fueled anti-Western extremism in Pakistan, a "narrative which leads them toward extremism": namely, that "the West is doing cruelty with us and the current war against terrorism is a crusade under which the Western forces come here against Islam." "In their minds," 008 elaborated, "this is a war between Islam and Christianity."

Source 010 cited references within the Qur'an about Jews and Christians to conclude that "the US and UK can never be friends or sympathizers with Pakistanis." Although opposed to sectarianism within Islam, 010 embraced the broader Salafi narrative that framed non-Muslims as enemies. "Anyone who has not read the kalma [Shahada—testimony of faith]," 010 said, "is an enemy of Islam." This interviewee, who is working to counter sectarian infighting amongst Muslims, has normalized the doctrine that Islam is the enemy of all non-Muslims, regardless of whether they are "people of the Book," i.e., followers of the Old Testament.

Source 012 also reflected this conspiracy mentality, shifting the blame for Pakistan's religious violence to foreigners: "every religion has sectarian divisions, but foreign powers have been exploiting divisions within Islam to give the religion bad publicity." Source 012 showed sympathy for the nearly universal "war on Islam" master conspiracy narrative, arguing that "the West has targeted 'jihad' because they want to bring about Westernization," and adding

Maulana Sami ul Haq of the Jamiat Ulema-e-Islam, seated center, in glasses.

that "the US and its allies are targeting Islam." 012 further noted that "the US is [the] largest weapon-producing state and it is invested in protecting the interests of the weapons industries. Therefore, making war is in the best interest of the US." Source 012 added that, "during the Cold War, Muslims supported the US. However, in order to justify the presence of NATO and the influx of weapons, the US needed to develop a new 'soft enemy,' and they began to set the Muslims up as the next enemy after the USSR. It was easy to exploit the Muslims, as they are illiterate, poor, and lack unity." 012 then claimed that "9/11 was an inside job," and that the American government is "the real enemy of Muslims," meaning more traditionalist Muslims, since "liberal/secular Muslims are rare, but their voice is magnified by the media, which is supported by US funding."

Source 018 expressed a more conspiracist "us vs. them" binary regarding non-Muslims. "Kafir is our enemy," he said, adding, "it says in the Qur'an that even if they become our friends, they will still turn their backs on us."

The second factor encouraging the spread of radicalism was antisemitism, which emerged in a few of the narratives. According to one general officer of the largely Islamized Pakistani military, conspiracy theories about Jews abound throughout Pakistan.[33] Source 011 described an antisemitic subculture in Pakistan and demonstrated his own inclination toward conspiracy-thinking by implicating the "hidden hand" of the Jews. 011 elaborated with a story from the early history of Islam, when the prophet Muhammad attempted to ally with the Jews in Medina. "The Jewish community created division within Islam," 011 declared. The Medina Jews "were pretending but actually were not Muslims and attempts were made to create *fitna* [tribulation] in order to weaken Islam's foundation."

Taqlidism

Both high general illiteracy and high religious illiteracy, along with a lower propensity for critical thinking among some segments of society, also provide fuel to rising violent extremism in Pakistan. Only 52 pecerent of youth stay enrolled in primary schools until fifth grade, and—according to the Annual Status of Education Report, 2012—few of those who do not drop out are actually learning.[34] Many students leave school due to cultural norms and economic demands, with the result that Pakistan's adult literacy rate is an abysmal 55 percent.[35] These educational deficiencies lead to a form of uncritical or blind faith known as *taqlid*, in which believers follow what one of the interviewees described as "bad" religious leaders and "militant mullahs" unquestioningly, as a way of demonstrating faithfulness to God. This propensity to follow religious extremists is stronger where cultural norms and lack of education prevent people from reading the religious scriptures and thinking for themselves. The problem of taqlid was reflected in several of the iterviewees' statements.

Educational deficiencies lead to a form of uncritical or blind faith known as *taqlid*.

Source 014, a lecturer in the former Federally Administered Tribal Areas (FATA) of Pakistan, which is now merged with the province of Khyber Pakhtunkhwa, similarly framed militancy in Pakistan mainly as a function of illiteracy. Literacy in the FATA-KP region is "very low," he explained, which makes "people easily influenced by extremists"; in other words, "the lack of education is the major cause." Source 010 also pointed to "lack of education," meaning that Pakistani students are not taught about the world and not taught to think critically or exercise reason, so they have little defense against those who try to indoctrinate them into militancy. Reflecting on the sources of extremism in Pakistan, Source 015 also pointed to how the schools "are not inducing the mentality of critical thinking."

It is in this context of illiteracy and cultural predispositions to uncritical thinking regarding religion that taqlidism emerges. Source 003, for instance, described sectarianism and other forms of extremism in Pakistan as a function of a taqlid mentality: "people blindly follow religious authorities, instead of reading the Qur'an or hadith themselves." Source 016, similarly, said that pervasive illiteracy provides fertile ground for extremism in Pakistan; he believed that "sectarianism is caused by a lack of critical thinking and education as well [as] blindly believing in rumors and following bad leaders." Source 017, the president of an NGO in Islamabad, also noted this tendency to follow religious teaching without question: "Our people blindly follow the instructions of these militant mullahs without any verification," adding that "the main problem [that] contributes to the expansion [of extremism] is illiteracy."

Socialization into Extremism

"Socialization" into extremism entails radicalization through interested agents, which include individuals and groups, both internal and external to one's society, such as the news media and, especially, the more personally intimate social media.

All of the 25 interviewees across Pakistan's various districts gave this factor of socialization primacy equal to the extremist ideologies themselves. They described a continuum of Pakistani and foreign non-state groups and local and foreign state government actors, all of whom find that certain kinds of violence against certain others can come in handy, and who therefore actively propagate it. For example, Source 015, who resides in the Khyber Pakhtunkhwa area and is a renowned figure in Pakistani society and a regular contributor to one of Pakistan's major newspapers, described three main actors who find militancy useful and who therefore actively promote it by various strategies:

> There are various aspects/sides and all are important. The first side is individual organization, specifically the militant organization that strategizes to permeate the militant discourse or narrative in society. The second is the state components, which give birth to extremism. There are various state institutions, such as the education system, the media, or laws of the state, which, in one way or the other, promote extremism. The third is the various foreign states and their policies—and sometimes our own policies—which triggered extremism.

What all parts of this socializing power network have in common is that each finds forms of violent extremism useful to attaining its own interests.

Saudi Arabia's Salafization Strategy to Contain Iran and the Islamic Democracy Movement

The first agent of socializing Pakistanis into extremism is Saudi Arabia's foreign religious proselytizing, especially that of its Wahhabi clerical establishment. Several of the interviewees described Saudi Arabia's powerful decades-long strategy to Salafize Pakistan as part of its defense-in-depth against a perceived expansionist Iran and against the Islamic democracy movement embodied by Islamists such as the Muslim Brotherhood.

Beginning in the 1980s, the minority sect of Deobandism in Pakistan was heavily influenced by Salafism proselytized by Saudi organizations, in particular the Saudi Islamic International Relief Organisation and the Muslim World League. Deobandi groups such as the Taliban, Tehrik-e-Taliban Pakistan, and Lashkar-e-Taiba still receive funding from various Gulf-based Salafi organizations.[36] A 2013 European Union Parliament policy report states: "According to the Wikileaks' cable #178082, jihadi recruitment networks were established in Punjab and supported with the funding of Saudi Arabia and the United Arab Emirates since 2005."[37] Source 014 echoed this, adding that it's "not only the militants" who are receiving foreign funds, but also "the state institutions and agencies."

The minority sect of Deobandism in Pakistan was heavily influenced by Salafism proselytized by Saudi organizations.

As was mentioned previously, Markazi Jamiat Ahl-e Hadith (JAH), or Party of the Tradition of the Prophet, is Pakistan's only Salafist party. In the words of Bizaa Zeynab Ali, a Pakistani doctoral fellow at New York University, JAH "overtly fosters militant jihadist networks in its midst," is "sustained by free-flowing Saudi money, assisted by a mainstream political party"—the Pakistan Muslim League—and is "protected by Pakistani intelligence services," meaning Inter-Service Intelligence, or ISI.[38] Source 012 likewise mentioned "other Muslim countries" that "are exploiting Pakistan and spreading sectarianism, because Pakistan is poor and dependent on them for aid/assistance/funds." 012 pointed to the Pakistani province of Baluchistan and its capital, Quetta, where "there have been some incidents of sectarian conflict fueled by foreign funding." In Baluchistan, the general consensus in the literature is that the Saudis are behind most of the problem, through their funding of anti-Shi'a groups on the border with Iran.[39] Source 007 described the problem in terms of "foreign funding."

Although anti-Shi'a sentiments in Pakistan had been on the rise since the 1948 Objectives Resolution, which instituted the Wahhabization of the state, the literature suggests that anti-Shi'a sectarianism emerged noticeably in the 1980s, and that this change was a function more of politics, rather than religion.[40] Pakistani researcher Aarish Ullah Khan, for instance, notes that "all the militant religious organizations in Pakistan that are involved in terrorism today originated in the period after 1979." He explains that "this epochal rise in religious radicalism was due not only to the personal inclinations of General Zia [Mohammad Zia-ul-Haq, president of Pakistan from 1977 to 1988], but also to the international and domestic political situation that arose after the Iranian revolution and the Soviet invasion of Afghanistan in 1979."[41] Khan adds that "the Sunni Islamization programme initiated by Zia antagonized Pakistan's Shias, and the consequent Sunni–Shia hostility provided the cornerstone for the violent sectarian conflict in Pakistan that followed," noting that it was "reinforced by the developing jihadi culture of the time and the [Shia] Islamic revolution in Iran." In other

words, Khan writes, "the 1979 Iranian revolution and the 1980–88 Iraq–Iran War resulted in a peak in Arab–Iranian rivalry that was reflected in the form of Sunni–Shia hostility in Pakistan, with consequences that both brought new support to and radicalized the opposing sects in Pakistan."[42] Other researchers have come to the same conclusion. Rohan Bedi states that "sectarian conflict in Pakistan is the direct consequence of state policies of Islamisation and marginalisation of secular democratic forces," and that this all "began with the Iranian Revolution of 1979, and the transformation of the secular Pakistani state by General Zia ul-Haq."[43]

But in no small part, the sharp rise of sectarianism in the 1980s was a matter of identity insecurity: the Pakistani Sunni majority feared an assertive Shi'a minority that began to enjoy much greater legitimacy due to the pan-Islamist momentum of the 1979 Iranian Revolution.[44] General Zia interpreted the Shi'a population's quest for greater political and religious rights as an indication of Iranian subversion. In response to Ayatollah Khomeini's support for Pakistan's Shi'a organizations, Zia invited Saudi Arabia to similarly sponsor Sunni organizations in Pakistan.[45] At the time of the revolution in Iran, Sunnis feared that people might "seek conversion from the Sunni faith to Shiism in order to seek exemption from zakat (the annual tax of 2.5 per cent on the savings of Muslims to be distributed among the poor) or from other, more rigid Sunni family laws."[46] It was in this context that vigilante Sunnis created Sipah-e-Sahaba Pakistan (Army of the Companions of the Prophet) in 1985 as a check on what was perceived as a major rise in Shi'a power.

Pakistan's anti-Shi'a takfirism was "created" after the Iranian Revolution in the 1980s so that "the Shi'a revolution would not spread in the region."

Most of the interviewees corroborated the literature's description of events, with some interesting nuance. Source 013, a high-level activist in the secular Awami National Party's student wing, explained how Pakistan's anti-Shi'a takfirism was "created" after the Iranian Revolution in the 1980s so that "the Shi'a revolution would not spread in the region." Source 013 further explained that anti-Shi'a militancy continues to be proselytized today at madrassas and mosques, and by Saudi-funded ulema. Thus, Pakistan's violent extremism problem was not so much fundamentalist Pashtunwali or tribalism, 013 said, but rather Saudi Arabia's "planned process for a specific program to contain the USSR and now Iran." Source 020 echoed this idea: prior to this Saudi campaign, "the attitudes of the people towards Shi'a were normal, cooperative, harmonious."

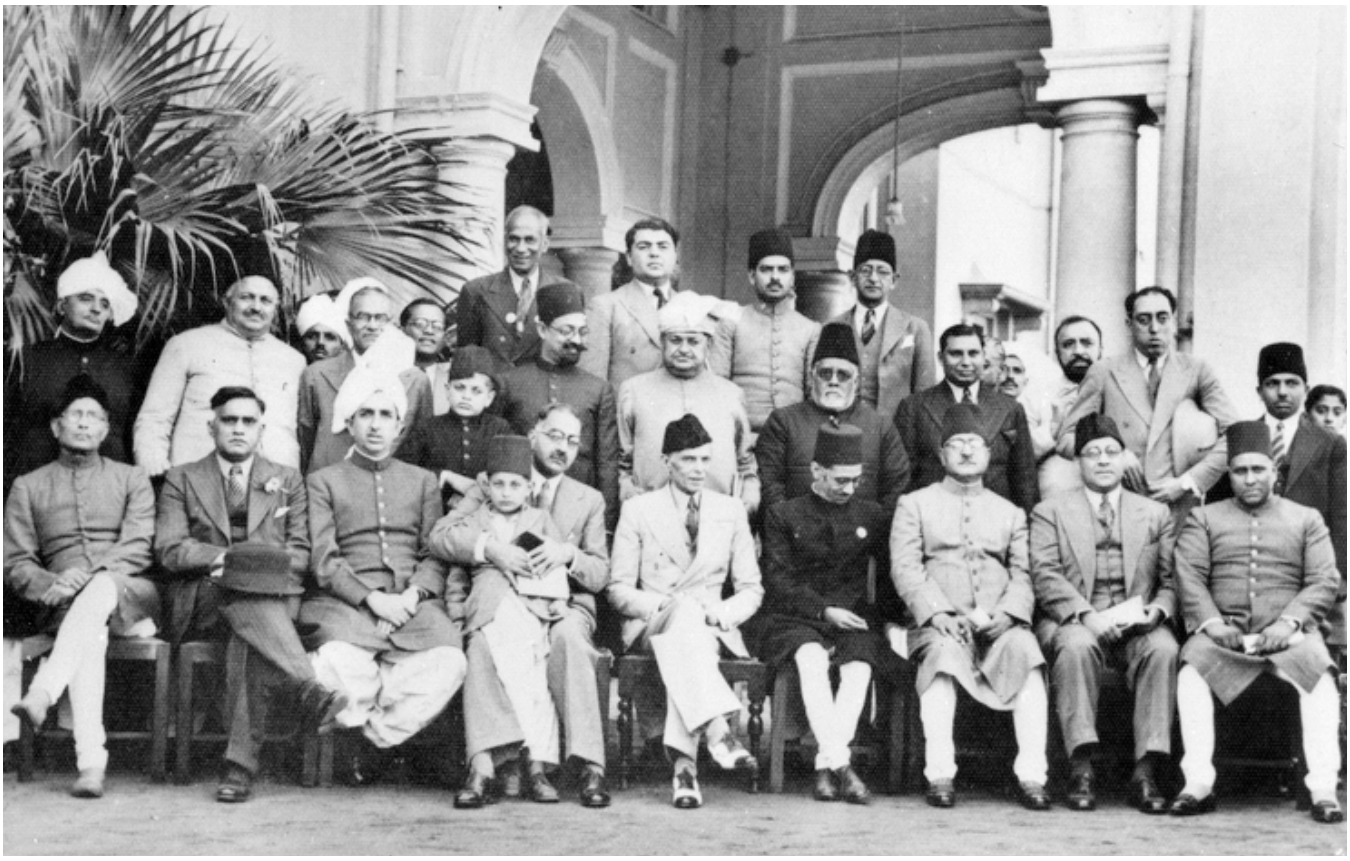
State-Sponsored Radicalizing Structures

The second major socializing source of radicalization, and one that will likely worsen in coming years, is the Pakistani government's alliance with Islamist movements. This alliance began with the tenure of President Zia-ul-Haq, who not only Islamized the state, but also nurtured violent extremist groups as part of Pakistan's defense-in-depth strategy against its archenemy, India. State-sponsored extremist groups like Lashkar-e-Taiba used violence to destabilize India's presence in Kashmir, and the state-sponsored Taliban helped destabilize Afghanistan to deny India a strong ally on Pakistan's western border.[47]

Hussain Haqqani described the problem of extremism as the state's ideology and its strategy, embodied in its two dominant institutions, the military and Islam.

Source 024 described Zia's strategy as a "military-mullah alliance." Hussain Haqqani, Pakistan's ambassador to the United States from 2008 to 2011 and an established scholar of violent extremism within Pakistan, corroborated this characterization. In his book, *Pakistan Between Mosque and Military*, Haqqani described the problem of extremism as the state's ideology and its strategy, embodied in its two dominant institutions, the military and Islam.[48] Haqqani described how the perception of foreign and domestic threats produced a mutually beneficial alliance of expediency between the Islamists and the military that has become an ensconced religio-political apparatus.[49] Both Zia and General Pervez Musharraf (president from 2001 to 2008, following a military coup) benefited from this nexus of the religious and military establishments, which received huge amounts of funding and equipment from the United States and Saudi Arabia in the fight against Soviet expansion in Afghanistan.[50] Extremism became even more economically useful after 9/11, as the central government, the Pakistani Army, and the ISI began playing a "double game," taking over $33 billion from the United States in military assistance and economic aid under the guise of countering some extremist groups, while secretly nurturing those groups, including the Taliban and others, and maintaining plausible deniability.[51]

Source 013 described how the army, ISI, and some local entities of the government take money from Saudi governmental and non-governmental organizations in exchange



Muslim League leaders after a dinner party given at the residence of Mian Bashir Ahmad, Lahore, 1940.

for turning a blind eye to the Saudis' support for radicalizing elements within Pakistan. Some of the Saudi money flows directly to the state, which in turn funds its useful militants. Source 022 asserted that Pakistan's military and ISI sponsor militants, from the Taliban to Sipah-i-Sahaba and its offshoots, with funding from Saudi Arabia and Kuwait. Corroborating this, Pakistan's former law minister Iqbal Haider framed "Saudi-Wahhabi" movements like the Taliban and Lashkar-e-Taiba as getting "their backing from the Pakistani military and its security agencies."[52] In this context, Source 013 described the army and ISI's strategy as "made for promoting radicalization."

Source 015 described how the Pakistani government's support of violent religious groups as a means to destabilize India and Afghanistan inevitably ended up backfiring. This is well-attested to in the literature; for instance, Khan describes the government's strategy of cultivating jihadist groups to destabilize Kashmir and Afghanistan as "both a tool and a curse."[53] The problem for the regime, in 015's words, "is how to create a weapon or monster to use against others who are enacting injustice, that doesn't turn on its creator for the same reasons." As a case in point, 015 noted that "here in Pakistan, a man Maulvi Noor Mohammad—who was the teacher of Baitullah Mehsud [leader of the Tehrik-i-Taliban Pakistan]—wrote a fatwa of 40 pages against Pakistan, in which he justified jihad in Pakistan." This has translated mainly into assassination attempts against government leaders, indluding the president, prime minister, and military generals, to force the government into accepting the extremists' demands.[54]

Public Education System and Extracurricular Groups

Another agent or institution of mass-level radicalization in Pakistan is the state public education system, and, in particular, the textbooks used at both the universities and public schools.

Source 001 implicated the government in a kind of low-level jihad enculturation. He described a government-sponsored section within the country's Islamic studies program that teaches the Quran's more jihad-inspiring texts. In 001's words, the government "prepared a specific curriculum" that is "spreading militancy and terrorism." 001 was apparently referring to the first objective in Pakistan's 2002 national curriculum requirements, found in its Islamiyat Examination Syllabus.[55] The learning objective of all Pakistani youth is to grasp the meaning of the eighth Qur'anic sura, known as Sura al-Anfal, in Arabic,

or "The Spoils of War." This sura is a key source for much of the militancy and "us vs. them" mentality in Muslim communities; one verse, for example, states: "Tell the disbelievers that if they desist, their past will be forgiven. But if they persist, then they have an example in those destroyed before them. Fight against them until there is no more persecution—and your devotion will be entirely to Allah" (8:38–39). 001 describes the teaching of this sura as "a completely jihadist project."

In 001's words, the government "prepared a specific curriculum" that is "spreading militancy and terrorism."

Source 020 said that the main mode by which extremism is transmitted is religious education that takes place in public schools, or "government schools." As an example, 020 explained that the seventh-grade curriculum lionizes Ghazi Ilam Din Shaheed, "and the children are led to see him as a hero." Ilam Din was a young carpenter from Lahore who, in 1929, murdered a Hindu who had been acquitted by the Lahore High Court on charges of blasphemy for a pamphlet allegedly derogating Islam's Prophet. An article in Pakistan's *The Friday Times* corroborated the widespread cultural lionization of this figure: "The idea of committing violence as a religious obligation is neither alien nor criminal for a sizeable number of people. It has travelled through years and manifests itself in popular culture and its various expressions. Its best expression is the heroic stature of Ghazi Ilam Din Shaheed. . . . In our textbooks, the character of Ilam Din is celebrated."[56] Source 020 then complained of a lack of non-violent role models in the Pakistani state curriculum, saying "if you look at the governmental school syllabus from class first to twelfth, there is nothing about Bacha Khan, who was the prophet of non-violence."

Consequently, 020 said, "I think there is no difference between madrassas and [public] schools regarding spreading of radicalization." Source 020 suggested this is even more pronounced in the Northwest, or Khyber Pakhtunkhwa Province, and claimed that "the syllabus change process is under the supervision of JI [Jamaat-e-Islami] personnel."

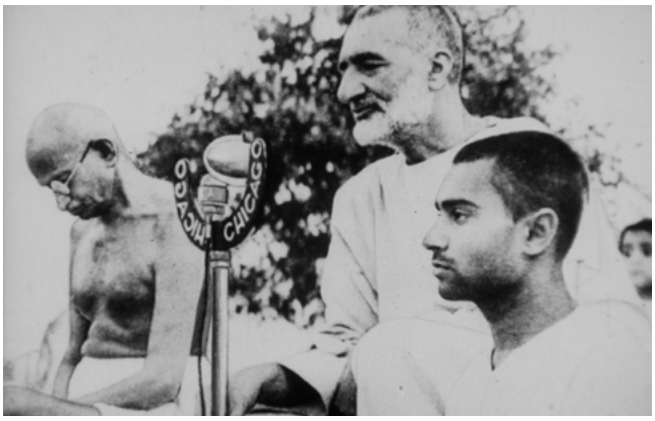
Students hold banners protesting lack of security at Bacha Khan University in Charsadda, Pakhtunkhwa Province, Pakistan, on 25 January 2016.

When *PBS Frontline* interviewed Fareed Paracha, Jamaat-e-Islami's deputy secretary general, about the group's activism in blocking curriculum reform, he said, "We think that education is rooted in the ideology and the social and cultural values of a nation. It should reflect the ideology. So we think our constitution places the responsibility on the state to develop an Islamic education system in the country."[57]

Source 024 also saw the public school system as a key node of radicalization: "We think the radicalization is developing in madrassas but the same is developing in our other [educational] institutions." Between the two educational institutions, 024 said, "there is a very minute difference." Speaking of the leaders of militant groups, 024 continued, "they are not from madrassas—from Asim Shaheed to Captain Khurram and his brother Brigadier Usman, who were members of Hizb ut-Tahrir—all these remained the students of the universities." 024 went on: "It is an injustice if we put all of the blame on madrassas, when extremism and radicalization also exist in our secular schools."

Source 015 elaborated on the role of Pakistan's education system in fueling support for religious militancy, saying, "The education system which is devised by the government produces the mindset that everything that is different or everything that is at variance is considered as [sic] enemy." This mindset is a classic Salafist trademark and is also reflected in a literal reading of the mandated Sura al-Anfal text. Echoing the view shared by several interviewees that a lack of critical thinking is the problem, 015 continued: "This education system is actually promoting one way of reality, only one angle to look at the reality," adding that "a worldview is promoted in which the critical thinking is negated and suppressed."

Beyond the official school curriculum, several interviewees pointed to the after-hours or extracurricular elements as being more important. Source 008 described religious extremism as being a regular aspect of mainstream schools' extracurricular activities. This narrative aligns with reports that Pakistan's universities have overtaken the madrassas as the primary sites of radicalization, with some reporting that one in five convicted terrorists have a bachelor's or master's degree.[58] Fundamentalist Islamist student organizations like Islami Jamiat-e-Talaba are supported by Jamaat-e-Islami, and are similarly working to promote Islamic values and remove parts of the curriculum that they believe are non-Islamic or too secular.[59]



Khan Abdul Ghaffar Khan (Bacha Khan, center) with Mahatma Gahndi (left).

Fundamentalist Islamist student organizations are working to promote Islamic values and remove parts of the curriculum that they believe are non-Islamic or too secular.

Deobandi and Salafi Institutions

Pakistan's many Deobandi and Salafi movements also play a large role in socializing young Pakistanis into a more violent extremist worldview. The literature suggests that the powerful role that Islamists like the Deobandis and JI now play in Pakistan's mainstream politics is a main driver not only of the general Islamization trend, but also of the extremist, more militant trend.[60]

Source 005 viewed the proselytizing group JuD as "doing a great job for jihad." Source 002 likewise identified the huge Islamist proselytizing movement Tablighi Jamaat as having a "high impact on society" with its local door-to-door proselytizing. Source 015 similarly said that the institutions responsible for proselytizing this worldview are many: "our education system, madrassa education system, coupled with religio-political parties and other movements, such as Jaish-e-Mohammad, JI, Al-Rashid trust, al-Akhwan and the Salafists of Arabia," all of which, he added, "have been working for decades." 015 said that these organizations justify militancy "through Qur'an and hadith," and by promoting a pan-Sunni master narrative that every societal problem "is due to absence of the caliphate." They then "explain how we will form the caliphate."

Source 014 said the regime doles out its limited resources to the Punjabi core patronage network and its state apparatus, and neglects the peripheral regions of Baluchistan, the FATA-KP, and Kashmir—the hot spots of militancy.

Source 015 said that it was these parts of Pakistani society, outside of this patronage network, where the more militant Islamist movements focused: "In a very planned manner, they reach into the marginal and vulnerable sects of community; they reach into the youth and socially marginalized" and those who are "politically marginalized." "Part of this strategy," 015 added, "involves 'social welfare work.'" He outlined several typical jobs programs promoted by the extremist groups, such as "giving justice, making bridges, solving problems to justify their [organization] and develop a stature." Once these organizations have gained a reputation for helping the marginalized, Source 015 explained, they are poised to expand their power and "build their resources," usually beginning with constructing madrassas, and then exploiting natural resources through such enterprises as orchid nurseries and mining operations as well as—in 015's words—"smuggling and kidnapping, for strengthening." Then, 015 explained, "they strengthen their networking with other militant organizations which are ideologically similar." Gradually, 015 said, all resistance to this apparatus of power is overcome; in his words, "the socially influential people are forced to leave or are eliminated from the area." Then, he added, the extremists "start a parallel state institution," such as a "judicial system, to solve the people's problems." The state's inability to meet the needs of these segments of society creates the vacuum that draws in this strategic stratum of non-state actors and enables the creation of a more extremist Islamist parallel society.

Imams, Television Preachers, and Madrassas

Source 003 previously stated that sectarianism and other forms of extremism in Pakistan are a function of taqlid mentality: "people blindly follow religious authorities [such as imams], instead of reading the Qur'an or hadith themselves." In this context, Source 014 said that "most of our people spend most of the time in mosques with the ulema," adding, "They believe that whatsoever the mullah says is part of the Qur'an and hadiths." Consequently, 014 added, "any direction the mullah chooses, they will choose that direction."

In addition to imams at the mosque, television preachers were a key source of the radicalization of Pakistan. Speaking of these influential preachers, Source 005 stated that "many people in Pakistan are inspired by Dr. Israr [Ahmed] and Dr. Zakir Naik." Dr. Israr founded JI offshoot Tanzeem-e-Islami, while Dr. Naik is an Indian Salafist televangelist and founder of the extremely popular Peace TV, who was awarded the King Faisal International Prize by the Saudi king for his "services to Islam."[61] Source 005 noted "Naik is inspired by Maulana Maududi's ideas about jihad."

Madrassas, according to the interviewees, also played a role in the radicalization of Pakistan. Source 013 saw religious education and madrassas as being the *key* cause of the spread of militancy. The problem, 013 said, didn't begin until the 1980s, when Saudi Arabian imams began proselytizing in the area of the FATA. Source 001 said that the madrassa curriculum "developed a specific mindset" that supports militancy. Source 007 identified the "madrassa and its teachers" as the proximate source of Pakistan's takfiri-jihadi-Salafi trends, along with syllabi and textbooks that offer a "wrong presentation of history."

Source 024 also said that part of the blame for Pakistan's rising extremism was due to the obviously radical madrassas such as the one "in Akora Khattak." Akora Khattak is a town located between Peshawar and Islamabad in the Khyber Pakhtunkhwa province; it is the site of Darul Uloom Haqqania, one of Pakistan's largest seminaries, which proselytizes Deobandi doctrine and has been dubbed "the University of Jihad."[62] Maulana Sami ul Haq of the Jamiat Ulema-e-Islam, the chancellor of Darul Uloom Haqqania until his assassination in 2018, was known as the Father of the Taliban, and the school counts among its alumni many senior leaders of the Afghanistan Taliban, including Mullah Omar.[63]

> **Darul Uloom Haqqania, one of Pakistan's largest seminaries, proselytizes Deobandi doctrine and has been dubbed "the University of Jihad."**

But, there is a key nuance worth noting. Source 004 said that the madrassa teacher was more important than the curriculum itself, because in extracurricular, after-hours settings, these teachers tended to foster militancy-supporting emotional dispositions in the immature students. Source 008 corroborated this, explaining that, although "traditional religious schools and madaris [plural of madrassa] have nothing in their curriculum about extremism . . . the environment in madaris, the extra-curricular activities, provide this opportunity." In this case, reform of the curriculum would not solve the problem, since extremist teaching takes place "under the radar" in extracurricular settings. But Source 016 lamented that "some unregulated NGOs promote negative propaganda against them," adding, "Critics wrongfully target all madrassas, because madrassas teach jihad."[64]

Media and Social Media

The literature on radicalization widely views the media, and especially social media, as virtual persons or agents of socialization, where a young person can be radicalized in a matter of days.[65] Three of the interviewees corroborated this view, but, again, with some important nuances for Pakistan specifically.

Source 001 implicated the media in glorifying militants; it "presents them as heroes," thereby inspiring the people, and in general, propagates a subculture with a "militant point of view." For instance, 001 noted that the aforementioned Surah al-Anfal is prominently featured on Pakistan's premier web portal, OnePakistan.com. Source 004 also said that the militant Salafism plaguing Pakistan today is spreading through virtual socialization, and "the main reason" is the broadcast media and internet-based social media. 004 said that in this realm, self-radicalization was dominant, and "youngsters particularly are getting these radicalizing materials through the internet, without any physical interaction with the outside world." Source 006 had a slightly different take on how Salafism spread in the Swat District; he said it was growing largely because of the effectiveness of FM radio in propagating the ideology of the Islamic state.

Identity Insecurity

Identity insecurity is the fourth broad factor in the radicalization framework. Three of the interviewees mentioned this factor in terms of an identity-related dissonance and low self-esteem. Source 007, for example, saw this dissonance as a product of Muslim geopolitical weakness, specifically the "crises in Palestine, Kashmir, Bosnia, etc.," along with "anger at the state, and anger at foreign states." 007 specifically emphasized the mere "presence of foreign states" as producing angst and militancy among Muslims. The dissonance is understandable. After all, if God really did give Muhammed his Word in the Meccan cave—if it is the one true religion—then why are the infidels so ubiquitous and more powerful in every way? In this vein, when asked whether religious reform in the curriculum would help counter militant Salafism, Source 008 did not think that would nearly go far enough. He explained why:

> In our region, we have a deficiency in the messages of peace; we have a worldview deficiency; we do not consider ourselves part of this world. Because of our weak

Pakistan's Swat district

Akora Khattak, Pakistan

> worldview, our curriculum is based on intolerance, superiority complex, and an emphasis on the past and future . . . . We hope for the caliphate under [ISIS]. This appeals to youngsters; it says, "If we create a caliphate, then we will look eye-to-eye with the West."

This crisis of low self-esteem and its radicalizing influence is even more pronounced in Pakistan's most socio-economically marginalized groups. Within the upper Swat District's caste-like socio-economic structure, for example, the Khan clan is dominant. Source 006 called this "Khanism" or the "superiority of Khan."[66] 006 further noted that the marginalized minority non-Khan groups in the Swat District suffered a crisis of identity of sorts, in the form of an inferiority complex. Although the Khan still owned most of the means of productions in the Swat District and therefore enjoyed both economic and political privilege, however, Salafism provided these marginalized groups with a narrative of religious superiority that dismissed the dominant Khanism. Salafi-inspired takfirism also legitimized violent resistance against the Khan clan by identifying its members as inferior kuffar, or unbelievers. This is why, 006 said, Salafism "spread in the area [Swat] like fire in the jungle."

Political Grievances

Much of the literature, including the literature on the sources of extremism in Pakistan, views political grievance as being typically the dominating factor in individual radicalization.[67] Pakistan seems to be an exception; a great majority of the interviewees surprisingly omitted this factor altogether, and two expressly countered it. For example, Source 004 characterized the role of "financial incentives" as "not important," anger at foreign states as "limited," and "underdevelopment and deprivation" as "not so important"—at least in the Northern Punjab. 004 went further, arguing that grievances against the state have "nothing to do with radicalization" in the early stages, and that political grievances "play a supporting role at the later stage" of radicalization. Source 004 knew of a "recent" study "that showed that religious dogmas—interpretations—are the main causes which create radicalization, and not political frustration."

About one third of the interviewees did mention the political grievance categories of economic deprivation, inequality, and US and Western foreign policy as intervening factors, with some interesting nuance.

Economic Deprivation and Inequality

Source 020 corroborated Source 004's view that Pakistan's underdevelopment and high unemployment are not nearly as important as religion itself in motivating radicalism. In Source 023's view, external aid from Saudi Arabia was the "most important" factor in Pakistan's rising extremism, while underdevelopment and lack of youth activities were factors "to some extent."

> **The Islamists in the upper Swat district "assured and promised that there will be health facilities, hospitals, justice in court," along with the ever-elusive "equality."**

But two other interviewees corroborated the literature's prevailing emphasis on deprivation-based extremism. In the Swat District, said Source 006, "people were motivated to see the ideal world," where "there would be justice, there would be good facilities for health, and there would be women's rights, and so on." The Islamists in the upper Swat District, 006 added, "assured and promised that there will be health facilities, hospitals, justice in court," along with the ever-elusive "equality." With such a utopian Islamic state held out before them, "the marginalized and anti-bureaucracy people quickly joined the new force." The "youth of Swat are mostly under- and unemployed," 006 explained, and these economically "frustrated youth . . . joined the political Salafists because they were promised a better life." Source 014 corroborated 006's view. "There is a deficiency of resources," 014 said, explaining why violent extremism had made such inroads in Pakistan, and specifically citing "education, food, or shelter."

US and Western Foreign Policy

Anti-Westernism in Pakistan is typically tied to the political grievance of the perceived "war on Islam" by the

Darul Uloom Haqqania, one of Pakistan's largest Islamic seminaries

United States. Source 014 cited the US's war on terror as a source of militancy in Pakistan, with the problem being "the West's dual and contradictory policies, especially towards the Muslim world, Afghanistan, Iraq, etc." Source 017 also said that US and Western policy is to blame for the rise of violent extremism. 017 framed the "war on Islam" by the West, citing the Salman Rushdie affair, the Muhammad cartoons in Europe, and the US support for Israel against the Palestinians.[68] He added:

> The world powers—the champions of human rights and justice—did not criticize Israel for their cruelty with Palestinians. Ultimately, Muslims will react. I suppose myself a secular, but still I have emotions for and am inspired by my sacred books and personalities. Every Muslim—if we see these dead bodies of innocent Muslims—will opt for radicalization.

For this reason, 017 concluded that the United States has replaced the Russians as the greatest enemy. "Most of the people have emotions that Muslims are under the cruelty of the West; therefore, they join the jihad." The occupation of Muslim lands, such as the US-led occupation of Afghanistan, has long been understood to be a defensive jihad trigger, and a key theme in Islamic scholar Yusuf al-Qaradawi's definitive 2009 *Fiqh of Jihad*.[69]

Source 018 also embraced the standard conspiracy theory of the West's war on Islam. "It's the agenda of foreign countries that Muslim countries don't get established," 018 said, adding that "if there is peace and stability, their power/influence will lessen." 018 said that "Israel is the biggest enemy," along with "India and America."

Source 022 listed US drone strikes as a minor factor. Drone strikes that killed family and tribal kin inflicted a social psychological trauma on those who remained that "we cannot imagine," said 022. Each of these deaths in the tribal area creates tribal debt and increases the level of tribe-wide animosity that accompanies the wrongful death of a close blood relative.

For 019, another key political grievance fueling support for militancy in Pakistan is anger at the Pakistani government for its partnership with the United States in the war on terror. Source 014 noted that the extremists "exaggerate the cruelty of the foreign states in Iraq, Syria, and Afghanistan, and then link them to the state of Pakistan, noting that it provides assistance to these infidel states."

Findings and Conclusion

This ethnography offers several value-added insights that build upon the existing literature regarding extremism in Pakistan and extremism more broadly. The main two theoretical insights are related to the mass-level radicalization of a country, and the primacy of ideology and the agents that socialize it.

Insight One: Mass-Level Radicalization of the Country

Many of the 25 interviewees described Pakistan as a country that has undergone mass-level religious radicalization. The idea of mass radicalization of a country exists only weakly in the literature and there are at present no case studies, although the long-term cultural project by Islamists like the Muslim Brotherhood to slowly Islamize all institutions of the state can be considered a softer form of mass radicalization.[70] In Pakistan, the Islamization of the state took place in more of a top-down fashion, as a result of the military-mosque alliance led by General Zia in the 1980s. As the intervewees made clear, the recurring theme of Pakistan's mass radicalization was not merely Islamiization, but Salafization.

> **In Pakistan, the Islamization of the state took place in more of a top-down fashion, as a result of the military-mosque alliance led by General Zia in the 1980s.**

The only other country, so far, that has experienced mass-radicalization in the form of Salafization is Yemen, which is experiencing what Gregory Johnsen calls "the increasing radicalization of the country's religious landscape."[71] But, the contexts and outcomes in Yemen and Pakistan are significantly different. In Yemen, the most consequential radicalization took place among the nominally Shi'a Zaydi community, which dominates the northern part of Yemen along the Saudi border; this community had been largely politically marginalized, despite comprising close to 40 percent of Yemen's population. The Muslim Brotherhood's Saudi-funded Islah party was pushing its version of Islam into every corner of the country, and the Zaydis radicalized in response to the increasing Salafization of the Sunnis around them.[72] In the north of Yemen, this threatened Zaydi cultural and religious values, as long-held orthodox Shi'a practices, such as praying at shrines, were denounced as heretical.

In summary, the increasing radicalization of the religious landscape in Pakistan unfolded as a result of the interplay of many largely unique and complex factors, with Salafization being perhaps the most salient one.

Insight Two: The Primacy of Ideology as a Factor of Extremism in Pakistan

The narratives from these 25 interviews tend to counter the prevailing view in the literature, including some of the literature focused specifically on Pakistan, which asserts that violent extremism in Muslim-majority communities has little or nothing to do with any religious-based ideology, and is essentially no different from other forms of terrorism that emerge mainly from political and economic grievances.[73] Typical in this frame, Sanchita Bhattacharya writes:

> The combination of lack of representation, poor governance, institutionalized corruption and economic stagnation are compelling ingredients for societal breakdown and disillusionment. The unemployed youth of Pakistan, who see little hope in traditional politics or the way of governance, are fascinated by the missionary zeal of the religious right wing. The rapid growth of Islamic militancy in Pakistan may be a consequence of poor governance and economic stagnation, and in no small measure due to the failure of the international financial institutions to provide firm and consistent support to a Pakistan, geared towards human development, rather than the mere avoidance of loan defaults.[74]

But only two of the interviewee narratives presented here even mentioned these factors, and neither of them framed these factors as having primacy over the others. Instead, all of the interviewees tended to dwell instead on the

ideology, as if the ideology itself—several different forms of extremist ideologies or doctrines—is the main explanation for the radicalization of the religious landscape in Pakistan. Recall how Source 006 said that the Islamism enshrined in Pakistan's founding has shaded to jihadism—"Nowadays, it is general thinking that 'jihad is religion'"—and how 007 said of extremism, "I think this is deeply rooted in our society." When extremism becomes deeply rooted, it becomes cultural, and from that point on, can persist without antecedent political grievances. In other words, regardless of the original conditions of emergence, the ideology itself was sufficient to cause further radicalization because of its widespread enculturation.

The Co-Primacy of Socialization by Interested Agents

Another key factor to which the interviewees gave co-primacy is the role of interested agents who socialize a person into extremism. As outlined above, the apparatus of extremism in Pakistan has several such socializing agent groups and institutions. Again, the idea of socialization into extremism simply means that the spread of extremism is a function of interested agents—both individuals and groups, both internal and external to the targeted society. To varying extents, all worldviews and ideologies, including shades toward violent extremism, are the result of purposive human-to-human proselytizing, even if it is indirectly conducted through social media, radio, television, and printed publications.

In this vein, all of the 25 interviewees across Pakistan's various districts gave primacy to this factor. They described a broad range of Pakistani and foreign non-state groups, and local and foreign government actors, who find the entire continuum of religious fundamentalism, including violent extremism, useful in the religio-political and geo-political realms, and who therefore actively propagate it.

> **A broad range of Pakistani and foreign non-state groups, and local and foreign government actors, find the continuum of religious fundamentalism, including violent extremism, useful.**

This factor is typically missing in the literature's models of radicalization. For instance, in their long list of what they call "mechanisms of political radicalization," Clark McCauley and Sophia Moskalenko outline a dozen factors: personal victimization, political grievance, joining a radical group, the role of love in joining a radical group, extremity shift in like-minded groups, extreme cohesion under isolation and threat, competition for the same base of support, competition with state power, within-group competition, Jujitsu politics (or terrorist success in getting the state to overreact), hatred of others, and the opportunity for martyrdom.[75] But as the interviewees in this ethnography suggest, only a few of those factors are relevant in the case of Pakistan, and not one factor in that long list has any primacy in Pakistani society. This finding shows why ethnographies of this sort are important in truly understanding a social phenomenon.

Key Takeaway and Recommendation

In the final analysis, Pakistan seems to be an outlier case in terms of the factors that have caused Pakistanis and the country broadly to radicalize. Two broad factors—political grievances and forms of identity insecurity—are almost always present in cases of radicalization, but the Pakistani interviewees said very little about either of these factors; only a third of them mentioned these factors at all, and none of them listed grievance or identity as foremost in the sources of militancy in Pakistan. To the contrary, the majority of the interviewee responses dwelled on factors typically deemphasized or not mentioned at all by the literature: both the ideology or culture itself, and the socialization into extremism by the religio-political strategies of various state and non-state agents and local and foreign actors.

These findings are important because they force us to approach radicalization into extremism as a much more complex phenomenon. Each case merits its own careful analysis, including the use of ethnographies, with the expectation that the resulting middle-range theories, like the one provided here in the case of Pakistan, may not conform to general models. The atypical findings of this admittedly small ethnography merit other studies—both ethnographic and traditional large-N case studies—that ask the same question: what specific *current* factors are causing the mass-level radicalization of this hugely important country, and what are the likely trends of each of those factors in the near and long terms?

Appendix I: List of Interviewees

001: a civil society activist working to contain militant extremism, among other things

002: [affiliation not noted]

003: a Salafi

004: worked for an organization in the northern Punjab that produced a counternarrative to Islamic extremism

005: has a doctorate degree

006: a highly educated and accomplished resident and activist of Pakistan's Swat District, who is leading a civil society organization focused on containing extremism

007: a government official in Peshawar

008: a professor and former dean at an Islamic university near Peshawar

009: a Pakistani professor of political science

010: a well-known Islamic scholar with a YouTube presence, who focuses on containing sectarian violence

011: An imam at a prominent madrassa, editor of a major Islamic journal, and a political representative

012: a Salafist affiliated with the Ahl-e-Hadith movement

013: a high-level activist in the secular Awami National Party's student wing

014: a lecturer in the former Federally Administered Tribal Areas

015: a well-known figure in Pakistani society and a contributor to one of Pakistan's major newspapers, who resides in the Khyber Pakhtunkhwa area

016: a former Deobandi and deputy amir within Pakistan's only Salafist party, Markazi Jamiyat Ahl-e-Hadith

017: the president of an NGO in Islamabad

018: a researcher with a graduate degree, and a member of the Saudi-funded Salafist movement, Ahl-al-Hadith

019: was working to curb extremism by reforming Pakistan's madrassas

020: an activist within the pro-US Awami National Party, who seeks to counter violent extremism through social media

021: a Salafist and member of Pakistan's Ahl-e-Hadith

022: a government official who writes columns for a Pakistani newspaper, and who was interviewed in Mardan

023: [affiliation not noted]

024: [affiliation not noted]

025: [affiliation not noted]

ABOUT THE AUTHOR

Dr. David D. Belt is a professor at National Intelligence University.

NOTES

1. Editor's note: *CTX* has published several articles on the topic of radicalization in Pakistan. See Amina Kator-Mubarez, "Equivocated Intentions: Blasphemy Laws in Pakistan, *CTX* 3, no. 1 (February 2013): https://nps.edu/web/ecco/ctx-vol-3-no-1-february-2013 ; Sanchita Batticharya, "Pakistan: Money for Terror," *CTX* 4, no. 4 (November 2014): https://nps.edu/web/ecco/ctx-vol-4-no-4-november-2014 ; and Surinder Kumar Sharma, "Hizb-ut-Tahrir: The New Islamic State," *CTX* 5, no. 1 (February 2015): https://nps.edu/web/ecco/ctx-vol-5-no-1-february-2015
2. All statements of fact, analysis, or opinion are the author's, and do not reflect the official policy or position of the National Intelligence University, Department of Defense, or the US government.
3. "Grounded theory is a research methodology that results in the production of a theory that explains patterns in data, and that predicts what social scientists might expect to find in similar data sets. When practicing this popular social science method, a researcher begins with a set of data, either quantitative or qualitative, then identifies patterns, trends, and relationships among the data. Based on these, the researcher constructs a theory that is 'grounded' in the data itself." See Ashley Crossman, "Definition and Overview of Grounded Theory," Thoughtco.com, 25 February 2019: https://www.thoughtco.com/grounded-theory-definition-3026561 ; see also, Kathy Charmaz, *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis* (Thousand Oaks, CA: SAGE Publications, 2006), 42-47.

4. All of the interviews were recorded in Urdu, Pashto, and Punjabi and translated by X and his assistant into English. Although X obtained permission to identify most of the interviewees by name, my partnering organization and I felt that they should remain anonymous to prevent possible retribution in an increasingly volatile religio-political climate. Our original intention was to expand the research into several more countries, but when the project's funding fell through, my partnering organization and X gave me permission to use these insightful narrative interviews for my own work.
5. Madiha Afzal, *Pakistan Under Siege: Extremism, Society, and the State* (Washington, DC: Brookings Institution, 2018), chapter 1.
6. Samuel P. Huntington, *The Clash of Civilizations and Remaking of the World Order* (New York: Touchstone, 1996), 126.
7. Ashok K. Behuria, "Sects Within Sect: The Case of Deobandi–Barelvi Encounter in Pakistan," *Strategic Analysis*, 32, no. 1 (January 2008): 57–80: https://doi.org/10.1080/09700160801886330
8. This Channel program document from the UK government is no longer available, but is approximated by HM Government, "Channel: Supporting individuals vulnerable to recruitment by violent extremists," (March 2010), 10. Per HM government, "Channel is part of the Prevent strategy. The process is a multi-agency approach to identify and provide support to individuals who are at risk of being drawn into terrorism." See "Channel Guidance," Gov.UK, 23 October 2012: https://www.gov.uk/government/publications/channel-guidance
9. The quote on the four-part conceptual framework can be found in Quilliam Foundation, *Radicalisation on British University Campuses: A Case Study* (London: Quilliam Foundation, 2010). This has been widely cited in the literature since 2010, and the author has used it since then, and discussed it with Quilliam's president at the time. Although it is no longer posted on Quilliam's list of publications, it is available at: https://www.safecampuscommunities.ac.uk/uploads/files/2016/08/qulliam_case_study_requires_upload.pdf
10. See, for example, John Feffer and Najum Mushtaq, "Islamic Blowback Part Two?" Institute for Policy Studies, 5 August 2006: https://ips-dc.org/islamic_blowback_part_two/ ; Ayyaz Gull, "Sectarian Politics in Pakistani Punjab: A Reappraisal," *The Historian*, 14 (Winter 2016): 81–83; Mohammad Waseem, *Politics and the State in Pakistan* (Islamabad: NIHCR, 2007), 124; Khaled Ahmed, *Sectarian War: Pakistan's Sunni-Shia Violence and Its Links to the Middle East* (Karachi: Oxford University Press, 2011), 24.
11. The 1948 Objectives Resolution "served as preamble for the constitutions of 1956, 1962 and 1973 and ultimately became part of the Constitution when the Eighth Amendment in the Constitution of 1973 was passed in 1985." See "Objectives Resolution," HistoryPak.com, nd.: https://historypak.com/objectives-resolution-1949/
12. Arshi Saleem Hashmi, "Historical Roots of the Deobandi Version of Jihadism and Its Implications for Violence in Today's Pakistan," in *Faith-Based Violence and Deobandi Militancy in Pakistan*, eds. Jawad Syed, Edwina Pio, Tahir Kamran, and Abbas Zaidi (London: Palgrave-Macmillan/Springer, 2016), 137.
13. "Pakistan's Barelvis—Transformation from Peaceful to Violent?" DW, 12 November 2017: https://www.dw.com/en/pakistans-barelvis-transformation-from-peaceful-to-violent/a-41744277
14. Shamil Shams, "The 'Wahabi Republic' of Pakistan," DW, 24 August 2012: https://www.dw.com/en/the-wahabi-republic-of-pakistan/a-16191055
15. Ibid. Lashkar-e-Taiba is an extremist group based in Pakistan that is responsible for a number of terrorist attacks across India and in Indian Kashmir beginning in 1990.
16. Rohan Bedi, "Have Pakistanis Forgotten Their Sufi Traditions? (Singapore: International Centre for Political Violence and Terrorism Research at Nanyang Technological University, April 2006), 3–4: https://web.archive.org/web/20131102091018/http://www.pvtr.org/pdf/RegionalAnalysis/SouthAsia/Madrassa%20_IDSS%20_%20_FINAL_.pdf
17. C. Christine Fair, "Islam and Politics in Pakistan," in *The Muslim World after 9/11*, Angel Rabasa, Cheryl Benard, Peter Chalk, C. Christine Fair, Theodore W. Karasik, Rollie Lal, Ian O. Lesser, and David E. Thaler (Santa Monica: RAND Corporation, 2004), 256, http://www.rand.org/publications/MG/MG246/.
18. Behuria, "Sects Within Sect."
19. "Pakistan's Barelvis – Transformation from Peaceful to Violent?"
20. Ghulam Rasool, "What are the Differences in the Deobandi, Barelvi, & Salafi Subsects of Sunni Islam? Why are They so Against Each Other?" Quora, 7 September 2020: https://www.quora.com/What-are-the-differences-in-the-Deobandi-Barelvi-Salafi-subsects-of-Sunni-Islam-Why-are-they-so-against-each-other/
21. Hashmi, "Historical Roots," 136–139.
22. This group includes sources 001, 003, 005, 010, 011, 012, 018, and 021.
23. "What is New about Al-Qaradawi's Jihad?," IkwhanWeb, 25 September 2009: https://www.ikhwanweb.com/article.php?id=21082
24. For more on these groups, see Narendar Singh, "Jamaat-ud-Dawa (Lashkar-e-Tayyaba)" SSRN, 29 October 2018: https://ssrn.com/abstract=3274368 or http://dx.doi.org/10.2139/ssrn.3274368
25. "US Blacklists Pakistan's Jamaat-ud-Dawa," Al-Jazeera, 26 June 2014: https://www.aljazeera.com/news/2014/6/26/us-blacklists-pakistans-jamaat-ud-dawa
26. Kuffar is the plural form of the Arabic word for disbeliever or infidel. Kafir is the singular form, used to refer to a specific person or entity.
27. Bizaa Zeynab Ali, "The Religious and Political Dynamics of Jamiat Ahle-Hadith in Pakistan," Columbia Academic Commons, 2010: https://academiccommons.columbia.edu/doi/10.7916/D8VH5X2X
28. Laura Mansfield, *His Own Words: Translation and Analysis of the Writings of Dr. Ayman al Zawahiri* (Old Tappan, NJ: TLG Publications, 2006), 324–326.
29. David Belt, "Journey to the Najd: An Introduction to the Post 9/11 Saudi Arabia," Industrial College of the Armed Forces, July 2006. This was a National Defense University curriculum reading based on high-level interviews conducted by the author in Saudi Arabia in 2006, and is available from the author upon request.
30. Sarfraz Khan and Hafeez-ur-Rehman Chaudhry, "Determinants of Sectarianism in Pakistan: A Case Study of District Jhang," *Middle-East Journal of Scientific Research* 8, no. 1 (2011): 237–243.
31. C. Christine Fair, "Explaining Support for Sectarian Terrorism in Pakistan: Piety, Maslak and Sharia," *Religions* 6 (2015): 1141.
32. Arif Rafiq, "How Pakistan Protects Itself from Regional Sectarian War," *National Interest*, 18 September 2015: https://nationalinterest.org/feature/how-pakistan-protects-itself-regional-sectarian-war-13873?page=0%2C1
33. Personal communication, May 2008.

34. Eirini Gouleta, "Educational Assessment in Khyber Pakhtunkhwa," *Global Education Review*, 2 no. 4 (2015), 21, https://files.eric.ed.gov/fulltext/EJ1080905.pdf,

35. Hamza Siddiq, "Violent Extremism in Pakistan: A Failure of Public Education," London School of Economics, 4 May 2017: https://blogs.lse.ac.uk/southasia/2017/05/04/violent-extremism-in-pakistan-a-failure-of-public-education/

36. Hashmi, "Historical Roots," 136–139.

37. Claud Moniquet, "The Involvement Of Salafism/Wahhabism In The Support And Supply Of Arms To Rebel Groups Around The World," EU Parliament Policy report, (June 2013), 6: https://op.europa.eu/en/publication-detail/-/publication/37e6841c-d424-4e9f-84c2-c7fbc97a836e/language-en

38. Bizaa Zeynab Ali, "The Religious and Political Dynamics of Jamiat Ahle-Hadith in Pakistan," Columbia Academic Commons (22 June 2012): 1: https://academiccommons.columbia.edu/doi/10.7916/D8VH5X2X

39. James M. Dorsey, "The Saudi Export of Ultra-Conservatism in the Era of MbS – an Update," *The Turbulent World of Middle East Soccer* (blog), 19 April 2018: https://mideastsoccer.blogspot.com/2018/04/the-saudi-export-of-ultra-conservatism.html

40. Amin Saikal, *Zone of Crisis: Afghanistan, Pakistan, Iran and Iraq* (London: I. B. Tauris, 2014), 4; Gull, "Sectarian Politics," 86.

41. Aarish Ullah Khan, "The Terrorist Threat and the Policy Response in Pakistan," SIPRI Policy Paper No. 11 (Stockholm: Stockholm International Peace Research Institute, September 2005), 7: https://www.sipri.org/sites/default/files/files/PP/SIPRIPP11.pdf

42. Ibid., 8.

43. Bedi, "Have Pakistanis Forgotten?", 4 –6.

44. Gull, "Sectarian Politics," 87.

45. Justin Jones, *Shia Islam in Colonial India: Religion, Community, and Sectarianism* (New York: Cambridge University Press, 2011), 239; Gull "Sectarian Politics," 88.

46. Khan, "The Terrorist Threat and the Policy Response," 16–17.

47. S. Akbar Zaidi, "Special Report: Darkness Descends 1977-1988: Despotic Islamisation," *Dawn*, 1 November 2017: https://www.dawn.com/news/1364410

48. Husain Haqqani, *Pakistan: Between Mosque and Military* (Washington, DC: Carnegie Endowment for International Peace, 2005), 311.

49. Ibid., vii–viii.

50. Ibid., 131.

51. Phil Stewart and Idrees Ali, "Exclusive: Pentagon Cancels Aid to Pakistan over Record on Militants," Reuters, 1 September 2018: https://www.reuters.com/article/usa-pakistan-military-idINKCN1LI01T

52. Shams, "The 'Wahabi Republic' of Pakistan."

53. Khan, "The Terrorist Threat and the Policy Response," preface. See also C. Christine Fair, "Lashkar-e-Tayiba and the Pakistani State," *Survival* 53, no. 4 (2011): 1.

54. Khan, "The Terrorist Threat and the Policy Response," 17.

55. Government of Pakistan (2002), National Curriculum; Islamiyat Classes IX-X, Islamabad, Ministry of Education (Curriculum Wing). See also Aga Khan University's Examination Board, Secondary School Certificate Examination Syllabus, Islamiyat Classes IX-X (Based on National Curriculum 2002), Karachi, June 2012: https://examinationboard.aku.edu/about-us/Syllabi-List/Islamiyat.pdf

56. Raza Rumi, "Blasphemy It Was Not," *Friday Times* (Pakistan), 30 October 2015: https://www.thefridaytimes.com/blasphemy-it-was-not/

57. Fareed Paracha, "Pakistan: The Lost Generation," *PBS Frontline*, n.d.: https://www.pbs.org/frontlineworld/stories/pakistan901/paracha.html

58. "Are Universities in Pakistan Becoming a Breeding Ground for Terrorism?," YouTube video, 11:59, posted by FRANCE 24 English, 20 September 2017: https://www.youtube.com/watch?v=dS3RYrvES1c

59. Nadeem F. Parach, "Bleeding Green: The Rise and Fall of the IJT," *Dawn*, 16 August 2012: https://www.dawn.com/news/742642/bleeding-green-the-rise-and-fall-of-the-ijt . See also the Islami Jamiat-e-Talaba website: https://jamiat.org.pk/about-us/ ; and also: https://jamiat.org.pk/wp-content/uploads/IJT-Intro.pdf

60. Jamal Malik, *Islam in South Asia: A Short History* (New Delhi: Orient Blackswan Ltd., 2012), 383; See also Gull, "Sectarian Politics," 84.

61. Shoaib Daniyal, "Why a Saudi Award for Televangelist Zakir Naik is Bad News for India's Muslims," *Scroll* (India), 10 March 2015: https://scroll.in/article/712341/why-a-saudi-award-for-televangelist-zakir-naik-is-bad-news-for-indias-muslims

62. Tim Craig, "Pakistan's 'University of Jihad' is Getting Millions of Dollars from the Government," *Washington Post*, 22 June 2016: https://www.washingtonpost.com/news/worldviews/wp/2016/06/22/pakistans-university-of-jihad-is-getting-millions-of-dollars-from-the-government/

63. Imtiaz Ali, "The Father of the Taliban: An Interview with Maulana Sami ul-Haq," *Jamestown Foundation* 4, no. 2 (23 May 2007): https://jamestown.org/interview/the-father-of-the-taliban-an-interview-with-maulana-sami-ul-haq/

64. For more on this topic, see Masooda Bano, "Beyond Politics: The Reality of a Deobandi Madrasa in Pakistan," *Journal of Islamic Studies* 18, no. 1 (January 2007): 43–68.

65. Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, "Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism," RAND, 2013: https://www.rand.org/pubs/research_reports/RR453.html

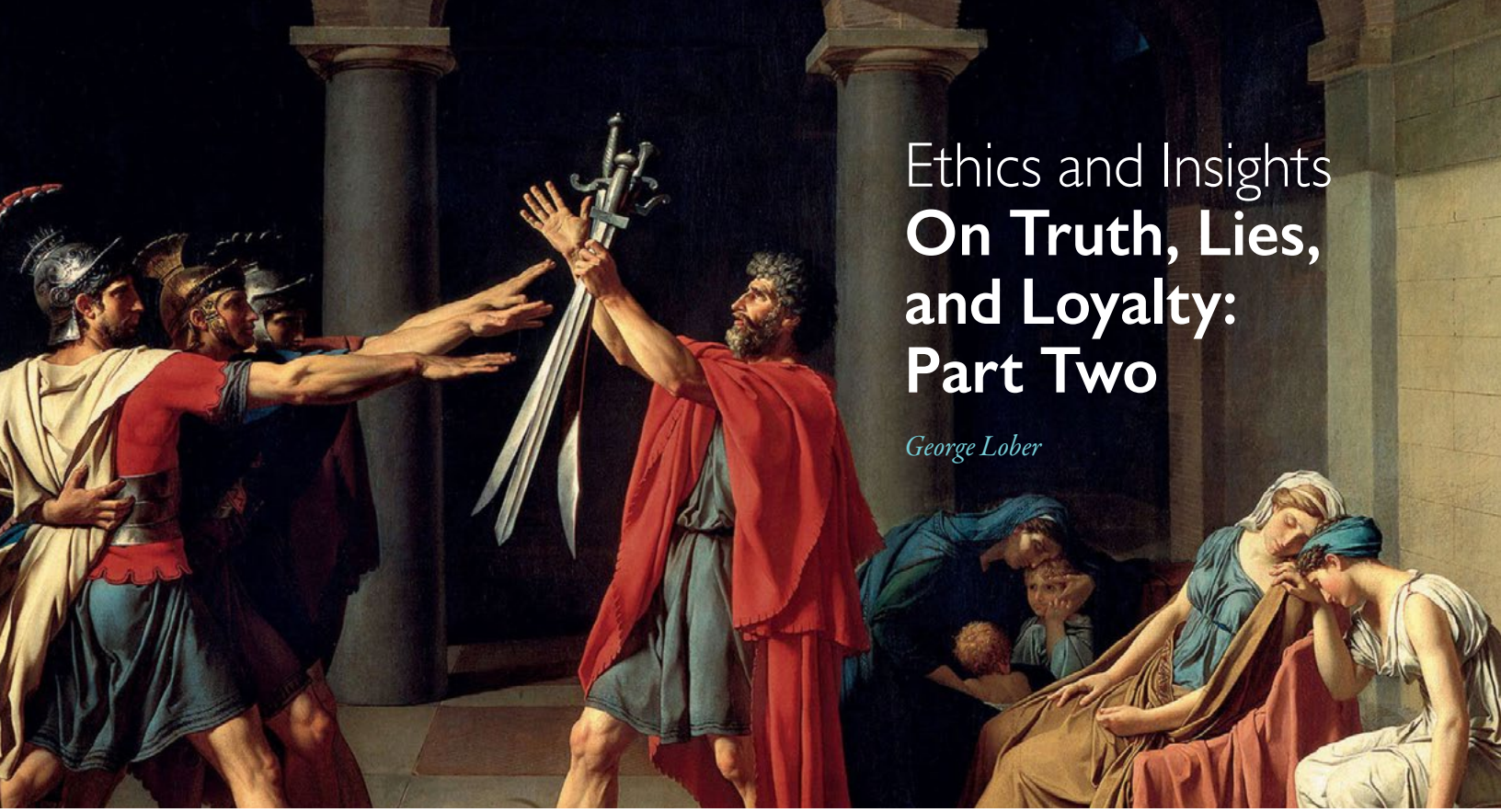
66. Pakistan's feudalistic socio-economic structure, in which the vast bulk of the country's wealth is held by a handful of families, is described in several studies. See, for example, Umbreen Javaid and Tahmina Aslam, "Feudalism In Pakistan: Myth Or Reality/Challenges To Feudalism," *Journal of the Research Society of Pakistan*, 54, no. 1 (January-June, 2017): http://pu.edu.pk/images/journal/history/PDF-FILES/15_54_1_17.pdf ; and Fahad Anwar, "The Feudal Culture," *The Nation* (Karachi), 17 May 2013: https://nation.com.pk/19-May-2013/the-feudal-culture

67. For example, see Eamon Murphy, *The Making of Terrorism in Pakistan: Historical and Social Roots of Extremism* (London: Routledge, 2013); Harriett Alan, et al., "Drivers of Violent Extremism: Hypotheses and Literature Review," RUSI, 16 October 2015; Eric Rosand, "In Strategies to Counter Violent Extremism, Politics Often Trump Evidence," The Brookings Institution, 6 May 2019: https://www.brookings.edu/blog/order-from-chaos/2019/05/06/in-strategies-to-counter-violent-extremism-politics-often-trumps-evidence/

68. Salman Rushdie's book, *The Satanic Verses* (New York: Random House, 1988), inspired anti-Western solidarity among Muslims worldwide and led to a fatwa legitimizing his assassination from Iran's Supreme Leader, Ayatollah Khomeini. "Anniversary of Rushdie book fatwa," Reuters, 14 February 2009; Daniel Pipes, *The Rushdie Affair: The Novel, the Ayatollah, and the West* (New Brunswick, NJ: Transaction, 2006). Nearly 20 years later, in

September 2005, the Danish newspaper *Jyllands-Posten* published 12 caricatures of Islam's prophet, Muhammad. The paper's stated purpose was to contribute to the debate about criticism of Islam and self-censorship, but many Muslims found the images offensive and Muslim agitators around the world whipped up violent protests against the paper. See Paul Reynolds, "Cartoons and the Globalisation of Protests," BBC, 22 February 2006: http://news.bbc.co.uk/2/hi/middle_east/4740020.stm

69. "What is New about Al-Qaradawi's Jihad?," IkwhanWeb, 25 September 2009: https://www.ikhwanweb.com/article.php?id=21082
70. Clark McCauley and Sophia Moskalenko, "Mechanisms of Political Radicalization: Pathways Toward Terrorism," *Terrorism and Political Violence* 20, no. 3(2008): 426–428; Hazem Kandil, "Islamizing Egypt? Testing the Limits of Gramscian Counterhegemonic Strategies," *Theory and Society* 40 (2011): 37–62.
71. Gregory Johnsen, *The Last Refuge: Yemen, al-Qaeda, and America's War in Arabia* (New York: Norton, 2013), 144.
72. Ibid.
73. See note 67.
74. Sanchita Bhattacharya, "Pakistan: Sectarian War Scourging an Entire Nation," *Liberal Studies* 4, no. 1 (January–June 2019): 87–105.
75. McCauley and Moskalenko, "Mechanisms of Political Radicalization," 426–428.



Ethics and Insights

On Truth, Lies, and Loyalty: Part Two

George Lober

The Oath of the Horatii, Jacques-Louis David, 1784

WITHIN THE FIRST FIVE PAGES OF HIS BOOK *How Good People Make Tough Choices: Resolving the Dilemmas of Ethical Living*, ethicist Rushworth Kidder draws a clear distinction between true ethical dilemmas and what he calls moral temptations. The former requires us to choose between two "right" courses of action—in essence, to make a "right versus right" choice. The latter, posing as an ethical dilemma, tempts us to choose between a "right" and a "wrong" course of action. We may want to believe our decision is the right choice, but in reality it is "a wolf-like moral temptation masquerading in the lamb's clothing of a seeming ethical dilemma."[1] A true ethical dilemma, he asserts, reaches "inward to our most profound and central values, setting one against the other in ways that will never be resolved simply by pretending that one is 'wrong.'"[2]

Kidder then asserts that actual ethical dilemmas fall into one of four paradigms, or right-versus-right choices: truth versus loyalty, individual versus community, short term versus long term, and justice versus mercy. He acknowledges that of the four, the truth versus loyalty paradigm "will seem the central issue on the ethical horizon—perhaps the only one."[3] This is because, at its core, the truth versus loyalty dilemma goes to the heart of human interaction; it asks us to choose between two highly prized human virtues, and in choosing one, it demands that we sacrifice the other. One may, for the sake of loyalty, sacrifice truth or, for the sake of truth, sacrifice loyalty. And under the right circumstances, Kidder asserts, either choice may be ethically justifiable. This assertion, though, creates an ethical wrinkle. If I choose loyalty over truth and then lie to protect someone with whom I feel a close bond, am I not committing an unethical act? Is Kidder suggesting that lying can be a good thing? Unfortunately, the answer to both questions is, "It depends."

While acknowledging the concerns of the philosopher Sissela Bok regarding the manipulative, unethical, and socially corrosive effects of lying, Kidder points out that "while truth-telling is indeed a sine qua non of an ethical life, it is not the whole of it. Frank and brutal truth-telling can accompany murderous tyrannies, loveless marriages, unjust societies, and irresponsible apathies."[4] Although he acknowledges the positive benefits of loyalty that can occur on the national, social, and deeply personal levels, he cautions, "at its worst, loyalty accounts for some of the most horrifying excesses of the century, perpetrated by those with allegiance to Hitler, Mao, Stalin, Saddam Hussein, and so forth."[5] However, he adds, loyalty "typically involves some component of responsibility, dedication, and honor. It also involves some recognition that there are obligations, even of the most elusive sort, that must be fulfilled."[6]

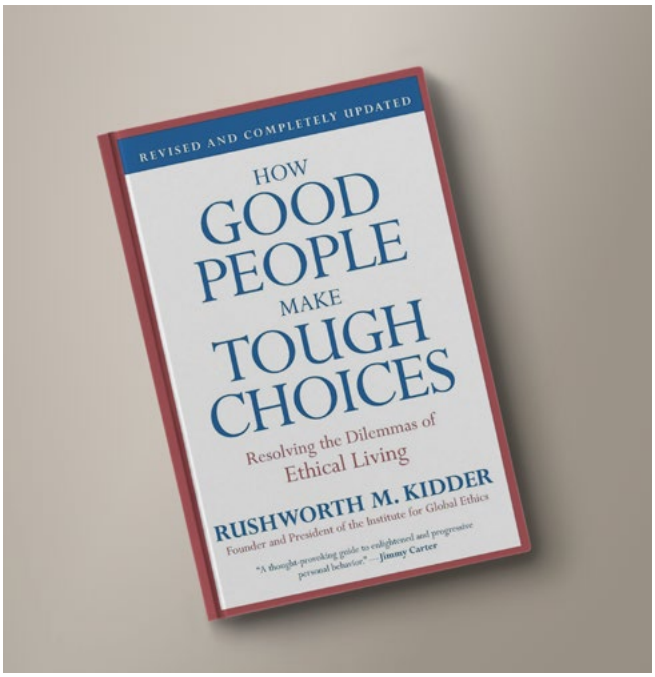
Kidder wants us to first recognize that truth and loyalty are ethical virtues which carry equal weight.

What, then, are we to do? How should we choose between telling the truth and honoring our loyalty to another? Kidder wants us to first recognize that truth and loyalty are ethical virtues which carry equal weight. After that, he advises us to carefully consider the circumstances, the individuals involved, and the consequences of our decision from the perspective of three resolution principles: choosing what's best for the greatest number affected; choosing to uphold a principle in light of possible difficult consequences; and choosing to exercise compassion and empathy.[7] Finally, he asks us to recognize that choosing between truth and loyalty is a difficult challenge and, ultimately, one that we should arrive at by asking ourselves which decision we can accept and live with as being the *most* ethically right.[8]

In that regard, no film of recent times highlights the truth-versus-loyalty ethical dilemma more clearly than the 2015 Danish film *A War*.[9] As the film begins, a Danish military company in Afghanistan is stationed at a forward operating base (FOB) in Helmand Province. The commander, Claus Pedersen, is coping with declining morale within the company as his men go on patrols where they are continuously exposed to sniper fire, ambushes, and IEDs planted by the Taliban. At the same time, at home in Denmark, Pedersen's wife struggles to raise their two children alone under the increasing strain of his absence.

One evening, in order to stem the loss of morale, Pedersen announces to the company that starting tomorrow, he will go on patrols with the men. However, as the weeks pass, the demands of the patrols added to Pedersen's duties as commander wear on him until, one morning while exiting a village compound, his patrol is attacked. The enemy fire is relentless, and no one in the patrol is able to locate the source of the attack, which appears to be coming from multiple locations. Suddenly, a member of the patrol is severely wounded and begins to bleed out. All elements of the patrol are pinned down while RPGs strike their locations. Pedersen, crouching behind a wall with the radio operator, nicknamed Butcher, realizes that he has to call in an airstrike from the tactical operations center (TOC) to protect his men and allow a medevac helicopter to land and airlift the wounded soldier to safety. But, he still doesn't know for certain the source and direction of the attack and cannot direct the airstrike.

At this moment, a radio call comes in from one member of the patrol, saying that the attack appears to be coming from the west. Pedersen checks a map and concludes the attack has to be coming from Compound 6, which lies west of their location. He tells Butcher to call in an



airstrike on Compound 6, but the TOC demands visual confirmation of the enemy in the compound before launching the airstrike. The enemy fire intensifies, and Pedersen is unable to obtain positive identification (PID) of the enemy in Compound 6. Nonetheless, he directs Butcher to "tell them I have PID!" This is a lie and Butcher knows it is a lie, but he calls in the positive confirmation and the airstrike is launched. Seconds later, Compound 6 is struck and the attack ceases. Within minutes, Pedersen and the patrol are able to carry the wounded soldier to a waiting helicopter and head back to their base.

A few days later, members of the Judge Advocate's (JAG) staff arrive at the FOB and begin to take depositions from Pedersen and all the men who were on the patrol with him the day of the attack. At the conclusion of the deposition process, Pedersen is charged with violating the Danish Military Code of Justice and killing eleven innocent civilians, all women and children, whose bodies were the only ones later discovered in Compound 6. He is sent back to Denmark to stand trial.

Once home, Pedersen is introduced to his defense attorney, who explains that the prosecution's case against Pedersen is very strong, and unless Pedersen can claim he had definite PID of the enemy in Compound 6, he almost certainly will be sent to prison. Pedersen tells the attorney the truth: he cannot testify that he had PID. Later, while driving home from the attorney's office, Pedersen tries to explain to his wife why he cannot lie before the court; he did not see the

enemy, he ordered the bomb dropped, and he will now have to accept the consequences of that action. However, she sees his decision as a betrayal of his loyalty to her and the children, and angrily urges him to lie for his own children's sake, arguing, "You may have killed eight children, but you have two alive children at home!"

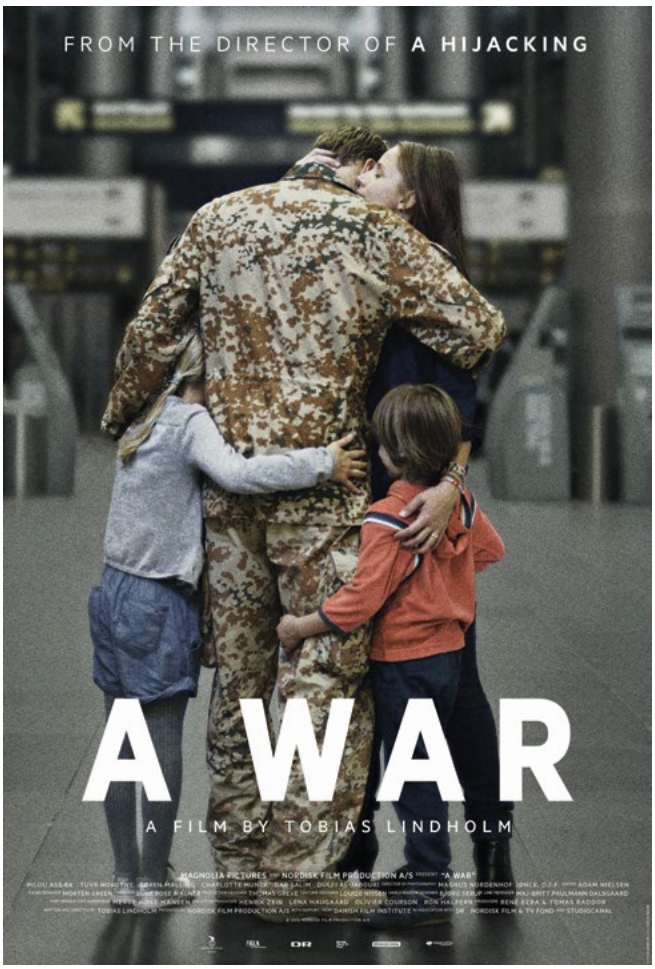
The trial begins, and the prosecution's case against Pedersen appears airtight. The prosecutors produce an audio file of Pedersen admitting during the firefight that he doesn't have PID and then telling Butcher, "I don't care who's in there!" This is followed immediately by his order, "Tell them I have PID!" They also submit depositions from every member of the patrol, each of whom states that he did not have positive confirmation of the enemy's location. Finally, the prosecutors display graphic photos of the victims of the airstrike.

When Pedersen takes the stand, he claims that although he personally did not have PID, he was told the location of the source of the attack by someone over the radio. Under further questioning, he testifies he cannot remember who told him, but he insists that the court cannot possibly understand the circumstances of the firefight that day, and reminds them that he had a duty to protect his men.

The last witness to take the stand is Butcher, the radio operator, who unexpectedly testifies that he clearly saw a muzzle flash from Compound 6. This statement contradicts his deposition and shocks the court. Pedersen and his attorney looked surprised. Butcher tells the court that he glimpsed the muzzle flash while crouching behind Pedersen as the commander stood up and quickly looked over the wall. He tells the court Pedersen was unaware of him crouching so close. When asked by the prosecution to explain the contradiction with his deposition, Butcher testifies that he wasn't asked *specifically* by the JAG staff if he saw a muzzle flash. When asked why he has remained silent about this vital piece of evidence for six months, he apologizes but simply says, that's just what happened.

After Butcher's testimony, the court deliberates and shortly finds Pedersen not guilty on all charges.

The film highlights at least three incidences of the complexity of the truth-versus-loyalty paradigm. In the first incidence, Pedersen chose loyalty to his men and lied to the TOC in order to initiate an airstrike that would both destroy the enemy and allow a medevac helicopter to land to pick up the wounded Danish soldier. In that light, his decision may be seen as choosing what's best for the greatest number—defined from his perspective as the



wounded soldier and the dozen or so other men of the patrol. Had he told the TOC that he did not have PID, the wounded soldier likely would have died, and others in the patrol might have been wounded or killed before PID was obtained.

In the second incidence, Pedersen refuses to lie before the court, and instead tells his defense attorney that he did not have PID before calling for the airstrike. He says this knowing the prosecution's case is strong and that, unless he says he had PID and is willing to testify to that fact, the odds of avoiding prison are extremely low. Yet he remains adamant that he cannot and will not lie in court, even when facing his wife's angry tears and the realization that his family is already fraying under the strain of his absences. A prison sentence will only make things worse. In that regard, his decision reflects an adherence to a higher principle. The difference between this decision and the one he made on the battlefield is admittedly stark. One explanation may be that this decision is made far from the fog of war and the confusing uncertainty of a firefight in which a fellow soldier is dying. It is made at home, in the

clarity of his family's love and respect, and in that light, rather than lie to save himself, he accepts responsibility both for his lie and the deaths of the women and children killed in the airstrike.

In contrast, it is possible to interpret the third incidence, Butcher's unexpected decision to lie before the court, as a decision made out of empathy and compassion for Pedersen. Butcher was at Pedersen's side during the firefight. He was aware of the stress Pedersen had been under. He too experienced the chaotic violence of the attack and witnessed Pedersen's frantic efforts to arrange for a medevac before the wounded soldier bled to death. He knew the responsibility that Pedersen felt for all those under his command. He was aware of Pedersen's ethical dilemma, and he realized that the rules of engagement (ROEs) were out of sync with the reality of the firefight on the ground. Do all of those considerations automatically make Butcher's decision right? The answer is "No"—at least not automatically.

According to Kidder, there are no "automatic" right choices in a true ethical dilemma. All three of the truth-versus-loyalty decisions made by either Pedersen or Butcher could be challenged. One could argue that while Pedersen's lie to the TOC may have been driven by a desperate need to protect his men, ROEs are intended to prevent tragedies of civilian death exactly like the one Pedersen caused. Just as one might point out that while it may be well and good for Pedersen to adhere to his principles while on trial, the permanent damage his likely imprisonment could inflict on family is both real and avoidable. And finally, while Butcher's lie may be rooted in compassion, it nonetheless undermines the integrity of both the judicial process and the reputation of the military.

Resolving true ethical dilemmas requires serious, critical consideration of the sequence of events, the actors and their motivations, the consequences of each possible resolution, the potential for a compromise, and the moral courage to make a decision. As Kidder attests, "ethics does not happen in a theoretical vacuum but in the push and pull of real experience, where details determine motives and character is reflected in context."[10] In the film, Pedersen's motives appear to be, first, his determination to protect his men, and later, his personal core values of truth and honesty. He is willing to accept responsibility for his first decision, which saved at least one life, and also for his second decision, which risks damaging and possibly destroying his marriage. By comparison, Butcher's motives are never clarified within the film. He does not offer any explanation to Pedersen after the trial, and Pedersen never comments on Butcher's testimony. As the courtroom empties, Pedersen remains seated at the defense's table with a bewildered look on his face.

It is possible that Butcher made his decision out of loyalty and concern for his commander; it's also possible that he made the decision based on reasons entirely more personal and complex. What the film makes clear is that, although Pedersen is found not guilty by the court on the basis of Butcher's lie, he remains guilty of causing the deaths of eleven civilians in an effort to save his men, and that reality will stay with him. The film also makes starkly clear the complex and difficult challenges of the truth-versus-loyalty dilemma.

ABOUT THE AUTHOR

George Lober taught at the US Naval Postgraduate School until his retirement in 2016.

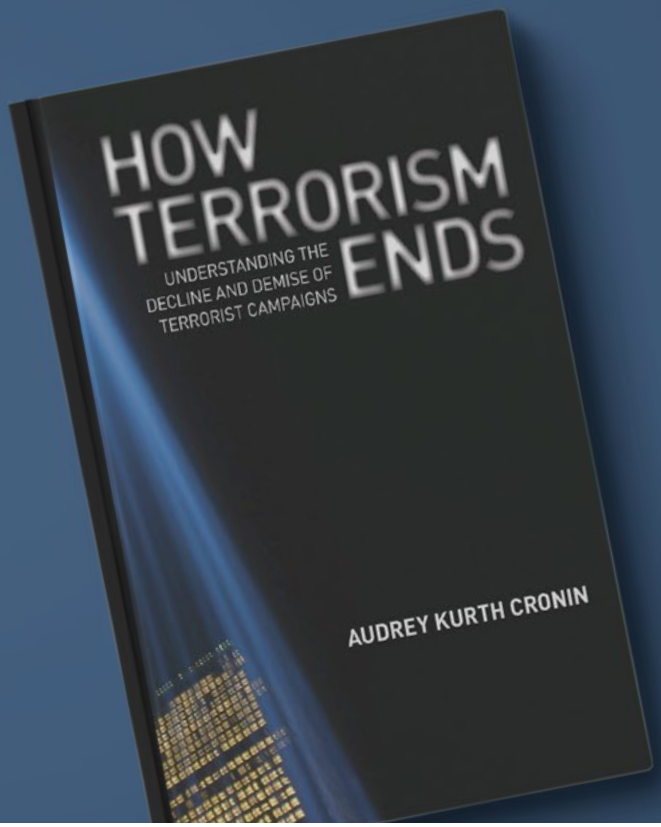
NOTES

1. Rushworth M. Kidder, *How Good People Make Tough Choices: Resolving the Dilemmas of Ethical Living*, rev. ed. (New York: HarperCollins, 2009), 6, Kindle.
2. Ibid., 5.
3. Ibid., 117.
4. Ibid.
5. Ibid.
6. Ibid., 117–118.
7. This is a succinct summary of Kidder's three resolution principles, which are detailed in ibid., chapter seven, 149–175.
8. This paragraph presents a succinct summary of Kidder's Nine Checkpoints for Ethical Decision Making, as detailed in ibid., chapter eight, 178–184.
9. *A War*, directed by Tobias Lindholm (2015; Denmark: Nordisk Film Production, 2016), iTunes.
10. Kidder, *How Good People Make Tough Choices*, 182.

The Written Word

How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns

Reviewed by Chief Warrant Officer 3 Rick Manley , US Army Special Forces



AFTER 18 YEARS OF PERPETUAL WARFARE, THE NEW AMERICAN generation will struggle to imagine a world in which their country is not in conflict. Combating terrorism is now a major role for the US forces that are stationed abroad in nearly 150 countries. It is easy to assume that this role will be a part of US overseas commitments forever, but author Audrey Kurth Cronin shows us that terrorist campaigns can, and do, end. In her scholarly and exceptionally well-written book, Cronin describes a six-part framework for understanding how previous terrorist campaigns have ended—through decapitation, negotiation, success, failure, repression, or reorientation—and applies this framework to consider the possible ways by which current campaigns may conclude. History, she suggests, can guide our policies toward enabling such ends.

How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns
By Audrey Kurth Cronin
Princeton: Princeton University Press, 2011
311 pages
Paperback: $22.00

"Focusing on how terrorism ends is the best way to avoid being manipulated by it,"[1] writes Cronin. This simply stated message could be useful to anyone, including CT professionals and policymakers, who sees global terrorism as a new fact of human existence and believes that the current wave of religious terrorism will never end. Cronin meticulously gathers case studies of the final stages of terrorist campaigns and presents that information in an understandable way. Although the book is clearly written with the researcher in mind, the author makes it easy to understand for even a reader new to counterterrorism theory.

> **The current strategy for combating Islamist terrorism, which requires the application of brute force to compel the enemy into submission, is destined to fail.**

Cronin begins with a thorough explanation of her research methodology. She asserts that there are three strategic actors in any terrorism campaign, which she refers to collectively as the "Triad:" "the group, the government, and the audience."[2] By analyzing the interactions between these three actors, Cronin determines that terrorism campaigns can have six possible outcomes: "capture or killing of the group's leader, entry into legitimate politics, the achievement of aims, implosion or loss of public support, defeat and elimination, and transition into other forms of violence.[3] These six outcomes, each of which is a separate

section of the book, comprise the framework through which she analyzes the campaigns of several dozen terrorist groups. This outline makes it easy for the reader to follow the flow of Cronin's theory through her discussion of group outcomes.

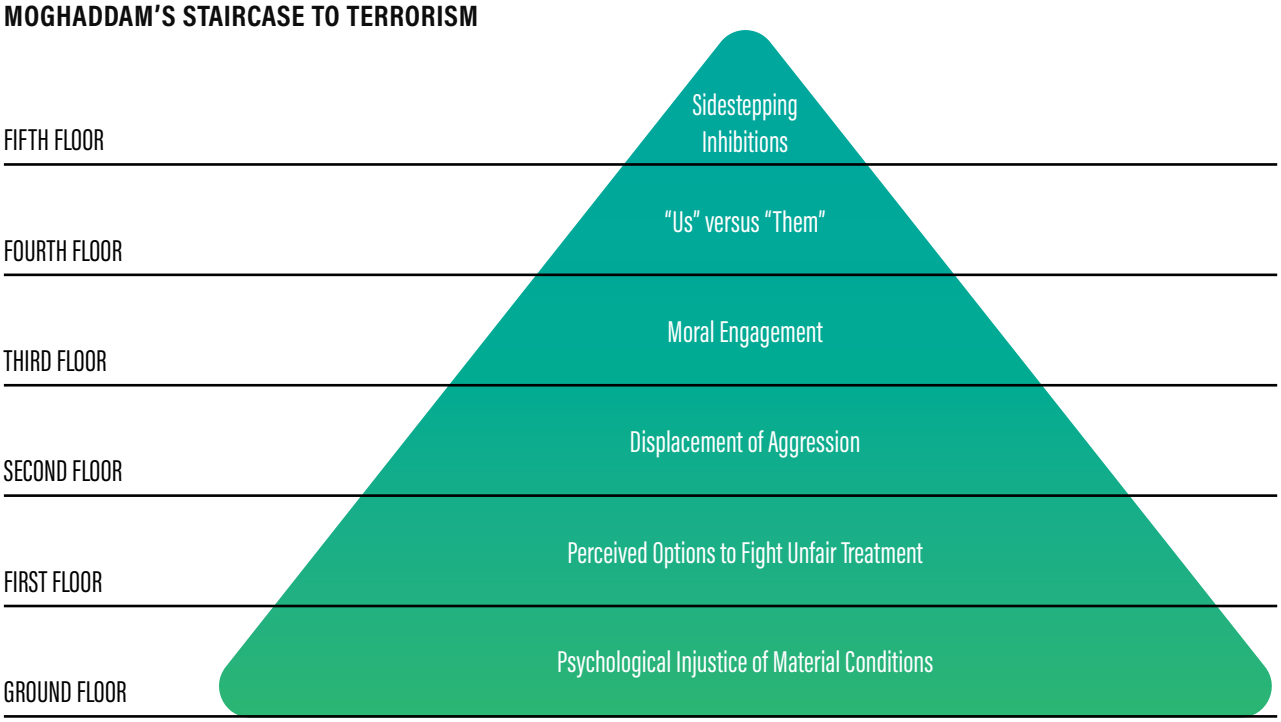
In summarizing *How Terrorism Ends*, three points must be addressed. First, Cronin explains that the current strategy for combating Islamist terrorism, which requires the application of brute force to compel the enemy into submission, is destined to fail. Terrorism is a battle of asymmetry in which a weak opponent attacks a stronger opponent; classic compellence is ineffective because the potential perception of overreaction by a military force provides legitimacy to the weaker opponent. This is a well-supported example of Ivan Arreguín-Toft's strategic interaction theory, which holds that a strong actor executing a direct approach can expect to lose to a weak actor conducting an indirect approach.[4] When they come under direct attack, Cronin explains, terrorists are able to "maximize their influence vis-à-vis the power of the state by finding ways to wedge open the flaws, cracks, imperfections, and vulnerabilities and break them wide open."[5] This approach seems to account for the rapid rise of Islamist terrorist activities in the years since 9/11, despite aggressive global military action focused on countering them.

Second, Cronin explains that an indirect approach to combating terrorism has a higher chance of success because "the key thing is to understand long-established processes of implosion."[6] The state has a much higher chance of causing the group to implode through lack of support if the state seeks to isolate and marginalize the terrorists from the community. Because the goal of terrorists is to provoke the stronger power or state to fight on their terms, Cronin argues that the state must remain conscious that the real battle is for legitimacy in the eyes of the community, and the most critical goal is to delegitimize the terrorist's message and means. As she points out, "marginalization from their constituency is the death-knell for modern [terrorist] groups."[7] This point reinforces what many professionals in the CT community have learned over the last 20 years: there is a need for deradicalization programs in vulnerable communities. Fence-sitting and passive support could be ideal targets of an indirect state-led campaign to decrease support for extremism among the moderate majority.

RAPOPORT'S FOUR WAVES OF MODERN TERRORISM

Anarchist Wave	Anti-Colonial Wave	New Left Wave	Religious Wave
Beginning: 1880s in Russia — Aim: Removal of repressive and abusive governments — Science: Assassinations and dynamite — Image: Martyr and Hero	Beginning: Treaty of Versailles at the end of WWI — Aim: Desire to be independent and form new states — Science: strategic removal of police, military, governmental figures to bolster support — Image: Freedom Fighters	Beginning: Vietnam War — Aim: Express disapproval of current system — Science: Hostages, kidnapping, assassinations as punishment — Image: Transition from Freedom Fighters to Terrorists	Beginning: 1979 Iranian Revolution, new Islamic Century and Soviet Union invading Afghanistan in 1979 — Aim: Creation of religious state — Science: Suicide bombing, mass killings — Image: Modern Jihadist Terrorists

MOGHADDAM'S STAIRCASE TO TERRORISM



> **A successful counterterrorism strategy must use "strategies of leverage rather than compellence to prevent the campaign drawing energy from the state's response."**

Finally, Cronin concludes that a successful counterterrorism strategy must use "strategies of leverage rather than compellence to prevent the campaign drawing energy from the state's response."[8] A strategy of leverage seeks to deny the terrorist group what it aims to achieve, whether that is an overreaction to a provocation strategy, attention to a particular grievance through polarization, or co-opting mass support through mobilization. The state must remain focused on not reacting in a manner complementary to the terrorist goal. Instead, strategies of leverage would adopt specific responses designed to deny the terrorists' objectives. In response to a provocation strategy, for example, the state might promote programs that develop resiliency in a particular community in response to terrorist actions, rather than resorting to repression and crackdowns. Again, according to Arreguín-Toft's strategic interaction theory, a strong actor committed to an indirect approach against a weak actor is much more likely to succeed. In this, Cronin and Arreguín-Toft would agree.

Cronin's book focuses on the ways in which the Triad of terrorists, governments, and audiences affects how specific terrorist organizations come to an end. David C. Rapoport's "Four Waves of Modern Terrorism" is a good complement to Cronin's thesis. Rapoport describes four waves of modern terrorism and asserts that each wave is "composed of organizations, but waves and organizations have very different life rhythms."[9] Rapoport's wave model is widely considered to be the most comprehensive and compelling analysis of modern terrorism, and a basic understanding of the four-wave theory would provide the reader with a beneficial lens through which to view Cronin's work.

Rapoport's theory can be seen as the macro view of the terrorism problem. For the micro view, another complementary work to Cronin's is Fathali M. Moghaddam's *Staircase to Terrorism*. Moghaddam focuses on the individuals who enlist to participate in terrorist activities and the motivating factors that enable their radicalization. Reflecting Cronin's ideas, Moghaddam states, "Over at least the last few decades, policies for ending terrorism have tended to be short-term, often driven by immediate political demands rather than by scientific understanding."[10] Moghaddam outlines the progression of conditions that can lead to terrorist activity, which is an important consideration when layered with Cronin's discussion of perception and identity as crucial factors for ending terrorist movements.

> **We must be motivated by the idea that current terrorist campaigns will end when we stop lending them legitimacy.**

Cronin's message to future counterterrorism professionals is clear: the state must insist upon "using strategies of leverage rather than compellence to prevent a campaign from drawing energy from the state's response."[11] In effect, we must be motivated by the idea that current terrorist campaigns will end when we stop lending them legitimacy and allow them to "disintegrate, falling under the weight of their own unpopular tactics."[12] In a chapter titled "How Al-Qaeda Ends," Cronin highlights this concept by posing it as a way to end al-Qaeda's global campaign. She explains that al-Qaeda gains strength by exploiting the fundamental differences in Muslims' worldviews through the use of rhetoric and propaganda. She asserts that al-Qaeda will lose its legitimacy when "the West removes itself from the heart of [that] fight and turns [al-Qaeda's] own abundant missteps against it."[13] In other words, she offers a way to win without fighting—one that is also particularly applicable to ISIS.

I strongly encourage anyone in the counterterrorism field, from soldier to policymaker, to become familiar with this work, and to apply its lessons to future counterterrorism efforts and policies. Cronin's research demonstrates significant depth and scope and is highly relevant to current discussions of counterterrorism. A counterterrorism professional who layers Cronin's work with the complementary readings mentioned above can expect to acquire a good understanding of the problem and its potential outcomes in a reasonably concise manner.

ABOUT THE AUTHOR

Chief Warrant Officer 3 Rick Manley serves in the US Army Special Forces.

NOTES

1. Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton: Princeton University Press, 2011), 1.
2. Ibid., 7.
3. Ibid., 8.
4. Ivan Arreguín-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* 26, no. 1 (Summer 2001): 93-128.
5. Cronin, *How Terrorism Ends*, 198.
6. Ibid., 203.
7. Ibid.
8. Ibid., 206.
9. David C. Rapoport, "The Four Waves of Modern Terrorism," in *Attacking Terrorism: Elements of a Grand Strategy*, ed. Audrey Kurth Cronin and James M. Ludes (Washington, DC: Georgetown University Press, 2004), 3-11, 54.
10. Fathali M. Moghaddam, "The Staircase to Terrorism: A Psychological Exploration," *American Psychologist* 60, no. 2 (2005): 166: https://doi.org/10.1037/0003-066X.60.2.161
11. Cronin, *How Terrorism Ends*, 206.
12. Ibid., 203.
13. Ibid., 196.

The Written Word

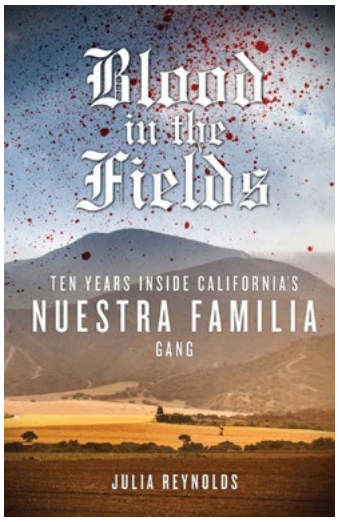
Blood in the Fields: Ten Years Inside California's Nuestra Familia Gang

Reviewed by MAJ George W. Bailey, US Army Civil Affairs

Salinas, California

THERE IS A HIDDEN WORLD AROUND US. Chances are, you see it daily but don't recognize the signs. The strange symbol that is spray-painted on an overpass, the guy in the team jacket at the grocery store, or the person with unusual tattoos passing you by on the street may be communicating something vital about your community that you fail to recognize. The people who live in this world walk their dogs on the same streets you do, go to school with your children, and may even attend the same church as your family. But they also kill for work and enjoyment, rob for beer money, and consider jail an opportunity for promotion. They are the street gang. They live in your world, but you don't live in theirs.

In this non-fiction account, Julia Reynolds follows members of the *Nuestra Familia* (Our Family, NF) prison gang and the street-level *Norteños* (Northerners) gang, offering readers an episodic view of gang life during the early 2000s, when the FBI operations "Black Widow" and "Valley Star" were ongoing. Reynolds supplements her own prison visits and interviews with news articles, court documents, and surveillance and informant recordings to reconstruct the events as they occurred. Counter-gang and counterterrorism professionals who are interested in understanding the inner workings of organized criminal groups will find this book useful for their professional development and research. However, casual readers will also find it both interesting and informative. The book is well sourced, and the author makes an intensive effort to present her research without personal interpretation. Rather than present her findings on gangs from a criminologist's analytical perspective, Reynolds chooses instead to let the gang members tell their story.



Blood in the Fields: Ten Years Inside California's Nuestra Familia Gang
By Julia Reynolds

Chicago: Chicago Review Press, 2014
338 pages
Paperback: $15.29

Most Central and Northern California youth are familiar with Nuestra Familia and the Norteños.

NF, founded in the late 1960s, has been evolving into a transnational umbrella organization that controls smaller street-level gangs. NF consists primarily of *La Familia* (the Family), the group's core leadership, and the Norteños, the street-level and lowest echelon of the gang. NF is centrally governed by *La Mesa* (the Table), an incarcerated board of "generals" and "captains" who exert command and control from within the prison system. Street-level Norteños are further organized into county- and city-level regiments, and serve as the entry point for NF membership.

Most Central and Northern California youth are familiar with NF and the Norteños. Young Chicano (Mexican-American) men may be attracted to the Norteños because of the respect that they believe Norteños receive, as well as the sex, partying, money, and drugs. The gang also has a unifying ideology called the Cause, a conglomeration of Latino cultural heritage, the United Farm Workers labor movement, and a sense of solidarity fueled by the abuse of Northern California Chicanos and Mexican immigrants by *La Eme* (the "M"), a Los Angeles-based street gang; La Eme and the *Sureños* (Southerners) are a mirror image of NF and the Norteños and are considered their primary rivals. Explaining the Cause and how its meaning has changed since NF's founding as the Salinas East Market (SEM) street gang, Reynolds writes:

> in the fight for their identity and rights, the SEMsters drew inspiration from the United Farm Workers and Chicano and Black Power movements. But the struggle against a vague establishment oppressor quickly took a back burner as the Sureño threat became the group's priority. SEM had transformed into a criminal gang that used civil rights jargon to lure youngsters into what they called the Cause. The Norteños' cause was not La Causa of the farmworkers and Chicano civil rights workers; it was a thuggish concept of uniting to beat down the perceived invasion of Sureños.[1]

Norteños tag

Norteños who aspire to become full-fledged NF members first have to earn the title of *carnal*, "blood brother," a step that usually involves committing murder.

Reynolds gives a great description of how NF recruits new members, indoctrinates them, and incentivizes violence, a process that is as ingenious as it is insidious. Norteños who aspire to become full-fledged NF members first have to earn the title of *carnal*, "blood brother," a step that usually involves committing murder on behalf of NF. Norteños are incentivized to become killers and conditioned not to equate incarceration with failure; all of NF's top leadership are incarcerated, and this is an accepted facet of gang life. Prospective Norteños are ordered by NF to use their time to further their education for the Cause. New members learn the history of NF and study literary works such as Machiavelli's *The Prince* and Sun Tzu's *The Art of War*.

The book also presents a valuable perspective on the nuances of the gang's administration. The Norteños pay taxes to fund the incarcerated NF leadership, who in turn send enforcement orders to the Norteños. The taxes fund special gang programs such as the protection of incarcerated

Then-California Attorney General Kamala Harris announces conclusion of Operation Red Zone, in which 16 local, state, and federal agencies arrested 101 gang members in Madera and Merced counties. Los Baños, Calif., 8 June 2011.

gang affiliates, support to members' families, and even a legal fund—similar in some ways to Hezbollah's taxation system and social programs. The Norteños enforce the rules of the organization, which usually involves killing any offender; in fact, Norteños kill more Norteños than they do Sureños, their archenemies. The Norteños who are caught and convicted of these crimes become members of the prison organization, and the cycle repeats.

Some of the gang members who appear in the book eventually reached a point where they began to see that the reality of life as an NF member was not what they once believed it would be. They realized that the Cause was a construct of their teen angst-fueled imaginations, and felt that they had become stooges of the NF Generals. Some members began to have their own families, and to question their choices and the meaning of their lives. However, they also knew that NF and the Norteños are "blood-in and blood-out" gangs, which means that the only way to leave is death. This is a recurring dilemma that many of the characters in the book came to face. Sal, one of the book's subjects, faces this impasse as he begins to come of age:

> [Sal] was a full-on familiano who had taken the "blood in, blood out" oath of the gang. According to the constitution he had vowed to uphold, the only way to leave Nuestra Familia was death. Yet now, for the first time since he swore to the Fourteen Bonds and put in the work to become a carnal, he wavered. Family tugged at him—his real family, not the prison gang generals who'd promised to replace the love of kin in exchange for his soul.[2]

Many of the gang members who do decide to leave the gang choose to debrief with counter-gang investigators. Getting away from the gang without being killed usually entails becoming an informant for either the FBI or California's Central Coast NF gang task force in exchange for witness protection.[3] Reynolds tells the story of the FBI's and the gang task force's use of informants during Operation Black Widow. At one point, the FBI lost track of a high-level NF informant who was acting as a sort of double agent, playing both sides of the law. Although ostensibly working with law enforcement, he continued to conduct Familia business and even "green-lighted" an execution; he then wore a wire (a hidden transmitter) and tried to call off the murder, but it turned out that this effort was a ruse by the informant to satisfy the FBI's need for incriminating evidence while maintaining his own innocence. In this case, the Norteños who carried out the execution were prosecuted and the

informant was protected. Mistakes like this riddled the FBI's entire operation, not only hurting the Bureau's creditability, but also creating tension between the FBI and the counter-gang task force. The book does an excellent job of illustrating complications such as these, as well as the bureaucratic hurdles involved in investigating and prosecuting gang members.

This book is a good resource for understanding the inner workings of NF, describing the organization from the perspective of gang members, informants, and law enforcement. Reynolds succeeds in organizing over ten years' worth of stories, information, and data into a single comprehensible work. She presents the facts within a dramatic storyline that is not only intriguing, but also contains real-world lessons that can be applied to counter other kinds of criminal organizations.

The many parallels between gangs like NF and terrorist organizations will be immediately apparent to the Special Operations community and counter-terrorism professionals. *Blood in the Fields* offers a fact-based, inside account of methods of recruitment, training, and indoctrination. It vividly captures how an organization's ideology can attract and bind members to a violent lifestyle that transcends an individual's love of family and instinct for self-preservation. Understanding the motivations and pressures that individuals and their communities face is valuable for designing counter-terrorism strategies.

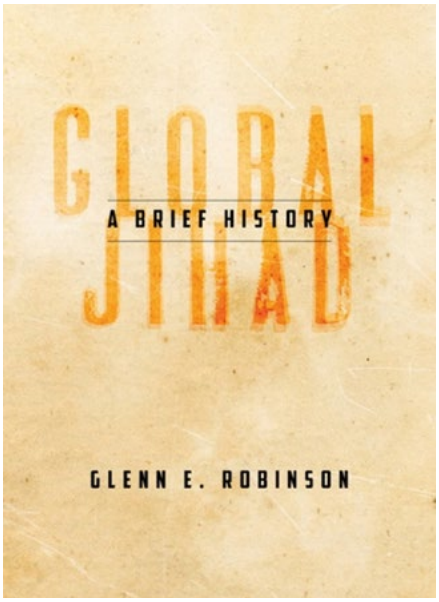
ABOUT THE AUTHOR

MAJ George W. Bailey is a US Army Civil Affairs officer.

NOTES

1. Julia Reynolds, *Blood in the Fields: Ten Years Inside California's Nuestra Familia Gang* (Chicago: Chicago Review Press, 2014), 9.
2. Ibid., 14.
3. The Central Coast NF gang task force is a regional task force that was formed by non-federal law enforcement agencies from Santa Cruz, Hollister, Watsonville, Castroville, and Salinas, California.

Publications



Global Jihad: A Brief History
Glenn E. Robinson

Most violent jihadi movements in the twentieth century focused on removing corrupt, repressive secular regimes throughout the Muslim world. But following the 1979 Soviet invasion of Afghanistan, a new form of jihadism emerged—global jihad. With this book, Glenn E. Robinson develops a provocative argument about this violent political movement's evolution.

Global Jihad tells the story of four distinct jihadi waves, each with its own program for achieving a global end: a Jihadi International to liberate Muslim lands from foreign occupation; al-Qa'ida's call to drive the United States out of the Muslim world; ISIS using "jihadi cool" to recruit followers; and leaderless stochastic terror to "keep the dream alive." Robinson connects the rise of global jihad to other "movements of rage" such as the Nazi Brownshirts, White supremacists, Khmer Rouge, and Boko Haram. Ultimately, he shows that while global jihad has posed a low strategic threat, it has drawn an outsized reaction from the United States and other Western nations.

ABOUT THE AUTHOR

Glenn E. Robinson is on the faculty at the Naval Postgraduate School in Monterey, California, and is affiliated with the Center for Middle Eastern Studies at the University of California, Berkeley. He has served as an expert advisor to USAID and the US Department of Defense.

Image Credits

Page 1: Wojtek Radwanski/AFP via Getty Images

Page 6: Jean Duplessis-Bertaux, Public Domain, via Wikimedia Commons

Page 7: Public Domain, via Wikimedia Commonspage 7: Defensie / CC0

Page 8: The Print Collector/Print Collector/Getty Images

Page 9: Unknown Author, Public Domain, via Wikimedia Commons

Page 10: Jean Duplessis-Bertaux, Public Domain, via Wikimedia Commons

Page 11: Lcpl. Tommy Bellegarde, Public Domain, via Wikimedia Commons

Page 18: Joseph Eddins, Public Domain

Page 19: Joseph Eddins, Public Domain

Page 20: Senior Master Sgt. Adrian Cadiz, Public Domain, via Wikimedia Commons

Page 21: Ministry of Defence, CC0, via Wikimedia Commons

Page 24: Defensie, CC0, via Wikimedia Commons

Page 25: Cmapm, CC BY-SA 3.0, via Wikimedia Commons

Page 26: Wojtek Radwanski/AFP via Getty Images)

Page 29: Hamed Saber, CC by 2.0, via Wikimedia Commons

Page 34: Imranrashid26, CC BY-SA 3.0, via Wikimedia Commons

Page 38: Irfan.anwaar.hussain, CC BY-SA 3.0, via Wikimedia Commons

Page 41: Asad Zaidi/Bloomberg via Getty Images

Page 45: British Library, Public Domain, via Wikimedia Commons

Page 46: Metin Aktas/Anadolu Agency/Getty Images

Page 47: Public Domain, via Wikimedia Commons

Page 50: Ersal Khan, CC BY-SA 4.0, via Wikimedia Commons

Page 51: Abdul Majeed/AFP via Getty Images)

Page 58: Jacques-Louis David / Public Domain

Page 66: Agarre16, CC BY-SA 4.0, via Wikimedia Commons

Page 67: Stalag 16, CC BY 2.0, via Wikimedia Commons

Page 68: Office of the Attorney General of California, Public domain, via Wikimedia Commons

Terms of Copyright

Call for Submissions

The *Combating Terrorism Exchange* (*CTX*) is a quarterly peer-reviewed journal. We accept submissions of nearly any type, from anyone; however, submission does not guarantee publication. Our aim is to distribute high-quality analyses, opinions, and studies to military officers, government officials, and security and academic professionals in the counterterrorism community. We give priority to non-typical, insightful work and to topics concerning countries with the most pressing terrorism and CT issues.

Submission Guidelines

For detailed submission guidelines, go to https://GlobalECCO.org and click on the *CTX* Home link. Then click on Submissions in the left menu bar.

CTX accepts the following types of submissions. Please observe the following length guidelines:

- **academic analyses** (up to 6,000 words)
- **reports or insightful stories from the field** (up to 5,000 words)
- **photographic essays**
- **video clips** with explanation or narration
- **interviews** with relevant figures (no longer than 15 minutes)
- **book reviews** (up to 2,000 words), review essays (up to 2,000 words), or lists of books of interest (which may include books in other languages)
- reports on any **special projects**
- Any kind of submission can be **multimedia**.

Submission Requirements

Submissions to *CTX* must adhere to the following:

- The work must be copyedited for basic errors *prior to* submission.
- Citations should adhere to the *Chicago Manual of Style*. See the latest version at http://www.chicagomanualofstyle.org/home.html
- The work submitted may not be plagiarized in part or in whole.
- You must have permission to use any images, videos, or statements included in your work.
- You must agree to our Terms of Copyright.
- Include a byline as you would like it to appear and a short bio as you would like it to appear (we may use either, or both).

Submissions should be sent in original, workable format. In other words, we must be able to edit your work in the format in which you send it to us, such as Microsoft Word—no PDFs, please.

Submissions must be in English. Because we seek submissions from the global CT community, and especially look forward to work that will stir debate, *we will not reject* submissions outright simply because of poorly written English. However, we may ask you to have your submission ŷedited before submitting again.

Ready to Submit?

By making a submission to *CTX*, you are acknowledging that your submission adheres to the requirements listed above, and that you agree to the *CTX* Terms of Copyright, so read them carefully.

Submit to CTXEditor@GlobalECCO.org

If you have questions about submissions, or anything else, contact CTXEditor@GlobalECCO.org

CTX is online at globalecco.org