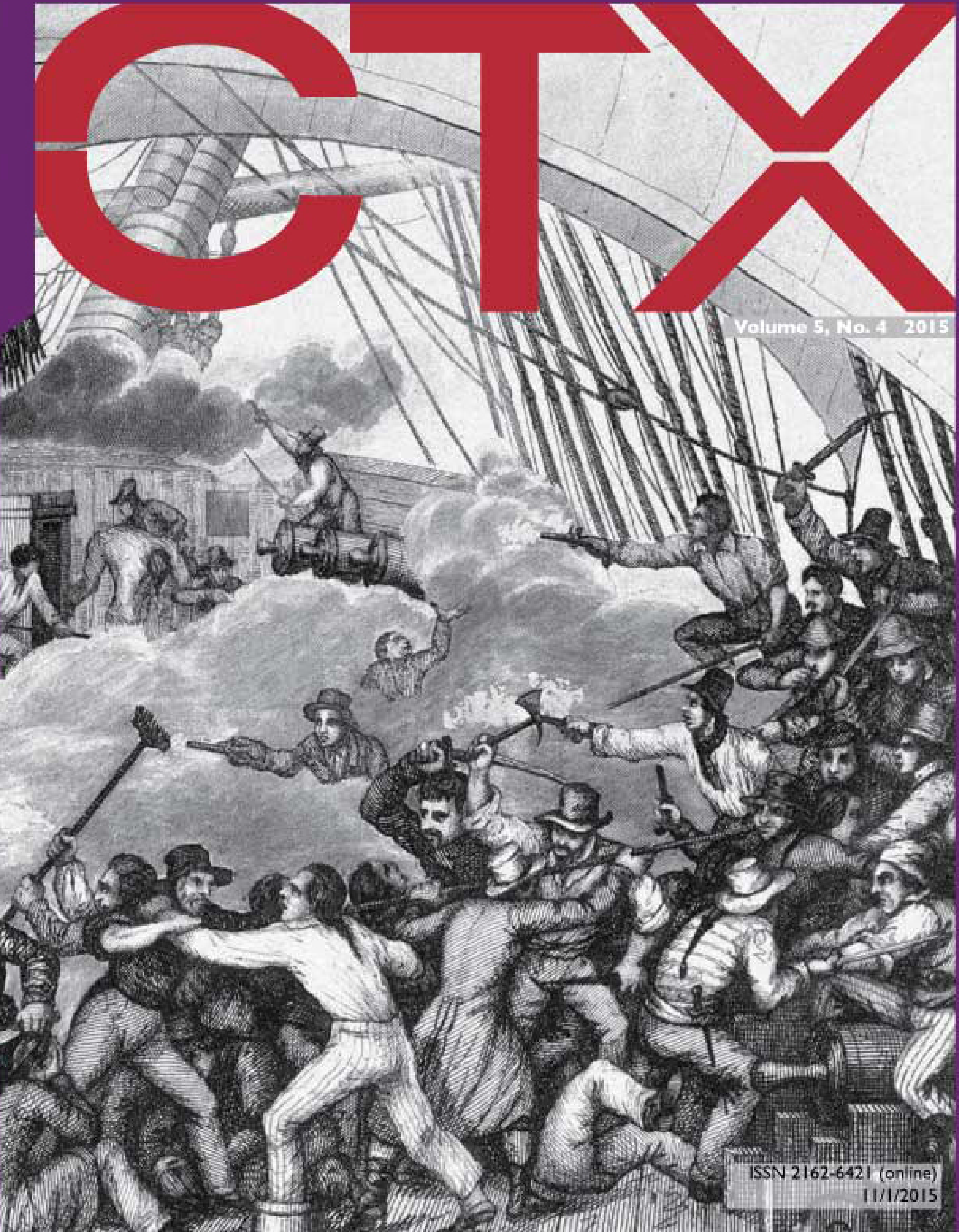
CTX

Volume 5, No. 4 2015



ISSN 2162-6421 (online)
11/1/2015

CTX

From the Editor

Special Operations Forces have perpetually been on the frontlines of the world's military conflagrations, using every tool and skill currently available to them to prevent potential fuel from catching fire. SOF battle the blazes of sectarian war, locate the spot fires of extremist infiltration, and help people clear away the ashes and get back on their feet after conflict. Many of you have been involved in countering insurgency in one capacity or another, and you'll appreciate the personal stories our authors in this issue of *CTX* have to tell.

The first story is not about fighting bad guys, but about how those who fight bad guys turn their skills to saving lives and delivering humanitarian relief. SOF Lieutenant Commander Gilbert Villareal describes what happened after Typhoon Yolanda (also known as Typhoon Haiyan) smashed the Philippines in late 2013. Dealing with the aftermath demanded as much of his training and courage as his counterinsurgency missions ever had. Disaster relief, LTC Villareal admits, doesn't seem "sexy" to most SOF warriors. But it is deeply rewarding and well within the scope of the special operations mandate.

The next two pieces, by retired Pakistani Air Commander Jamal Hussain, take us back to the commando raid that killed Osama bin Laden in 2011. The first essay addresses the question of how four US helicopters managed to cross into Pakistani airspace, fly 100 nautical miles to Abbottabad, carry out the attack, and (minus one Blackhawk that crashed) escape back over the Afghan border before Pakistan's air defenses could react. The second essay rebuts, point by point, investigative reporter Seymour Hersh's recent retelling of the bin Laden raid as a top-level conspiracy of mass deception.

The Liberation Tigers of Tamil Eelam (LTTE) fought a 30-year insurgency against the armed forces and government of Sri Lanka that nearly tore the country apart. Colonel Sylvester Perera describes how he and his fellow commanders struggled to adapt their legacy British-style training and strategic planning to counter the highly mobile and innovative LTTE. A united national front, COL Perera concludes, is vital for the future of Sri Lanka.

Major Daniel Pace uses his experience in Baghdad during the surge of US forces in 2007 to highlight the price a country may pay if it fails to unite after internal conflict. His platoon succeeded in replacing disrupted government services and channels of influence with its own improvised systems in an important Sunni neighborhood. But this success paradoxically deepened sectarian distrust once it came time for the Americans to pull out.

The skies around us, Captain Benjamin Seibert points out, are increasingly filled with those remote-controlled aircraft called drones. Drones are great for reconnaissance, lauded and vilified for their ability to deliver missiles, and promoted as the next big thing in online shopping. CPT Seibert warns, however, that drones and their attendant technologies are a terrorist's dream, and no one seems to know what to do about the danger.

Extremists have already shown us how quickly and effectively they can spread their ideology in cyberspace and how useful the internet is as a means of recruitment. Lieutenant Colonel Robert Schultz draws parallels between the open seas and the electronic frontier, and suggests that it's time we looked back to the age of privateers for inspiration about how to deal with cyber terrorists.

Nations and international organizations, including the UN and NATO, have embraced a concept for crisis management called the *comprehensive approach* (CA), which purports to enable the coordination of assets to contain and resolve crises. The problem with CA, as Lieutenant Colonel Sándor Fábián points out, is that no one agrees on a common definition for the concept, much less what it entails.

For our CTAP interview, Dr. Doug Borer of the US Naval Postgraduate School interviews counterinsurgency and crisis response specialist David Kilcullen about current trends in counterinsurgency planning and operations. Dr. Kilcullen also discusses ISIS at length: are we in the midst of a new Thirty Years' War, fomented to a large degree by information technology? That, warns Dr. Kilcullen, is a question worth asking.

We have two book reviews in this issue. The first, by Major Bradley J. Krauss, explores *American Force: Dangers, Delusions, and Dilemmas in National Security* by senior national security expert Richard K. Betts. While this book might seem to lie somewhat outside the CT-COIN realm, MAJ Krauss recommends it for military personnel like himself who are reentering academia after a long period of active service, and need to "jump-start" their capacity for critical thinking about international relations. The second book, *The Hour between Dog and Wolf: Risk Taking, Gut Feelings, and the Biology of Boom and Bust* by John Coates, examines the nexus between biology and decision making in high-stress environments. Lieutenant Adam Karagouz describes some of the implications for risk-taking organizations like special operations teams.

In this issue's Moving Image review, Ian Rice finds the AMC television series *Turn: Washington's Spies* satisfying for both its historical reenactment of eighteenth-century irregular warfare and as sheer entertainment. *Turn* follows a number of characters on both sides of the American Revolution as they seek to undermine their opponents' base of support among the colonists through intrigue and espionage.

Be sure to take a look at the latest publications from the Joint Special Operations University in our Publications Announcements. Write to CTXeditor@GlobalEcco.org and let us know what you think about what you've read in *CTX* or anything else in the CT world that's on your mind. You can also keep up on global CT news and comment on articles by "liking" Global ECCO on Facebook. If you are interested in submitting an article for possible publication, send it to CTXSubmit@GlobalEcco.org.

ELIZABETH SKINNER

Managing Editor, *CTX*
CTXEditor@globalecco.org

Inside This Issue

ABOUT THE CONTRIBUTORS

Dr. Doug Borer is an associate professor of Defense Analysis at the US Naval Postgraduate School (NPS), Monterey, California. He earned his PhD in political science from Boston University in 1993. Dr. Borer's academic postings include the University of the South Pacific, the University of Western Australia, Virginia Tech, the Universiti Kebangsaan Malaysia, and the US Army War College. In 2007, he co-founded (with Dr. Nancy Roberts) the Common Operational Research Environment (CORE) Lab at NPS. In 2011, he and Dr. Leo Blanken created the Combating Terrorism Archive Project.

Lieutenant Colonel Sándor Fábián is a Special Forces officer in the Hungarian Army, currently serving as head of the Assessment and Evaluation Branch, NATO Special Operations Headquarters, in Mons, Belgium. In 2006, CPT Fábián helped create the Hungarian Special Forces Battalion as a Special Forces company commander. In early 2009, he was promoted to major and deployed to Afghanistan as the commander of the Hungarian Special Forces element. In June 2012, MAJ Fábián became the senior Special Forces advisor at the Operational Directorate of the Hungarian General Staff. He was promoted to lieutenant colonel in 2014.

Air Commodore (Ret.) Jamal Hussain is the director of Pakistan's Center for Air Power Studies. Commissioned in 1966 as a combat pilot in the Pakistan Air Force (PAF), he remained in active service until his retirement in 1997. He is a graduate of the Air Command and Staff College, USAF, and the National Defence College (NDC), Pakistan. He served as an instructor at NDC, commanded an operational air base, and was commandant of the Joint Services Staff College. After retirement, Air CDR Hussain served as director of the Pakistan Civil Aviation Authority for three years and took his current post in 2001. Hussain has written two books, *Air Power in South Asia* (self-published, 2005) and *Dynamics of Nuclear Weapons in South Asia* (PAF Press, 2006).

Lieutenant Adam Karagouz is a US Naval Special Warfare officer currently pursuing an MS degree in the Defense Analysis department at NPS.

Dr. David Kilcullen is the founder and chairman of Caerus Global Solutions, a strategic research and design consultancy, and is chairman of First Mile Geo, a geospatial analysis start-up that helps afflicted communities create participative maps to guide humanitarian assistance efforts. During 24 years' service as an infantry officer in the Australian Army, Dr. Kilcullen was seconded to the US State Department as chief strategist in the Counterterrorism Bureau (2005–2006), then became a senior counterinsurgency advisor to General David Petraeus in Iraq (2007) and senior advisor for counterinsurgency to Secretary of State Condoleezza Rice (2007–2008). He is the author of numerous scholarly articles and three books, including PROSE Award winners *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford University Press, 2009) and *Out of the Mountains: The Coming Age of the Urban Guerrilla* (Oxford University Press, 2013).

Major Bradley J. Krauss is a graduate of the US Military Academy. During more than 10 years of active Army service, he has served in both command and staff positions in support of contingency operations in Iraq, the Philippines, and Afghanistan. MAJ Krauss is currently pursuing a graduate degree at NPS, where his research focuses on the future role of Special Operations Forces in supporting the geographic combatant commanders' objectives.

Colonel Sylvester Perera is currently working toward a master's degree in Defense Analysis at NPS. He joined the Sri Lankan Army as an officer cadet in 1990 and was commissioned as a second lieutenant to the Gemunu Watch regiment in 1992. He has held numerous appointments in command, staff, and instructor capacities during his military career, including commander of a platoon and company in the 6th Battalion and commander of the 8th Battalion of the Gemunu Watch. COL Perera served in the directing staff of the Sri Lankan Defence Services Command and Staff College from 2012 to 2015.

Major Daniel Pace is a Special Forces officer with 14 years of service in the US Army. He has operational experience in Iraq, Afghanistan, Colombia, and Peru. MAJ Pace earned a BA in philosophy from Texas A&M University and is currently pursuing his master's degree in Defense Analysis at NPS. He plans to return to the Special Forces regiment after graduation.

Ian C. Rice is a US Army officer with over 24 years of active service. He has served in a variety of command, staff, and advisory positions in support of combined operations in Afghanistan, Iraq, and Korea, all of which concentrated on the challenges of irregular war. He is currently a PhD candidate in political science at the University of California, Los Angeles, where his research focuses on the impacts of military assistance activities on the institutional development of partner militaries and subsequent effects on domestic and regional politics.

Lieutenant Colonel Robert Schultz is a US Army information operations officer and a 2015 US Army War College Fellows program graduate from NPS. He is currently assigned as the G7, information operations chief for the US Army's 1st Corps.

Captain Benjamin Seibert currently serves as a foreign area officer in the US Army. As an armor officer, he deployed to Iraq in 2006–2007 and 2008–2009 with the 3rd Squadron, 4th United States Cavalry Regiment. He also served as a troop commander in the 11th Armored Cavalry Regiment at the Army's National Training Center. He recently graduated with an MA in National Security Affairs from NPS.

Lieutenant Commander Gilbert Villareal is an officer in the Philippine Navy, where he has served with the Naval Special Warfare Group for 13 years. He is currently working toward a master's degree in Defense Analysis at NPS.

COVER PHOTO

Boarding of the *Triton* (a British East Indiaman) by the privateer *Hasard*. Engraving by Ambroise Louis Garneray via Wikipedia at https://en.wikipedia.org/wiki/Triton_%281787_EIC_ship%29#/media/File:Triton-Hasard-stitched.jpg.

DISCLAIMER

This journal is not an official DoD publication. The views expressed or implied within are those of the contributors and do not necessarily reflect the views of any governmental or nongovernmental organization or agency of the United States of America or any other country.

TERMS OF COPYRIGHT

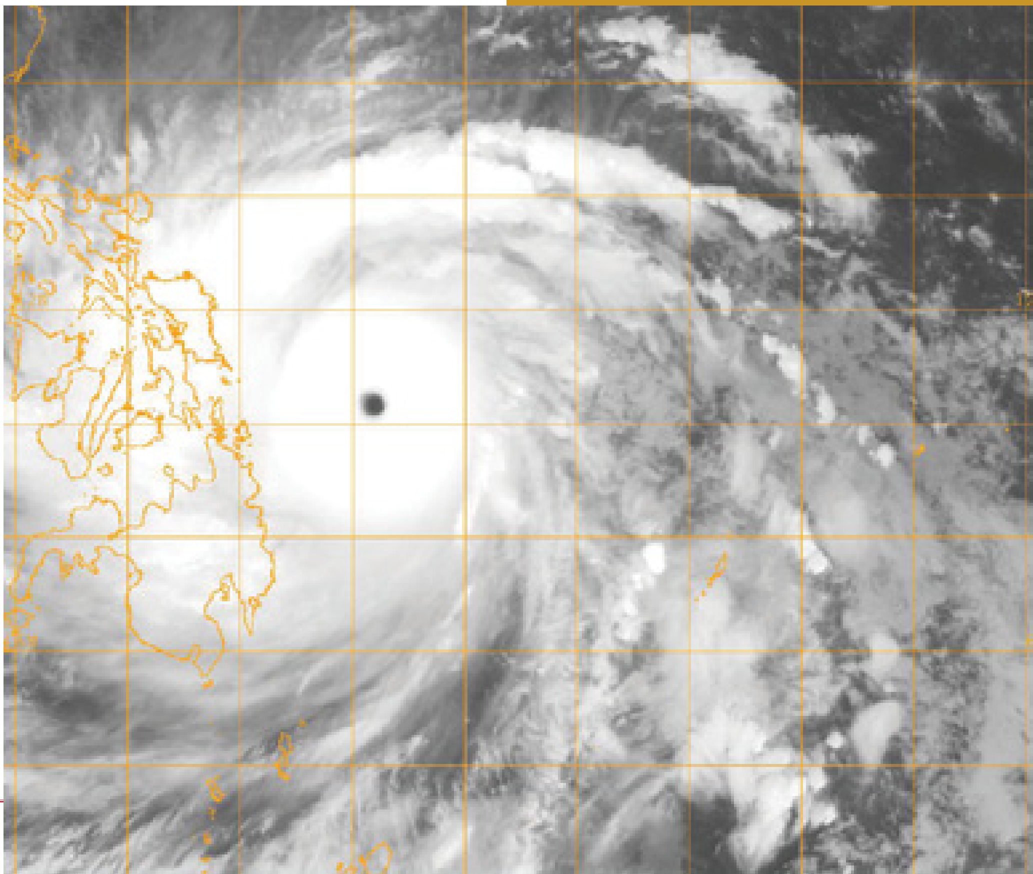
Disaster Response: A Not-So-Sexy Kind of Job

LCDR Gilbert G. Villareal, Philippine Navy

When Typhoon Yolanda hit the Philippines in early November 2013,[1] I was a staff officer with the Philippine Fleet (Division category), while at the same time serving as the deputy commander of a SEAL-type unit of the Naval Special Operations Group (NAVSOG). It was my last week on these two assignments before I was to pursue a more traditional career path as a naval officer in the Philippine Navy. My experience dealing with the aftermath of Yolanda taught me some important lessons that I believe could be vital for commanders and any military personnel assigned to Humanitarian Assistance and Disaster Response (HADR) in an area devastated by natural calamity or war. I am writing through the lens of my experience as a staff officer of a battle group, an assessment officer with SOF experience, and a contingent officer on the ground conducting HADR. Many SOF personnel consider HADR to be an unsexy kind of deployment: a time-consuming aspect of "soft power" projection suitable for regular soldiers and reserve forces or in the United States, the National Guard. There's supposedly no action in the HADR theater, nothing special or even significant about this kind of mission. After all, the thinking seems to go, if the Navy and other conventional forces can do this kind of trivial military operation, why should the SOF be expected to respond?

THE TEAM LEADER WAS IN TEARS AS HE DESCRIBED THE ENDURING DRAMA.

When dealing with both adversaries and crisis management, however, the SOF are very capable and can respond to any situation. As Yolanda struck the Philippines, the entire Armed Forces of the Philippines (AFP) was on alert. As a member of the battle staff, I was assigned to monitor all events concerning naval units, especially those naval assets and personnel that were dispatched to the areas devastated by the typhoon. I was also tasked with a collateral duty, to monitor and approve the deployment of all SEALs assigned to NAVSOG units across the Philippines, whether they were in training, already deployed, or otherwise tasked. As the typhoon ravaged the country, particularly Samar province, we all monitored the effects, trying to determine what we could do and what we needed to deploy to mitigate the damage and help the survivors. In my dual role, I informed my SEAL commander that the majority of our men from each area command of the AFP—Luzon, Visayas,



ONLY 10 POLICEMEN AND 12 SOLDIERS SURVIVED THE STORM SURGE.

and Mindanao, including a company from our headquarters sized for quick response—were being pulled out of training and other deployments to complement the ongoing HADR mission.

Adversary from the Field

After that first day spent monitoring the situation, I tried to contact the team leader of a squad of SEALs assigned to a navy command post in the city of Tacloban, the capital of Samar province. I could not reach him by phone or military radio. After two days, we finally made contact through a team from NAVSOG that augmented the Naval Task Force. This team immediately directed a contingent of Naval Logistics Support Vessels, which were loaded with personnel and relief goods to support the victims of Yolanda, to the stricken city.

When I finally spoke to him, the team leader was in tears as he described the enduring drama he and his men had experienced. He said that the four members of his team were accounted for; they had survived the storm surge and saved all the naval personnel in the command post. But they regretted not being able to save others, especially the 56 policemen and 23 army personnel who were also stationed inside the command post compound at the time. Only 10 policemen and 12 soldiers survived the storm surge.[2]

How did the four SEALs manage to survive such tragedy? As the team leader talked to me, one thing he kept mentioning was the training he had received as a SEAL. Everyone at his post was shocked at how fast the water rose, he told me; all of the people in the compound were shouting, but no one was moving or initiating any action. Although his men were good swimmers, he said, they knew

that even they could not survive among all the debris being carried by the water, and seconds count in such a situation. The four SEALs punched a hole through the wooden roof of their barracks. Two men took ropes from the laundry lines, tied these lines to coconut trees, and brought them down through the hole in the roof. At this time, the team leader told me, the water was six to seven feet high, and they couldn't see anything because of the rain and the wind. They kept shouting to the others in the compound, but the only ones who responded were the navy personnel in their barracks. That's what the officer kept telling me: the navy men were the only ones the SEALs saved. The men held onto the ropes as the water level quickly increased to 10 feet, with strong wind and rain and seawater flowing everywhere. The men managed to get up onto the roof and hold on to each other until the flood subsided several hours later. The majority of the people inside the compound, including those in the police and army barracks, were drowned. According to the team leader, they were all taken by surprise and were swept away by the flood. As the water rose, he and his men thanked God that they were saved, but he was also proud and thankful that his SOF skills helped him and his men survive, and pushed them to save others who were at the threshold of death. He felt that his training automatically came back to him when he needed it.

I WAS AMAZED TO SEE HOW FAST SOF UNITS REACTED.

When the water went down, the men and everything around them were left soaking. The sight of all the dead bodies in the compound—hanging from electric poles and trees, or lying in the grass and strewn about—left most of the survivors traumatized, except, as the SEAL leader asserted, his team. He was again in tears as he talked to me. The first thing he did after the waters subsided was consolidate his team and the survivors inside the compound. He then divided them into five groups: one group to search for and retrieve any survivors

Distribution of supplies to people in the coastal barangays affected by the typhoon in Samar Province, Philippines

Picture of LC 551 (Philippine Navy Logistic Ship)—It carried more or less 3,000 people from Samar to Cebu immediately after Typhoon Yolanda. It also served as the initial command and control platform of the Armed Forces for the Philippines immediately after the typhoon. It helped bring supplies and relief goods to the victims of Yolanda.

inside the compound; the second group to gather supplies, especially food and water and any communications equipment; the third group to assist the first group in looking for survivors and also to gather the bodies of the victims; the fourth group to start fixing the compound's structures, especially the roofs and the barracks; and the fifth group to search for the nearest coordinating office or government command post that still had electricity and communications. This turned out to be over 10 kilometers away in Tacloban City and took more than a day for the team to reach.

This was the first day after Yolanda made landfall on Samar province. The government, including me, a staff officer of the Philippine Fleet, had no means of communication in the crucial first 24 hours after the devastation. I can't say whether bureaucracy and politics played any role at that time, but the management of the crisis had some shortcomings. Government officials did not anticipate how great the damage would be.

Regarding my other set of duties, all NAVSOG personnel in the impact area and in the headquarters were alerted before Yolanda hit, were accounted for once the storm subsided, and by the second day were deployed all over the Philippines, with the majority of them going to Samar province. This is an example of how quickly and easily SOF units can be deployed and delivered, and how SOF can adjust to any given mission.

While I was monitoring the deployment of the NAVSOG personnel, I also checked some of the AFP units that were augmenting the contingent in devastated areas of the Philippines. I was amazed to see how fast SOF units like the NAVSOG, the Army Rangers, the Army Special Forces, and the Air Force Special Operation Wing reacted. They were the ones who immediately responded and were already prepared to depart by the time I contacted them. On that first day, they were waiting either in the airport for C-130 transports or on the pier for ships to take them to their areas of responsibility, such as Tacloban City and Samar province. This was the situation during those crucial first three days: some AFP units, even the reserves, were still waiting for instructions. Some were delayed because they had to wait for the relief goods and supplies intended for the victims. But some were still waiting for decisions from higher command. AFP camps, such as the General Headquarters and Villamor Air Base, were quickly flocked by volunteers and overwhelmed with contributions of goods, but there were administrative problems with the relief efforts, such as determining who would be in charge. Without going into further detail on these problems, the purpose of this narrative is to look at how SOF units can be effectively deployed in crises for HADR, which the United States and some other nations call a Military Operation Other Than War,[3] and the projection of "soft power" as a means of humanitarian assistance.[4] HADR is an important role for any military and requires military personnel to be capable of a rapid response to any given calamity, whether natural or manmade. The more quickly and efficiently they can react, the more effective the armed forces of a nation will be in any crisis.

THE DEVASTATION CREATED BY YOLANDA LOOKED LIKE A ZOMBIE LAND.

Boots on the Ground

After a week of monitoring the storm's aftermath as a staff officer in the Philippine Fleet, I was relieved from my desk duties and assigned to go to Samar as a fleet assessment and coordinating officer. I was again tasked with dual functions: I would be an assessment officer for post-disaster damage and a liaison officer to coordinate certain requirements for the naval assets and personnel located in Samar. Following a week's leave, I reported to Tacloban City. While I was in Samar, I both heard and witnessed for myself story after story of survival, heroism, professionalism, cooperation, courage, and resiliency of people pulling their lives back together after the storm. Comparing it to some of my previous HADR operations, I have to say that the aftermath of Typhoon Yolanda was the worst situation I have ever encountered in my life. The heavily damaged no-man's land that I had seen in 2000 during the All-out War against insurgents in the southern Philippines was no match for the devastation created by Yolanda, which looked like a combination of a no-man's land and a zombie land. All the dramas of life had unfolded—stories of ordinary and extraordinary human behavior and of instinctive survival were conveyed not only by the news media but by the different people I talked with and interviewed. There were no rich and poor people, privileged people, or people with high political status in this disaster. Everyone upon whom the wrath of nature fell was equally a victim.

When I arrived in the Tacloban area, the authorities' focus was still on ensuring stability, but the local government and its provincial disaster management team (PDMT) were already in close coordination with international organizations, including the United Nations and the US Joint Special Operations Task Force-Philippines (JSOTF-P), as well as the governments of Israel, Canada, Japan, China, South Korea, and others. The PDMT comprised contingents of the AFP, the Philippine National Police, other concerned agencies, and various volunteers. I was part of the navy contingent of the AFP. A majority of the contingents from the different AFP and reserve units were tasked with augmenting the army's

8th Infantry Division, which had to take the lead in organizing and spearheading all of the AFP contingents that arrived for disaster response, even though most of its personnel were missing. Infrastructure from the brigade headquarters down to the company outpost was critically damaged by the typhoon. I was told that most of its personnel were among the casualties of the storm. As I learned this, some questions came up for me, which I noted in my logbook: If your unit or even you yourself are prepared to respond to a natural or manmade disaster but you become the victim of such a disaster, what will you do? What can others do? Do we have contingency plans for such a situation?

This thought struck me with fear, but then I remembered the SEAL team leader who rescued the navy personnel during the typhoon. It came to my mind that instinct and skills are the essential requirements to keep oneself and one's family safe in every situation that might arise. Disaster survival skills should be taught so that they become instinctive for everyone, especially to our families and fellow military personnel.

A Model for Disaster Response

During the week that I stayed in the Tacloban area, I saw how countries could cooperate with one another to help the Philippines, especially in devastated areas like Samar province. It was so enlightening—and somehow amazing to me—to witness how countries could coordinate in times of disaster and to see the positive response of all these countries' representatives, whether military or government officials. They all respected the host country's officials, down to the provincial and local governments. Again, question after question came to my mind: Could this also be a model for insurgency and terrorist incidents? In the event of insurgency or terrorist activity, should the host nation remain in control? Will decision making in large-scale emergencies come down to the local government officials in the affected area? If this protocol could work in a disaster-stricken nation, it seemed like it should also work for other problems.

US disaster response to other nations, such as the post-typhoon Philippines, takes a comprehensive approach. Through initiative and the assets that were already in place, the United States was one of the first responders in the aftermath of Typhoon Yolanda. The JSOTF-P dispatched personnel and air assets for immediate assistance. The Disaster Assistance Response Team, the US Agency for International Development, and the Office of US Foreign Disaster Assistance quickly followed, assessing the situation and trying to fill all essential requirements in the worst-hit areas. I experienced firsthand how these US teams managed a rapid-response situation, including some innovation and adjustment that were needed in the post-typhoon environment. At the same time, there were lots of responders in the area who were eager to do their jobs. They respected the host country representatives, especially the local government officials who were in control in the disaster area—even the AFP was not the leading agency at that time. In the report I wrote for my commanders, I suggested that the disaster response I witnessed could serve both as a model for doctrine development and the basis for best practices in a HADR operation, especially in a country like the Philippines that is prone to typhoons, earthquakes, and other types of natural and manmade disasters.

The Vital Role of the Special Operations Forces

When I thought about the intervention methods and the deployment of responders during my time in Tacloban, it occurred to me to include in my report a discussion of the ways in which SOF could play a vital role in the HADR mission. But I have my own reservations about presenting this idea. If disaster relief became a formal role for our SEALs, some would perceive it as a role for lesser men, not for SOF, who are trained to be elite warriors and killers. Most of my fellow SOF warriors would hate me for making them take on a "not sexy" job like disaster response.[5] But I truly believe that SOF can make the difference in saving hundreds or even thousands of lives if they are deployed not only as trained first-responders but also as the first people sent into disaster-stricken areas. Humanitarian assistance and disaster response may not seem sexy, especially for specialized soldiers who take pride in their killer instincts, but they can make a big difference by giving people the precious gifts of life and hope.[6] In my career, I have participated as a responder in three major disasters: flash floods, a sunken ship, and the typhoon. In each instance, my capacity and my capability were challenged to the utmost limit. The work was rewarding and fulfilling, even though I have also had experience with combat missions and fighting as a SEAL operator. The HADR mission is always on my bucket list of priorities—it keeps me going and meets my professional goal of helping other people in times when they need help the most. But what also keeps me thinking about the deployment of SOF units for HADR is not just the experiences I've had, but also the fact that I can see how advantageous it would be to develop SOF as highly professional specialized response units.

There are five factors that I believe make SOF ideal as immediate responders in a disaster.

1. SOF are rapidly deployable compared to their conventional counterparts. SOF units can be immediately inserted into any disaster-stricken area and make an initial assessment of conditions before the conventional support or other units are deployed to the area. In another typhoon scenario, for example, SEALs could conduct an initial damage assessment of the piers and coastal infrastructure, conduct a hydro survey, and fulfill other essential requirements for ships carrying food, medicines, shelters, and other relief goods. Lack of information about the safety of some of the piers and wharves damaged by Typhoon Yolanda was a problem for responders. Some ships, for instance, hesitated to dock at some of the piers in Samar province, which meant their cargo did not reach the people who needed it.

Ranger and SOF units could also clear vital roads blocked by the calamity so that trucks carrying troops and goods could reach the affected areas. Paratroopers could assess the airport and airstrips to find alternate landing zones as needed after any calamity. It took two or three days after Yolanda passed to clear the Tacloban airport because there were no trained personnel on the ground. If paratroopers had been dropped immediately after the typhoon struck the province, airlift and supplies could have been quickly provided to the victims, thereby saving hundreds more lives. The Civil Affairs Group could conduct morale briefings, give people the information they need to survive, and provide support and comfort in a post-disaster situation.

2. SOF are highly specialized and have the skills to do initial assessments before the main effort of delivering support and logistics begins. Most SOF personnel have skills in multiple languages and could serve as communicators, not only to higher command but also to the local people. SOF personnel could also identify and set up the best tactical command post or command and control area.
3. SOF personnel are the most disciplined members of the military. They have a high workload capacity and a high sense of tolerance and professionalism. Most of the work that follows the initial assessment after a disaster is about helping people and saving lives. Minute by minute, responders hear people screaming for help and begging for rescue. Some soldiers have difficulty in this situation, especially when dead bodies are scattered all around. A SOF operator can better tolerate these conditions and fulfill the task of prioritizing who needs to be saved.
4. A SOF officer is the best initial ground commander for HADR. If the disaster area has no initial command or authority left functioning, a SOF officer is the most fit to organize crisis management. His training and deployment—including leadership training—have prepared him to respond to this kind of management situation. When a Philippine SOF commander was tasked to head the initial contingent of the AFP after Typhoon Yolanda, he performed his duties quickly and efficiently before transferring them to the local government and the army division. His performance made a difference, and he was even praised by the US president for how well he performed during that crucial time of chaos and uncertainty.
5. Information operations, including Civil Affairs and psychological warfare, is another important aspect of special operations. This function is vital for all responders and units, international and local, acting in support of a HADR operation. A fellow student at the US Naval Postgraduate School proposed building a website that would cater to responders and units conducting and supporting HADR operations, with information on safe navigational routes and cleared road networks; updates on casualties and medevacs; airport clearance; important relief supplies; a directory of victims and families looking for lost members; and so on, to help coordinate all the international units and relief organizations, including military responders.

These are the lessons I have learned as a SOF disaster responder. My experience can serve as a case study for how SOF can be deployed effectively in what may be a "not-so-sexy" job, but one that could positively affect hundreds of lives by giving disaster victims hope and helping them survive manmade and natural disasters like Super Typhoon Yolanda in the Philippines. ❖

ABOUT THE AUTHOR

LCDR Gilbert Villareal is a SOF officer in the Philippine Navy.

NOTES

[1] Typhoon Yolanda (known internationally as Typhoon Haiyan), a Category 5 super typhoon, is estimated to have been the most powerful storm to reach land in recorded history. The storm took three days to pass over the Philippines but was at its height on 8 November 2013.

[2] Much of the destruction from the typhoon came from the enormous waves of seawater that the storm pushed onto low-lying coastal areas. These storm surges were estimated to reach as high as seven meters in some places. Reynaldo Santos, Jr., "Powerful Yolanda Hits Eastern Visayas," Rappler, updated 9 November 2013: http://www.rappler.com/nation/special-coverage/weather-alert/43183-20131108-yolanda-am-update

[3] James Callard and Peter Faber, "An Emerging Synthesis for a New Way of War: Combination Warfare and Future Innovation," *Georgetown Journal of International Affairs* 3, no. 1 (Winter/Spring 2002): 61–68.

[4] Joseph S. Nye, Jr., *The Future of Power* (New York: United States Public Affairs, 2011), 47.

[5] Doug Borer, "HADR: Not a Sexy Job for SOF" (lecture, Naval Postgraduate School, Monterey, Calif., April 2015).

[6] Ian Rice, "History of Specops [*sic*]" (lecture, Naval Postgraduate School, Monterey, Calif., 7 April 2015).

The Phantom Raid

Air CDR (Ret.) Jamal Hussain, Pakistani Air Force

Note: This essay was written in September 2011, four months after the raid that killed Osama bin Laden.

The computerized log register at the Air House shows that at 0207 local time on 2 May 2011, an urgent telephone call for the air chief came in.[1] When the air chief came on the line, the army chief, his land counterpart, informed him of confirmed reports of aerial activity, weapons fire, and a helicopter crash around the northeast garrison town of Abbottabad. "Is there any flying activity from the PAF [Pakistani Air Force]?" the army chief inquired. The air chief replied in the negative. The only reason PAF helicopters would be flying at that late hour of the night was if they were on a search-and-rescue mission to find a PAF aircraft reported to have crashed in the area during night flying. The air chief would have been informed about a downed aircraft, so that was not likely to be the reason for the activity. The army chief confirmed that, besides the suspicion that the air intrusion may have originated from the western border on a mission that was not yet clear and appeared to be the handiwork of the Americans, no other details were available at that time.

Unsettled by this alarming news, the air chief wondered what could be the objective of such a brazen raid. As far as his knowledge went, Abbottabad had nothing of strategic value to defend, or the PAF would have deployed point-defense radar and other air defense systems to protect it against air or land attacks. Maybe the Indians actually believed their own oft-repeated mantra about Kashmiri terrorist training camps at Manshera, adjacent to Abbottabad, and had undertaken a foolhardy venture. Or perhaps the Americans, under the misperception that some of Pakistan's strategic assets were located in Abbottabad, had conducted an airborne assault to seize them. That notion made little sense, however, because if the United States ever did mount an operation to take over or destroy Pakistan's nuclear weapons, it would conduct a mass multiple-point raid rather than a stealthy solitary one. Whatever might be the motive of the aggressor, however, an immediate response from the PAF was warranted.

AT 0207 LOCAL TIME ON 2 MAY 2011, AN URGENT TELEPHONE CALL FOR THE AIR CHIEF CAME IN.

While still speculating about the motive and the nature of the apparent aerial attack, around 0210 the air chief issued orders to his air defense commander to scramble a pair of F-16 fighters from the nearest base. Their instructions were to go over Abbottabad and look for any flying intruders. If any were detected, the fighters had clear orders to engage and shoot the intruders down, regardless of their country of origin. This was really a very bold and courageous decision, because by then it was becoming increasingly likely that the United States, rather than India, was the aggressor. To protect the nation's honor and assert its sovereignty, the PAF was prepared and ready to challenge and engage a far superior adversary that could boast an annual budget of US$171 billion, compared to the relatively meager annual budget for the PAF of about US$1.01 billion.[2]

In addition to getting regular updates on the progress of the scrambled jets, the air chief gave instructions for the immediate enhancement of the entire country's air defense alert status and directed the duty staff to report to him on the status of all air defense radars. He wanted to know whether any radars had picked up intruders from either side of the border or had experienced any jamming.

As the hours passed, news started to trickle in that confirmed an aerial intrusion from the west, apparently by US forces, that targeted a solitary compound within a kilometer of the Pakistani Army's Military Academy at Kakul. The goal of the mission appeared to be the capture or elimination of a key al Qaeda leader whom the Americans suspected was holed up in the compound. The scrambled fighters, meanwhile, had reported from over the site, and despite an extensive search, could not locate any aerial activity in or around the locale. As was later learned, the helicopters that had led the air assault had completed their operations and exited the area, and were returning to their home bases in Afghanistan by the time the Pakistan F-16s had arrived on the scene.

At around 0835 Pakistan Standard Time, US President Barack Obama appeared on television and triumphantly announced that, through a bold heliborne operation inside Pakistani territory, "a small team of Americans" had killed the number-one US enemy, Osama bin Laden. "Justice has been done," the president said.[3]

This news made headlines in all major international and local news sources by the following morning and dominated the news over the following days; one such headline cryptically stated, "Obama Gets Osama."[4]

"OBAMA GETS OSAMA."

The fact that four foreign helicopters were able to penetrate more than 100 nautical miles inside Pakistani airspace without being detected by the country's air defense network and remain there for nearly two hours (approximately 80 minutes for the ingress and exit phases and 40 minutes over the site) was of serious concern and warranted a major investigation. Later in that same morning, the air chief convened a very high-level team headed by a three-star air marshal to conduct a thorough probe into the incident and submit a report. Because all official activities at the Air House and at all the air defense units, including the status of the radars and other systems, are electronically recorded, the investigation would be able to accurately determine the status of the sensors during the critical period and whether any target was picked up or a unit experienced jamming.

The investigation report was completed within three weeks and scrutinized at the highest level at Air Headquarters. Its salient findings were (1) all PAF radars that were deployed during the period under scrutiny were serviceable and operational; (2) no targets were picked up by any of the deployed sensors, nor did any sensors experience jamming; and (3) there were no system failures or any slackness on the part of the air defense operators on duty.[5]

And yet four helicopters were able to cross the Afghan-Pakistani border undetected by a fairly sophisticated air defense network, penetrate over 100 nautical miles into Pakistan, operate for more than half an hour, and return to Afghan airspace before anyone in Pakistan's security forces knew they were there. The report highlighted system limitations and technological deficiencies against a sophisticated aggressor, along with inadequate low-level radar coverage on the western border, as possible explanations for the undetected raid.

To understand how this incident could have happened without some degree of incompetency or outright failure of the air defense network and its operators, it helps to have some basic knowledge of the nation's air defense network, its strengths, and its limitations.

The outermost layer in a nation's air defense system is the detection of incoming air raids. Ground-based radars are the primary means by which most countries with air defenses maintain a constant vigil against the intrusion of hostile air elements. Airborne radars like the airborne early warning and control platforms do supplement a country's air defense ground environment, but they are expensive alternatives and are used primarily to supplement certain limitations of ground-based radars. These systems are very useful during crises and wars, but to keep them operational on a 24/7 basis during peacetime is prohibitively expensive. Even the United States cannot afford such a luxury.

Ground-based radars come in two distinct versions: high-level and low-level. High-level radar is optimized to pick up high-flying targets and, depending on the altitude of the target and the power of the radar, can easily detect targets up to 250 miles away. Low-level radars, which have the ability to reduce the amount of "ground clutter" (i.e., signals reflected from the ground) they pick up, are used to detect low-flying targets. Because of the earth's curvature, the maximum range at which a target flying at 250 feet or less above ground level can be detected is generally about 25 miles. To overcome this limitation and the interference of natural and manmade obstacles, such as hills and buildings, a series or network of radars is needed to illuminate a particular area. Figure 1 shows a schematic diagram to illustrate the principle.

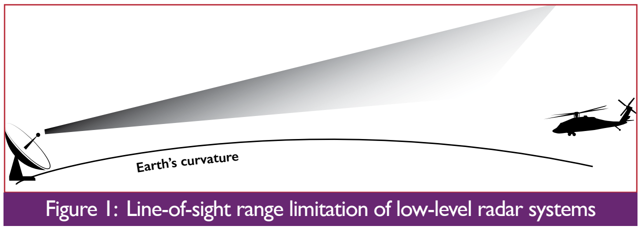


Figure 1: Line-of-sight range limitation of low-level radar systems

Pakistan has to monitor its airspace for both high- and low-level air incursions from its eastern, western, and southern borders. Given that high-level radars have a range of over 250 miles and a very wide cone of coverage, six to seven such units operating on a 24/7 basis can adequately cover the entire airspace of the country. Low-level monitoring of the borders, in contrast, presents a significant challenge. Because low-level radars have limited range and a much smaller cone of illumination, these units must be deployed linearly and in depth to give enough early warning of low-flying intruders to the air defense units. To cover the entire length of the country's borders would require more than 250 such radars to be deployed. Moreover, because of their specialization, low-level radar units have a limited lifespan and if operated on a 24/7 basis, will have to be overhauled at regular intervals. In less than a decade, they will have outlived their usefulness and must be replaced. Continuous low-level radar coverage of the entire border of Pakistan is, therefore, not possible. It may be remembered that even the United States, with an annual defense budget of over $700 billion, cannot afford the luxury of perfect radar coverage along its southern border with Mexico, which time and again is breached by drug smugglers flying low in small aircraft to drop their deadly merchandise. How, then, does the PAF attempt to overcome this severe limitation?

The procurement and operational deployment of the PAF's air defense radar network are governed by the threat perception, an official posture that is formalized by the service in conjunction with the relevant authorities at the highest level. In the current scenario, the PAF has complete high- and low-level radar coverage along its eastern border with India. During the Soviet invasion of Afghanistan in the 1980s, much of the western border, especially the northern border with Afghanistan, was provided with round-the-clock low- and high-level coverage, and the Air Force paid a high price in terms of the wear and tear on its equipment due to the constant vigil. After the Soviet withdrawal in 1988, the aerial threat from the west was downgraded. As long as coalition forces ruled the air "waves" in Afghanistan and Pakistan remained an ally in their war against the Taliban and al Qaeda insurgents, the PAF envisaged no serious aerial threat from that quarter. Currently, although a complete high-level umbrella covers the western border, low-level cover is limited. Only those installations in locations that have been identified as vital have point defense radars and ground-to-air defenses. There are enough gaps in low-level coverage that an adversary could penetrate Pakistan's airspace from the west and avoid detection.

AS LONG AS COALITION FORCES RULED THE AIR "WAVES" IN AFGHANISTAN, THE PAF ENVISAGED NO SERIOUS AERIAL THREAT FROM THAT QUARTER.

The success of US Operation Trident Spear, as the bin Laden operation was called, was vital for the United States in general and the Obama administration in particular. The planners left no stone unturned in their efforts to ensure that the raid achieved its objective, utilizing every operational, electronic, and avionic option available to them. To avoid detection, they carefully mapped the footprint of some of the low-level radars en route and chose a path beyond the array's surveillance ranges. In addition, the aircraft flew very fast at very low altitude and through valleys wherever possible, thus further reducing the chances of detection. Furthermore, the two Blackhawk helicopters that carried out the actual mission had been specially modified to incorporate stealth technology. Special paints and modified design features made these platforms virtually invisible to the current generation of radars. Not satisfied with these measures, the planners made sure the helicopters were equipped with radar warning receivers and jammers. Should Pakistani radars have illuminated the choppers despite their stealth capability, the US pilots would have gotten a warning through their radar warning receiver and been able to resort to jamming. From an operational viewpoint, jamming is a last resort to be used only when it is confirmed that the opponent's radar system has detected the intrusion. In the event, the raid went undetected, and no jamming was required.

The US planners had one final ace up their sleeves. While the operation was in progress, they were continuously monitoring Pakistan's communications for any sign of reaction. If Pakistan had reacted in time by scrambling fighters, Admiral Mike Mullen, the chairman of the Joint Chiefs of Staff, was standing by to ring up his counterpart and inform him that it was an American raid and that Pakistan should not interfere. If Pakistan decided to engage the intruding helicopters anyway, the United States would free its own fighters, which were already patrolling the Afghanistan-Pakistan border armed with the latest beyond-visual-range missiles. The PAF fighters would then be challenged by a force of significant numerical and technological superiority. Very few episodes in the history of aviation can match the meticulous planning, deployment of cutting-edge technology, and professional execution that characterized the helicopter-led assault on the Abbottabad compound, deep in Pakistani territory.

THE CHAIRMAN OF THE JOINT CHIEFS WAS STANDING BY TO RING UP HIS COUNTERPART IN PAKISTAN.

Could the current air defense network of Pakistan have done any better against such a sophisticated operation? Perhaps not. What needs to be done to prevent another such intrusion? Given the severe imbalance between the capabilities of the US Air Force and the PAF, the answer probably lies in negotiations and diplomacy. If negotiations should fail and it is called upon to defend the nation, the PAF is ready to take on any adversary, even the US Air Force, and will fight to the bitter end, regardless of the cost. ❖

ABOUT THE AUTHOR

Air CDR Jamal Hussain (Ret.) is the director of Pakistan's Center for Air Power Studies.

NOTES

[1] The Air House is the official residence of the chief of staff of the Pakistani Air Force.

[2] Figures are approximate. For details of the US Air Force budget estimate for Fiscal Year 2010, see Department of the Air Force, SAF/FMB, *United States Air Force: FY 2010 Budget Overview* (Washington, D.C.: Dept. of the Air Force, May 2009): http://www.saffm.hq.af.mil/shared/media/document/AFD-090508-028.pdf . For the Pakistani Air Force's figures, see "Defence Budget for FY-2012–2013 Announced," *Pakistan Military Review* (blog), n.d.: http://pakmr.blogspot.com/2012/06/defence-budget-for-fy-2012-2013.html

[3] For a transcript and video of President Barack Obama's remarks announcing the death of Osama bin Laden, see Macon Phillips, "Osama Bin Laden Dead," *What's Happening* (blog), 2 May 2011: https://www.whitehouse.gov/blog/2011/05/02/osama-bin-laden-dead

[4] Will Durst, "Obama Gets Osama," *The Blog* (blog), *Huffington Post*, 6 May 2011: http://www.huffingtonpost.com/will-durst/obama-gets-osama_b_858762.html

[5] The low-level radars deployed on the northwestern border were of vintage German origin, dating back to 1978. US aircraft would have the electronic countermeasure capability to plot and jam these radars with relative ease. Pakistan's radar inventory currently also includes units from several nations, including the United States and Germany. The performance of all radars is recorded and preserved in cassettes and tapes, which allowed the investigators to determine whether the protocol for radar deployment (determined by the current security status) was followed, and whether the ones that were operating in the border sector in question experienced any jamming. The investigation's recommendations included a revision of the deployment protocol.

Seymour Hersh Reignites the Bin Laden Raid Controversy

Air CDR (Ret.) Jamal Hussain, Pakistani Air Force

The news that broke in Pakistan on the morning of 2 May 2011, that a US special operations team had conducted a daring night raid inside Pakistan to eliminate terrorist Osama bin Laden, left the Pakistani public in a state of shock and utter disbelief. At first, a significant majority in the country refused to accept that bin Laden could have sought refuge—or, possibly, been given shelter by Pakistan's Inter-Services Intelligence (ISI)—at a location scarcely more than a stone's throw from the Army's prestigious military academy at Kakul. As the narrative unfolded over time, however, the truth about the presence of bin Laden in Abbottabad and his elimination by a US SOF team finally dawned on a deeply humiliated nation, but most people remained highly skeptical about the official American version of the raid.

MOST PEOPLE REMAINED HIGHLY SKEPTICAL ABOUT THE OFFICIAL AMERICAN VERSION OF THE RAID.

An exposé by investigative journalist Seymour Hersh, "The Killing of Osama bin Laden," published in the May 2015 *London Review of Books*, categorically rejected the American claim that "the mission was an all-American affair, and that the senior generals of Pakistan's army and Inter-Services Intelligence (ISI) were not told of the raid in advance."[1] A sizable section of the Pakistani public agreed with Hersh's assertion, igniting a fresh debate over the raid within Pakistan that had the skeptics gloating, "I told you so." While Hersh's reputation for professional integrity makes it hard to dismiss this latest piece on the bin Laden raid, at the same time, his past acclaim should not guarantee automatic acceptance of his viewpoint.

Before embarking on a critical examination of the bin Laden raid narrative as pieced together by Hersh, it would help to briefly assess one of the assumptions on which he apparently bases his version of events. Hersh claims that the helicopters carrying the SOF operators could have ingressed deep (about 100 nautical miles) inside Pakistani airspace undetected only if someone high in Pakistan's military command were complicit with the raiders. If this conjecture is faulty, as I believe it is, then Hersh's entire analysis is built on a dubious foundation.

On the night of 1 May 2011, in the border sector where the raiders crossed into Pakistan's airspace, there were only a few low-level radars deployed between Peshawar and Abbottabad, whose primary function was to facilitate and monitor local Pakistan Air Force (PAF) activity. Because friendly NATO and International Security Assistance Force airpower operating across the border in Afghanistan had full control of the airspace, no serious threat was envisaged from the western front—hence, comprehensive low-level radar coverage of the western front was not considered necessary.[2]

The PAF does have airborne sensors in the form of airborne early warning and control (AEWC) platforms, which can greatly enhance low-level detection capability when deployed in a given sector. There were no AEWC aircraft in the air when the raid materialized on that fateful night, however, because these very expensive systems are meant for use primarily during actual war or in military

General Ashfaq Parvez Kayani and Lieutenant General Ahmed Shuja Pasha

exercises. With the aid of the electronic surveillance and electronic countermeasure capabilities that it possessed, the US Air Force could therefore easily have plotted the range of the handful of low-level radars deployed in the sector and selected a route well beyond their detection capability. Using a combination of stealth technology, nap-of-the-earth flying (terrain masking, flying under the radar), and a route plotted to keep them in the shadow of the hills, flying in undetected was, to use a cliché, a piece of cake for the raiders. It is believed that in addition to all of these precautions, the flight team had a contingency plan to spoof and jam the PAF radars if any units still managed to pick up the aircraft.[3]

Hersh's assumption that the PAF had the wherewithal to guarantee detection of four ultra-low flying helicopters, two of which were masked with stealth technology, even over such a distance, displays his naïveté about the workings of air defense systems. In any investigation, when the investigator accepts certain assumptions as truth, there is a subsequent tendency to cherry-pick only that evidence that supports the initial assumptions, even if it comes from sources that are normally considered unreliable and unacceptable. What follows is a chronological sequence of key events before, during, and after the actual raid, as portrayed by Hersh.

1. Bin Laden's presence in Pakistan was disclosed by a "walk-in"—a retired senior ISI officer who came unbidden to the US embassy in Islamabad in August 2010. The officer told officials there that bin Laden was being kept in protective custody by the ISI at an isolated compound in Abbottabad.
2. General Ashfaq Parvez Kayani, the powerful chief of the army staff, and Lieutenant General Ahmed Shuja Pasha, the head of the ISI, initially denied any knowledge of bin Laden's presence in the country but eventually had to concede that he was in their custody. They were persuaded to cooperate with the CIA-conceived plan to kill or capture bin Laden after negotiating for some quids pro quo, particularly regarding military aid.
3. Kayani and Pasha were kept in the loop about the air raid and were made responsible for ensuring that the PAF stayed out of the way.[4] They were also told in no uncertain terms that any efforts to relocate bin Laden from his Abbottabad hideout would have serious consequences not only for the Pakistani generals but for their country as well. For their part, Kayani and Pasha insisted that "you can't have a big strike force. You have to come in lean and mean. And you have to kill him, or there is no deal."[5]
4. The two sides jointly agreed that the United States would wait a week before formally announcing that bin Laden had been killed by a drone strike in the hilly region of the Pakistan-Afghanistan border, a story that Pakistan would subsequently confirm. The crash of one of the Blackhawks as it attempted to drop team members onto the Abbottabad compound's rooftop, however, made it impossible to keep the raid a secret. Once it was clear that the mission had succeeded, a backroom argument began in the White House: "Should Obama stand by the agreement with Kayani and Pasha and pretend a week or so later that bin Laden had been killed in a drone attack in the mountains, or should he go public immediately? The downed helicopter made it easy for Obama's

"YOU HAVE TO COME IN LEAN AND MEAN. AND YOU HAVE TO KILL HIM."

political advisers to urge the latter plan. … Obama had to 'get out in front of the story' before someone in the Pentagon did."[6]

5. Much to the dismay of US Secretary of Defense Robert Gates, Obama acted on the advice of his political team, taking all the credit for the mission with only a vague mention of any involvement by the Pakistani government: "It's important to note that our counterterrorism cooperation with Pakistan helped lead us to bin Laden and the compound where he was hiding."[7] Kayani and Pasha had little choice but to accept the official US version, refuting any involvement with the US plan or prior knowledge of bin Laden's presence in the country. The appearance of incompetency was a lesser evil for them than complicity.
6. Hersh maintains that the sea burial of bin Laden's remains cannot be verified and, according to his unnamed source, never took place. In his telling, the remains were either strewn over the Hindu Kush mountains or interred in some undisclosed location.

THE APPEARANCE OF INCOMPETENCY WAS A LESSER EVIL THAN COMPLICITY.

Each of these points presents some problems. On the subject of the ISI walk-in postulated by Hersh, although such a possibility cannot be ruled out, Hersh fails to provide any credible source to support this story beyond the one unnamed former US intelligence official who is the sole source for almost the entire article. The US administration provided a slightly different version of events. In the initial press briefing after the raid, a senior intelligence official confirmed, in guarded terms, that Pakistan had provided crucial information that intensified the CIA's focus on the Abbottabad compound. "'The Pakistanis did not know of our interest in the compound,' said the official, 'but they did provide

President Obama and other officials in the "Situation Room" watching live feed from drones operating over the bin Laden complex us information that helped us develop a clearer focus on this compound over time. … [T]hey provided us information attached to [the compound] to help us complete the robust intelligence case that … eventually carried the day.'"[8] One reporter's version of the story claimed that "the ISI had given the CIA a mobile phone number without knowing its significance and that US surveillance of that number led eventually" to an al Qaeda courier and finally to bin Laden.[9] This was apparently the extent of the cooperation to which Obama had briefly referred in his triumphant announcement.[10]

WHAT STOPPED PRESIDENT MUSHARRAF FROM USING THIS PRICELESS ASSET?

The purported initial denial by Kayani and Pasha of bin Laden's presence in Pakistan and their subsequent admission that the al Qaeda leader was in their custody raise a number of questions. If, as Hersh maintains, bin Laden had been in the ISI's custody in Abbottabad since 2006, then-President and Army General[11] Pervez Musharraf must have known about it and given his consent and approval to the scheme. What stopped Musharraf from using this priceless asset to save his rapidly sinking political ship in 2007?[12] An offer from him to then-US President George W. Bush to eliminate America's most wanted terrorist—with or without officially admitting the role of Pakistan in his capture—would have been a God-sent opportunity for both of them. For Bush, bin Laden's capture and/or destruction would have been the crowning glory of his presidency, and would have given a significant boost to the Republican Party and the election campaign of the Republican candidate John McCain in the 2008 US presidential election. In an interview with CNN's Piers Morgan in late May 2011, however, Musharraf repeatedly denied any knowledge of bin Laden's presence in Pakistan

Former Presidents George W. Bush and Pervez Musharraf and clearly stated that had he known, he would have extracted maximum benefit for himself.

> If there was complicity, and [bin Laden] was there for five years, I get directly involved. That means I was complicit. … Now, if that was the case, I would like—I would have wanted to take leverage out of it. When I was at the receiving end in the 2007 [inaudible], I should have done something with this Osama bin Laden card and gained advantage. … I would have done something to turn the tables in my favor. … I would have used this card in my favor.[13]

Even conceding that Musharraf missed the trick, what prevented Kayani and Pasha from relocating bin Laden to a much more securely guarded facility when they were initially confronted with his presence in Abbottabad? A cynic might insist that they must have been blackmailed, coerced, or bought off. To begin with, it is simply bizarre to imagine that the ISI would hide a priceless asset like Osama bin Laden in such an undefended and vulnerable spot—that is not how the service is known to operate. Far less valuable assets than bin Laden are guarded very heavily when in ISI custody. Just as important, once Kayani and Pasha were coerced into accepting the US raid plan, could they not have suggested an alternative that would have still allowed the US administration to come out smelling of roses without discrediting the entire nation of Pakistan?[14] If, as Hersh insisted, bin Laden was in the custody of the ISI, the agency could have moved him physically, dead or alive, to a remote region of the inaccessible Afghan frontier where the brave SOF team could have staged their heroic raid with far less danger. The failure of the top Pakistani generals to do so would have painted them as dim-witted at best, or traitors at worst. While one may disagree with many of the policies of the top leadership of the Pakistani armed forces, dismissing them as dimwits or traitors is something not even their harshest critics would do. The Hersh version just does not hold water.

Washington
8:32 AM ET
NEW DEVELOPMENTS
WHAT REALLY HAPPENED IN BIN LADEN KILLING?
Seymour Hersh | Investigative Journalist
LIVE
CNN
8:32 AM ET

Did Kayani, Pasha, and Gates honestly believe, as Hersh implies, that two fully laden Blackhawks could unload heavily armed SOF personnel in a fairly well-built-up area of Pakistan and sit there for a minimum of 30 minutes, and that the entire incident would go unnoticed by the local populace?[15] Given the level of cooperation between the ISI and the CIA, as described by Hersh, would it not have made more sense to pre-position a helicopter and a small team of CIA operatives inside the compound, and after taking possession of bin Laden (dead or alive), have them fly off to Afghanistan and then claim, as agreed, that bin Laden was eliminated in a drone strike elsewhere? Was Obama so politically naïve that he gave his blessing to the delayed announcement scheme, or had he planned to double-cross the "not-so-bright" Pakistanis and his own secretary of defense from the outset?

DOES HERSH WANT US TO BELIEVE THAT THE REPUBLICANS ARE ALSO MORONS?

Hersh claims that Obama was able to extract tremendous political mileage from the bin Laden raid, to the point that it was touted as one of his crowning overseas achievements and helped him win reelection in 2012 with relative ease. If Obama blatantly lied to the American public about the raid, however, were his Republican enemies so simpleminded that they could not see through the farce and expose him? A charge of such magnitude, if proven, was bound to have led to Obama's subsequent impeachment. Does Hersh want us to believe that, like Kayani and Pasha, the Republicans are also morons?

Finally, Hersh questions the ceremonial sea burial of bin Laden's remains. His undisclosed sources suggest that the sea burial never took place and that the remains may have been either tossed overboard from the helicopters as they flew over the Hindu Kush mountains or buried elsewhere. While his assertions are within reason, Hersh does not give any verifiable source to back up his claim. In either case, it makes sense for the White House to have made a public display of the body's disposition in a way that prevented bin Laden's followers from turning his burial site into a pilgrimage place for radicals—if any part of him were anywhere on land, someone was bound to claim they knew where it was. Scattering bits of his body across the mountains (and thus leaving his death uncertain), as Hersh claims took place, if it became known, could easily incite a violent backlash among his followers and imitators while making Americans feel squeamish. The sea burial may in fact have been a lie, but it was a good idea nevertheless.

For the general public in Pakistan and the international audience abroad, the failure of the ISI, renowned the world over for its professionalism in the murky world of espionage, to detect the presence of Osama bin Laden so close to the army's prestigious military academy for more than four years is very hard to swallow. While the hunt for bin Laden had the highest priority in the United States, the mere possibility of his presence in Pakistan was a nightmare scenario for both the ISI and the national leadership. Whether the ISI captured him and handed him over to US forces or killed him outright, either action could have had major fallout within Pakistan because of bin Laden's cult following among a section of the public. Harboring him was equally dangerous and likely to be viewed as an extremely hostile act by the United States and its Western allies. Besides economic and political sanctions, Pakistan could have found itself directly in the crosshairs of the American military. The world is a witness to the destruction of Afghanistan and the Taliban-led Afghan government after they dared to refuse to hand over bin Laden to the United States in 2001.

Besides the helicopter crash that woke up the neighborhood, the shooting and blasting of doors by the commandos continued for the next 40 minutes. According to journalist Jane Corbin, neighbors had alerted the local police about the crash of a helicopter, but the police were told to stand down by the Abbottabad army high command.[16] The possibility that the Americans had warned the Pakistanis at the last minute about a raid on a high-value target, without specifying who, and that the local authorities judiciously turned a blind eye, is a theory Pakistan's security analysts favor.[17]

Given the murky history of rogue elements within Pakistan's military and intelligence who are sympathetic to Islamic militants, the possibility that these sympathizers provided support to bin Laden and his motley group at their hideout in Abbottabad cannot be ruled out.[18] There is still, however, no conclusive proof whether the presence of bin Laden was known by the country's top intelligence and military commanders, or whether he was indeed in their custody. The one possible explanation for the failure of the ISI to detect bin Laden's presence was its leaders' firm belief and fervent hope that he was either dead or—more likely—barely surviving on the fringes of the Pakistani-Afghan border. The ISI never seriously hunted for bin Laden within Pakistan, thus falling victim to its own canard.

In conclusion, the broad contours of the official US account of the bin Laden raid appear plausible, but as the deputy director of the CIA told one reporter, "there are parts of the US account the world may never be told. … 'Not a hundred percent of the story is out there.'"[19] Exaggerations concerning the tactical details of the behind-the-scenes intelligence work and the actual raid, such as those depicted in the Hollywood film *Zero Dark Thirty*, are at best the kind of propaganda tool very commonly wielded by the victor.[20]

Seymour Hersh needs to take a closer look at his sources and revisit his monograph on the real story behind Operation Neptune Spear, as the bin Laden raid was known to its planners, if he wishes his latest work to be taken seriously within academia. ❖

ABOUT THE AUTHOR

Air CDR (Ret.) Jamal Hussain is the director of Pakistan's Center for Air Power Studies.

NOTES

[1] Seymour M. Hersh, "The Killing of Osama bin Laden," *London Review of Books* 37, no. 10 (21 May 2015): http://www.lrb.co.uk/v37/n10/seymour-m-hersh/the-killing-of-osama-bin-laden . Hersh received acclaim early in his journalism career for work that exposed the My Lai massacre in Vietnam. More recently he helped break the story of the Abu Ghraib prison scandal in Iraq.

[2] For details on high- and low-level radar systems function, see Jamal Hussain, "The Phantom Raid," in this issue of *CTX*. In peacetime, Pakistan does not maintain standing air patrols along its borders. Pilots rotate on standby, ready to scramble instantly when alerted.

[3] In this event, spoofing and jamming were not necessary; the raiders progressed to the destination undetected. Nor was Abbottabad under low-level radar surveillance, perhaps because it was not considered a vulnerable area during peacetime.

[4] Hersh, "Killing of Osama bin Laden."

[5] Ibid.

[6] Ibid.

[7] Ibid.; Macon Phillips, "Osama Bin Laden Dead," *What's Happening* (blog), 2 May 2011: https://www.whitehouse.gov/blog/2011/05/02/osama-bin-laden-dead

[8] Gareth Porter, "Exclusive Investigation: The Truth behind the Official Story of Finding Bin Laden," *Truthout*, 3 May 2012: http://www.truth-out.org/news/item/8866-finding-bin-laden-the-truth-behind-the-official-story

[9] Jane Corbin, "Have We Been Told the Truth about Bin Laden's Death?" BBC, 17 June 2015: http://www.bbc.com/news/world-middle-east-33152315

[10] Ibid. Obama acknowledged Pakistan's cooperation in a single sentence of his post-raid speech.

[11] He did not retire from the Army until November 2007, following reelection.

[12] Musharraf fled Pakistan for exile in Britain in August 2008 after the parliament called for his impeachment.

[13] See minute 4:50 of "CNN Official Interview: Pervez Musharraf Eyeing Old Job," YouTube video, 6:32, posted by CNN, 26 May 2011: https://www.youtube.com/watch?v=DlRyUZf_oAA

[14] According to Hersh, "Pasha and Kayani were responsible for ensuring that Pakistan's army and air defence command would not track or engage with the US helicopters." Hersh, "Killing of Osama bin Laden." Hersh's assumption that someone high in the military command could make such a promise on his own, without taking the PAF air chief into his confidence, is misled. The air defense system of Pakistan is directly under the command of the chief of the Air Staff PAF, and only he could guarantee that there would be no interference with the airborne intruders. The entire ground radar network related to early detection, the airborne early-warning platforms, and the interceptor fleet are entirely under the command of the PAF. In the aftermath of the bin Laden raid, it was the PAF and not the Pakistani army that came under fire for failing to detect the raiders.

[15] Within half an hour of the departure of the helicopters, the attack was breaking news on a number of local TV channels. I personally heard a number of eyewitnesses say they were alarmed by the noise of the helicopter crash and the sound of gunfire. According to some witnesses, any efforts to approach the site were met with warnings in Pashto from loudspeakers within the compound, telling people to stay away.

[16] Corbin, "Have We Been Told the Truth?"

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] *Zero Dark Thirty*, directed by Kathryn Bigelow (Los Angeles: Columbia Pictures, 2012): http://www.imdb.com/title/tt1790885/?ref_=nv_sr_1 . *Editor's note*: You can read a review of the film *Zero Dark Thirty* by Kalev Sepp in *CTX* 3, no. 2 (May 2013): 99–101: https://globalecco.org/documents/10180/605826/Vol+3+No+2+WEB+FINAL.pdf/1e3bb0fe-1959-4cb3-86f9-294c44c81fc9

The Sri Lankan Civil War: A Personal Reminiscence

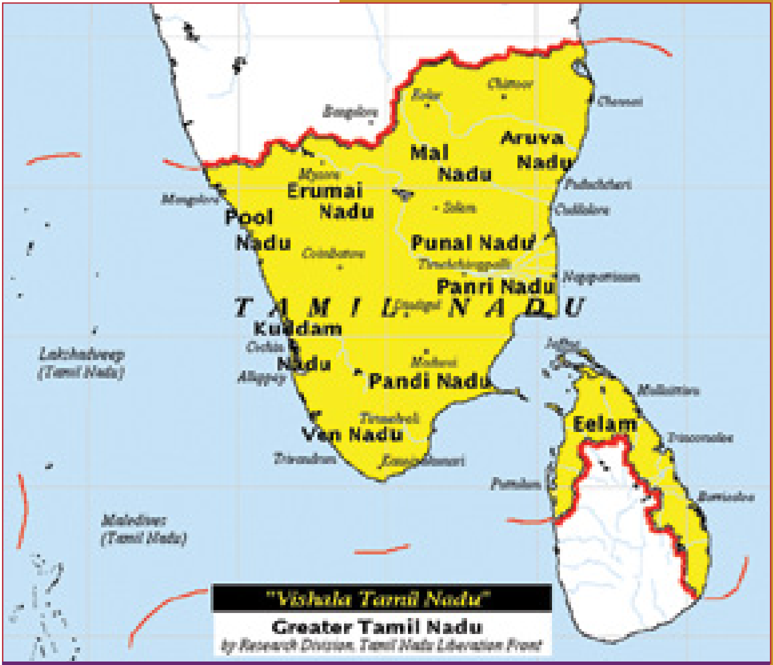
COL Sylvester Perera,
Sri Lankan Army

As a member of the Sri Lankan armed forces, I have served since 1992 in various capacities that dealt with the planning and execution of counterterrorist operations against the ruthless insurgent organization known as the Liberation Tigers of Tamil Eelam (LTTE). The effort to eliminate the terrorists completely from Sri Lankan soil through military strategy and political and national will superseded all other national priorities and was ultimately successful. In this article, I discuss my operational experience in different stages of the conflict with the LTTE, the progress the armed forces achieved over time, and our success adapting small-group tactics to overcome LTTE strongholds and defenses. Finally, I describe my experience in the post-conflict period and offer recommendations for how to achieve sustainable peace in Sri Lanka.

TAMILS VIEW THE NORTH AND EAST OF SRI LANKA AS THEIR ANCESTRAL HOMELAND OF EELAM.

Historical Origins of the Conflict

Sri Lanka's geostrategic situation is a prime factor in the country's ethnic divisions. The northern tip of the island is only a few miles from the Indian coastal state of Tamil Nadu, which is home to more than 50 million primarily Hindu ethnic Tamils (see map 1). The territorial dispute between the majority Sinhalese population and the Tamils goes back more than 2,000 years, to a time when a Tamil king from the Indian mainland is said to have invaded Ceylon (the name of the island before it became a republic in 1972), and his descendants continued to struggle with the Buddhist Sinhala kings for territory. Tamils, however, do not believe that they are a migrant community and view the north and east of Sri Lanka as their ancestral homeland of Eelam. This is their core issue, similar in some ways to that of the Palestinians in Israel.



Map 1: Greater Tamil Nadu

Like India, Ceylon was occupied by the British Empire until 1948. Under colonial rule, Tamils played a large role in the civil service and business communities, but when independence came, they did not want to be ruled by the majority Sinhalese, whose policies they felt were discriminatory. Over the ensuing years, Sri Lanka's leaders and political parties failed to effectively address these issues, including the growing separatist movement. The armed insurgency that arose in the country's north in the 1970s was the culmination of these failures.

The LTTE was formed in 1976 by Velupillai Prabhakaran, who envisioned not only a separate Tamil state that would encompass the historically Tamil northern and eastern parts of Sri Lanka, but also a greater Eelam ("Precious Land") aligned with the state of Tamil Nadu in India. The so-called First Eelam War began in 1983 when the killing of

Sinhalese government soldiers in an LTTE ambush led to violent anti-Tamil riots. The Second Eelam War began in 1990 after Indian peacekeeping forces pulled out, and the violence between Tamil guerrillas and government forces escalated once again. Although the armed Tamil insurgency has been put down for now, the seeds of separatism, rooted in this historical perspective, will continue to sprout.

Anti-Terrorist Operations against the LTTE in Sri Lanka (1992–1996)

On 3 November 1990, I joined the Sri Lankan Army as an officer cadet and underwent training at the General Sir John Kotelawala Defense University in Colombo and the Sri Lankan Military Academy in Diyatalawa. On 14 December 1992, after successfully completing my military training, I was commissioned as a 2nd lieutenant attached to a regiment of the 6th Infantry Battalion, called the Gemunu Watch. In 1993, I completed a degree in defense studies at the Kotelawala Defense University and subsequently joined my battalion in the eastern part of the country, where we conducted limited operations against the LTTE in the area.

OUR ENEMY ALWAYS HAD THE INFORMATION ADVANTAGE.

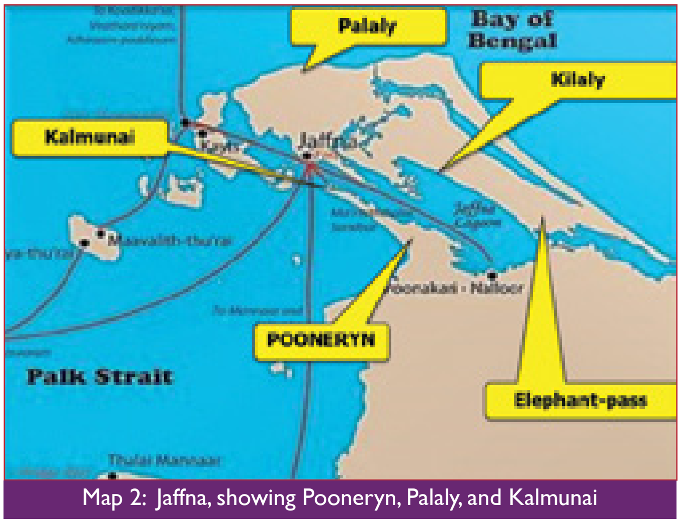
Around that time, following the withdrawal of the Indian Army's peacekeeping force and with massive support from the Tamil diaspora, the LTTE insurgency had reached a stage of open combat. Our battalion's aim, therefore, was to destroy the LTTE cadres who were operating from the nearby jungles and thus clear the threat they posed to our main camp and the nearby Sinhala and Muslim villages. Our warfare strategy was conventional, and we remained focused on one objective at a time. Because of this, our enemy always had the information advantage. While we were on the offensive, the LTTE were able to either withdraw or cut off our troops and inflict heavy casualties by throwing the collective strength of their local forces at us. Accordingly, we were able to achieve only very limited success in these early stages. The experiences I describe in the following sections illustrate just how resourceful and tenacious the LTTE were in fighting for their independence, and what the Sri Lankan armed forces had to undertake and learn in order to defeat them. (See appendix A for a list of these engagements and their dates and locations.)

The Reinforcement of Pooneryn Camp

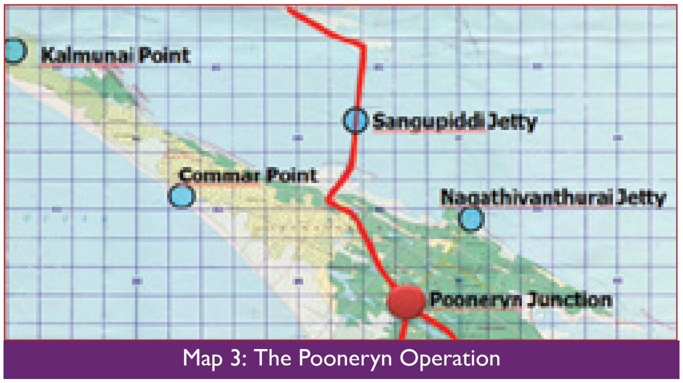
The Pooneryn military sector is in the northwest of Sri Lanka, separated by Kalmunai lagoon from the city of Jaffna to the north. A route connecting Jaffna with the south used to run up through Pooneryn. The Elephant Pass causeway, the other main route between the north and south, lies about 12 miles east of Pooneryn. The Pooneryn military sector was established to seal off the Tamils' Jaffna peninsula stronghold and pave the way for an assault on Jaffna from Pooneryn itself. Nagathivanthurai Naval Base, to the northeast of the Pooneryn sector, was monitoring civilian and LTTE movements on the lagoon. The area south of Pooneryn was under LTTE control.

On 11 November 1993, at 0020 hours, the LTTE launched a massive attack on the Pooneryn Army Camp. On this particular day, I was serving as a platoon commander in the Gemunu Watch, which was conducting search-and-clear operations in the eastern jungles. About four hours after the attack began, we were heli-lifted to Palaly Air Base, situated in the northern part of Jaffna, to try to reinforce the besieged Pooneryn Camp (see maps 2 and 3). The air force's Bell 212, Bell 412, and MI-17 helicopters from Palaly attempted to insert our first platoon by air but were forced to withdraw under heavy LTTE fire. Simultaneously, at about 1500, after seven hours of sailing, a group of commandos made an attempt to land off Kalmunai (the western tip of Pooneryn). Heavy LTTE fire did not allow these reinforcements to gain a foothold on the beach, while the accompanying naval vessels were unable to get close enough to the shore to give effective covering fire because of the shallow water. Ultimately, all our attempts to insert forces failed due to heavy resistance.

On the following day, 12 November, the air force launched air strikes against the LTTE forces, but our efforts to land any aircraft near the Pooneryn base failed again due to continuous attacks by the Tigers. By this time, some of the surviving soldiers from the army camp had managed to make contact with us by radio. They told us that their group of about 550 men had moved down the southwest coast of Pooneryn and therefore could be reached more easily than the main army camp. In the evening, our pilots dropped supplies, including food, medicine, and batteries, to the besieged men. Finally, on 13 November, our team of commandos, supported by infantry, made a successful beach landing southwest of Pooneryn. Simultaneously, our pilots accomplished their assigned task and safely reached the soldiers' location. As a platoon commander, I landed with the battalion a few miles away from the main base in Pooneryn as reinforcement. As we moved in, we evacuated wounded soldiers and rushed them to a helicopter landing area that we had cleared. We were able to clear the area with enough heavy fire to enable the naval troops and helicopters to land. In response to our successful landing and advance, the LTTE forces started to withdraw from Pooneryn. On 14 November, the fourth day after the initial attack, we consolidated our control of the entire camp.



Map 2: Jaffna, showing Pooneryn, Palaly, and Kalmunai



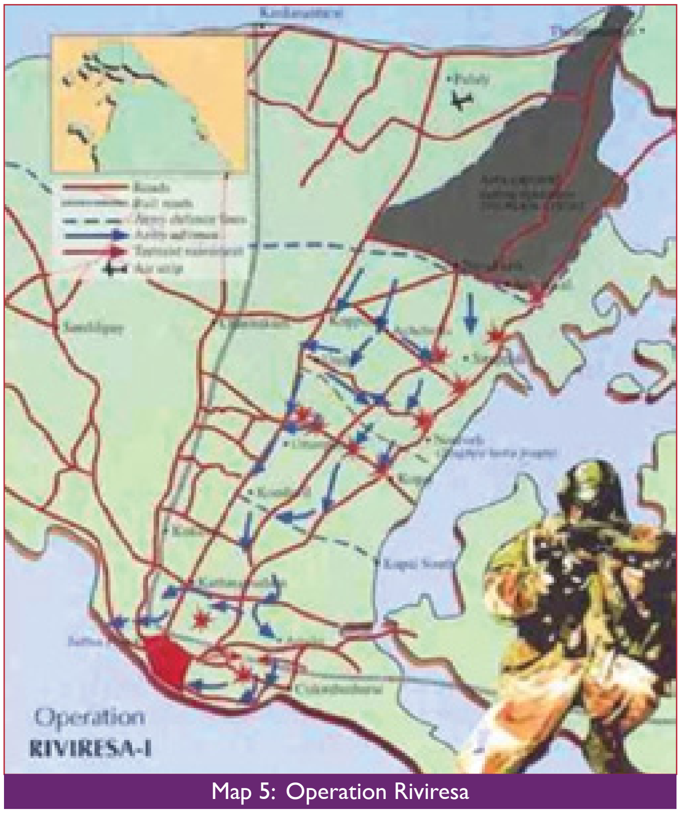
Map 3: The Pooneryn Operation

During the First and Second Eelam Wars (beginning in 1983 and 1990, respectively), the LTTE stayed on the offensive, and the government had to react to their innovations.[1] Pooneryn is a vast area guarded jointly by the army and navy. When the Pooneryn base was attacked in the incident I described above, the full strength of the camp was 1,500 soldiers, while the total strength of the LTTE cadres at that time was understood to be over 5,000. The LTTE's guerrilla tactics—including infiltrating through the forward line of troops, attacking from the rear, and wearing a uniform similar enough to allow them to mingle with the regular army soldiers—contributed greatly to their successes. The LTTE also concentrated all their resources against security forces in their major offensive operations. They managed to overrun many military bases, inflicting heavy losses and damage, just as they had in their attacks in Pooneryn.

Operation Riviresa: The Liberation of Jaffna

Operation Riviresa was the largest operation ever launched by the Sri Lankan security forces; its objective was to take Jaffna from the LTTE. During a brief

Map 4: Operations Riviresa and Thunder Strike



Map 5: Operation Riviresa

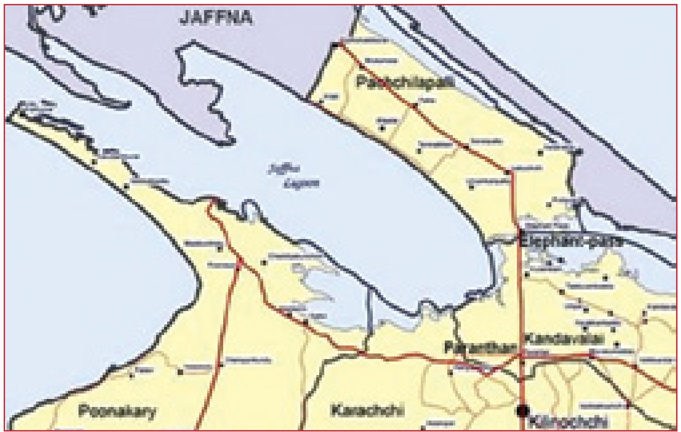
cessation of hostilities following national elections and a change of government in 1994, the LTTE was able to regroup, restock, and train sufficient cadres to enhance its offensive capability. This raised concerns within the government, and our worst fears were realized in late April 1995, when the LTTE downed two military aircraft using surface-to-air missiles and repeatedly attacked naval craft, thus severely hindering the army's movements into and out of the Jaffna Peninsula. At this point, the Sri Lankan government decided that offensive action to regain the peninsula was imperative. Accordingly, our battalion trained for three months on Kayts Island, situated to the west of Jaffna, focusing on the skills for fighting in built-up areas. Because there were no civilian inhabitants on the island, we did our training with live fire. After completing this training, in July 1995 we were transported to Kankesanthurai Harbor, on the northern coast of Jaffna, by naval mechanized landing craft. Our reserve strike division launched a preliminary operation (called Thunder Strike) to capture the town of Achchuveli, approximately 16 kilometers north of the city of Jaffna (see maps 4 and 5). This was a highly successful operation in which the LTTE suffered heavy casualties. Its outcome largely supported Operation Riviresa by boosting troop morale and reinforcing Palaly Air Base.

On 1 October 1995, just before Operation Riviresa began, our battalion launched an offensive to expand the Palaly forward defensive line along the Kankesanthurai–Jaffna road. We took Mallakam town, which is 10 kilometers from the town of Jaffna, by surprise, and were able to destroy a large number of terrorists during the LTTE's foiled counterattacks. Subsequently, on 17 October, we shifted our battalion to the Point Pedro–Jaffna road (the easternmost approach of Operation Riviresa) and started our advance from Achchuveli town along with the western approach along the Palaly–Jaffna road (see map 5).

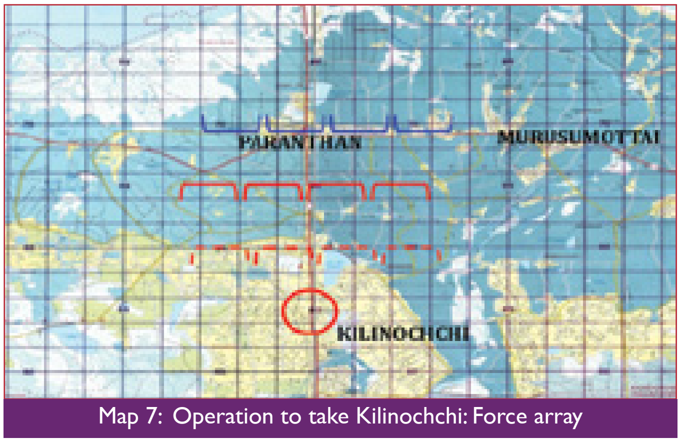
For the first time in the history of Sri Lanka, the armed forces launched an offensive operation involving three divisions. Our two infantry divisions launched the operation along a narrow front on converging axes using conventional tactics. We were vulnerable to LTTE indirect fire, but the concentration of force, which was applied at the right time and place, helped to outnumber the LTTE and subsequently demoralized them. Unprecedented concentrated fire from artillery, mortars, and tanks, combined with air and continuous ground assaults, broke the will and cohesion of the LTTE forces. On 2 December, we entered Jaffna city but found it abandoned—it looked like a ghost town. The LTTE had taken everything before their withdrawal, and the inhabitants had fled. In the aftermath of the operation, we resettled the 600,000 civilians who had camped on the west side of Jaffna Peninsula during the operation. This operation was a turning point for the LTTE as a guerrilla force, and the point at which the mindset of the Tamil population began to turn away from supporting the LTTE, who were moving toward a losing endgame.

Operation Sath Jaya: The Liberation of Kilinochchi

About seven months later, on 18 July 1996, having experienced a battlefield defeat at Mullaitivu (the main town of Mullaitivu District, situated on the northeastern coast of the Northern Province), Minister of Defence General Anuruddha Ratwatte ordered Operation Sath Jaya to be launched on 26 July. The goal was to liberate the LTTE stronghold of Kilinochchi (the main town in Sri Lanka's north, located 100 kilometers southeast of Jaffna) and rebuild the reputation of the government after that demoralizing defeat. Our earlier victory during Operation Riviresa gave our forces the experience they needed to plan for the liberation of Kilinochchi. At the beginning of the operation, I was the second in command of Bravo Company. Our battalion started the march into LTTE territory from Paranthan toward the east as a deception and met with strong enemy resistance. Only about five kilometers in, the LTTE intercepted our troops and launched a heavy attack. On the following morning, as the troops again attempted to move in the same direction, the LTTE staged another counterattack. We suffered heavy casualties, including two platoon commanders and many senior noncommissioned officers.



Map 6: Operation to take Kilinochchi: Major routes



Map 7: Operation to take Kilinochchi: Force array

After two days of intense fighting on the eastern flank, Special Forces opened another approach from west to east on our western flank. Subsequently, my battalion withdrew from the eastern feint and made our real move on the western front. On 26 September, when our battalion tried to break out toward Kilinochchi from the new approach, the LTTE launched a spoiling attack with heavy artillery and mortar fire support. We lost 168 soldiers, including some officers. Tragically, my company commander died in my lap as the result of a gunshot wound to his chest. Nevertheless, we managed to kill all of the LTTE cadres who took part in the spoiling attack. The commanding officer appointed me to take over as company commander and ordered me to continue our operation to capture Kilinochchi town, which we achieved against heavy resistance on 30 September 1996.

Operation Unceasing Waves II

On 27 September 1998, on my first day back with the battalion after attending overseas training with the Indian armed forces, the LTTE launched a successful attack against my battalion's defenses in Kilinochchi, 10 miles south of Elephant Pass (see maps 6 and 7). I was the commander of Bravo Company, 6th Battalion, Gemunu Watch, for an operation codenamed "Unceasing Waves II." Our battalion was holding a defensive line facing southward toward the LTTE stronghold. At around 0100 hours, our defenses began to receive small arms fire, along with a heavy barrage of artillery fire. During this attack, the LTTE also started shelling the tactical headquarters of the brigade and battalions. The guerrillas penetrated our defenses from the flanks and started firing from our front and rear with massive fire support. After we had spent many hours of fighting off their ceaseless assaults, the LTTE managed to cut our forces off from the rear and surround our defenses. They fired rocket-propelled grenades at the tanks, armored personnel carriers, ambulances, and other vehicles that were involved in reinforcement and the evacuation of casualties. Our battalion nevertheless remained intact, and we effectively repulsed all the waves of assaults, but at the cost of heavy casualties.

After two days of fighting, at 1700 hours we received orders to withdraw from the defensive line toward Elephant Pass, but we were still completely surrounded by the LTTE. We eventually managed to conduct a tactical withdrawal in contact. By that time, I had lost one of my platoon commanders and many soldiers. The LTTE subsequently took control of the town of Kilinochchi and a five-mile stretch of the A9, the Jaffna–Kandy road, which remained in their hands until the army liberated the area in 2009. Conversely, on the same day that the LTTE captured Kilinochchi, security forces took the city of Mankulam, the main township south of Kilinochchi.

Strength and Leadership Problems for the Sri Lankan Forces

A major issue for military leaders and planners during this time was a lack of adequate forces. Army personnel were not equipped and trained adequately to conduct offensive operations, and the army had an acute shortage of the troops it needed to conduct operations and hold ground, problems that were evident from the beginning of the conflict. Unfortunately, successive governments did not address these deficiencies, and there were numerous incidents at Kokavil, Mulathive, Elephant Pass, and Mandathive where our forces failed to counter LTTE attacks. During the initial period of the Second Eelam War, in 1990, Sri Lanka's armed forces were in a defensive posture except for domination patrols to destroy or capture enemy soldiers and equipment; destroy installations, facilities, and key points; and harass enemy forces. These patrols also provided security for larger units as needed. The navy and air force took a supportive role by providing logistical support to the army where it did not have land access to its bases and camps.

Operation Riviresa was one of the major operations conducted by Sri Lanka's armed forces against the LTTE, and it was both well-planned and well-coordinated. The primary objective of the operation was the capture and liberation of the town of Jaffna and the rest of the Jaffna peninsula. By contrast, during Operation Sath Jaya to capture the LTTE stronghold of Kilinochchi, the country's political leadership overrode the advice of military commanders and drove the army to stretch its forces beyond the practical limits of defense. Political leaders were wrongly convinced that the LTTE would collapse after the recapture of Jaffna city.

Operation Riviresa had us advancing along two road axes, which enabled us to protect our flanks throughout the offensive and prevent any counterattack by the LTTE. During Operation Sath Jaya, however, a shortage of troops left our southern flank mostly open to the LTTE's counterattacks. We marched into the LTTE stronghold of Kilinochchi on a single axis and sustained heavy casualties from LTTE artillery and mortar fire, in addition to their counterattacks and spoiling attacks. The broad front and width of Operation Riviresa provided enough maneuverability for our troops and armor, while by comparison, Operation Sath Jaya's narrow front restricted the maneuverability of the assaulting troops and armor. Furthermore, because we focused our operation on a single objective, the LTTE were able to throw their entire strength at us, delay the operation, and inflict heavy casualties. During both operations, we observed that our relief system to rotate soldiers into and out of the front lines did not function well, which meant that soldiers were exhausted from remaining continuously on the battlefront. New recruits and soldiers who were not trained prior to the operation accounted for most of our casualties.

DURING OPERATION SATH JAYA, THE COUNTRY'S POLITICAL LEADERSHIP OVERRODE THE MILITARY COMMANDERS.

During the initial stages of the Eelam Wars, our manpower shortages meant that we were unable to maintain security even in areas where the war did not reach. When the LTTE began losing battles in the northern and eastern regions that had been under their control, they began to carry out periodic attacks on economic, political, and social targets in the south. The LTTE's most lethal weapon was suicide bombings, for which we had no answer.

From these experiences, I came to understand that the success of operations depends primarily on sound intelligence, which depends in turn on the structure and function of the intelligence agencies. In the fight against the LTTE, there were many government agencies and departments with various structures and functions dedicated to conducting strategic planning for operations. They functioned in isolation, however, which made it difficult for them to integrate their work and also slowed the dissemination of information and intelligence. To complicate things further, the various branches of the intelligence agencies and the people working within them tended to compete with one another rather than cooperate. In most cases, these agencies were unable to provide clear situational pictures developed from the available intelligence, but rather were inclined to provide just some information collected from a few sources. LTTE strategies, tactics, motives, and intentions shifted constantly, depending on the local and international situations, but the information provided by the intelligence services throughout the conflict was almost entirely inaccurate, which meant that the military lost the initiative.

In one instance, the military did receive an accurate intelligence picture, and the subsequent operation was successful. In 1995, the LTTE attacked the Weli Oya area, in the northeastern part of the Sri Lankan mainland, but thanks to good information, the Sri Lankan Army was able to cut off and ambush the insurgent fighters, who lost over 300 cadres killed or injured. This was the first time the LTTE had lost such large numbers. Other than this one event, however, the intelligence provided to the military lacked answers to the vital questions of when, where, what, and how—the most fundamental aspects of a useful intelligence picture. As a result, our operations either were ineffective or became nightmares of shock and surprise for our troops.

Because the intelligence agencies entirely failed to understand the importance of good intelligence and how it could be exploited in warfare, the LTTE took advantage of the situation to conduct a large number of successful surprise attacks on high-value targets. LTTE terrorists assassinated several political and military leaders, including, in 1993, President Ranasinghe Premadasa. This situation ultimately led to misunderstanding and a loss of credibility between the intelligence agencies and the ground troops.

Another area in which the LTTE had an advantage was in using public relations to build support for their fighters and their cause. The army did not have any experience handling either public relations or the media, so we did not inform the public about our successes or failures or do anything to counter LTTE propaganda. The LTTE were therefore very effective at winning sympathy and financial support from the Tamil diaspora and others around the world.

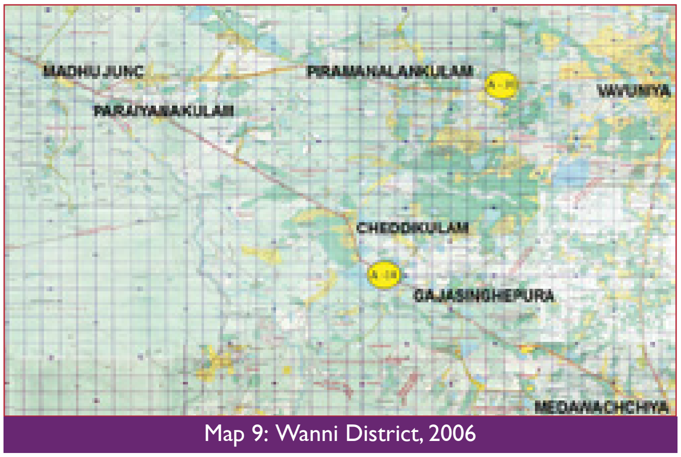
THE LTTE WERE VERY EFFECTIVE AT WINNING SUPPORT FROM THE TAMIL DIASPORA.

The Fourth Eelam War (July 2006–May 2009)

After I graduated from the Army Command and Staff College in 2006, I was posted as brigade major to the 214th Infantry Brigade in Vavuniya, one of the major districts in the Northern Province of Sri Lanka.[2] At this time, LTTE leader Prabhakaran had boycotted all attempts at peace made by the new government, and after a long ceasefire (2002–2006), fighting began again. My brigade's mission was to conduct an operation along two approaches from the east and the west to liberate the LTTE stronghold in a region called the Wanni (see maps 8 and 9). The situation had become critical after several attacks on military convoys in my brigade's area of operations. My commander ordered me to provide an effective plan to deploy troops on two major roads from Vavuniya to the west coast. The goal was to stop clashes in which Tigers were inflicting heavy casualties on the brigade and killing a number of civilians.

I did a thorough study of the brigade's area of responsibility and the many incidents that had occurred there, such as Claymore ambushes and suicide attacks on military convoys and civilian buses on the southern roads that lead toward the west coast. These roads were supposed to be protected by the military in conjunction with specially trained police, but I found that there was no proper coordination, understanding, or confidence between police and military personnel. After discussing the matter with the brigade commander,

Map 8: The Wanni Operation, 2006



Map 9: Wanni District, 2006

I organized a training team with a few officers and Other Rank (non-commissioned) instructors and prepared a syllabus for a police refresher military training course. I planned the training to focus mainly on field craft, tactics, map reading, and weapons training, along with lectures on leadership, motivation, and team-building. The training was completed within two months as planned, under my close supervision and control. The police officers who went through the course started respecting the military more, because we had trained them in the skills they needed. Subsequently, we deployed police troops very effectively along the main roads, while the military conducted offensive operations against Tiger forces in the jungle. This training and cooperation allowed us to greatly reduce the overall threat and the number of incidents that occurred.

Changing Strategy

After efforts to negotiate a settlement with the LTTE during the fifth round of peace negotiations failed, in July 2006 the army started an all-out assault against the LTTE with the blessings of the new government.[3] The LTTE itself shifted to an open offensive posture using semi-conventional tactics, such as establishing camps and bases and holding defensive lines. As the insurgents became more visible militarily, we realized that there should be a shift in our own strategy, away from the conventional warfare we had been practicing in the previous Eelam Wars toward an insurgent-centric approach that aimed to isolate and destroy the LTTE. During Operations Riviresa and Sath Jaya, we concentrated more on capturing ground, a strategy that did not have much impact on the LTTE organization itself. Now all military efforts would be directed according to this unconventional strategy, which was completely new to our experience.

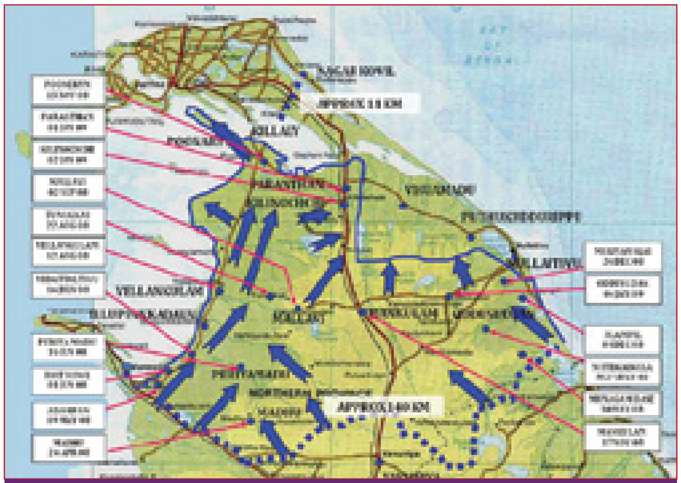
Thus, in mid-2006, using all the resources available, we began major—and what turned out to be final—offensives against the LTTE in a bid to end the three-decade–long conflict. Unlike previous phases of the war, this time the entire army enjoyed complete operational freedom to launch the offensive, using the best men to do the tasks. We adapted the unconventional tactics of small-group operations in broad fronts along all three approaches from the south. The privilege of exercising mission command and initiative went to junior leaders, including Other Rankers. I should mention here that the small-group operations conducted by special infantry operations training (SIOT) platoons were commendable. These SIOT platoons carried out special operations in the immediate vicinity (within four to five kilometers) against strong LTTE defenses that were preventing the security forces' advance. We never limited small-group operations to the elite forces but committed the SIOT platoons extensively. In the meantime, we used the rest of the battalion manpower to find, fix, and destroy the insurgents and hold the ground thus captured. These operations were very successful.

Subsequently, in August 2008, I was selected to hold a staff officer appointment at the United Nations Missions Force Headquarters in Haiti and left Sri Lanka to take up this new post.

Elements of Our Victory against the LTTE (2007–2009)

Our army finally achieved victory in 2009, after liberating the Eastern and Northern Provinces and giving freedom to the Tamil people who had been under the thumb of the LTTE. When we analyzed and compared the earlier and later stages of the conflict, what stood out was the change in military training. Since independence in 1948, army training in Sri Lanka had consisted of traditional maneuver training based on British doctrine, with the addition of some improvised training that would suit the Sri Lankan environment. During the ceasefire of 2002 to 2006, the army conducted SIOT training to address LTTE fighting strategies. SIOT operations took away the freedom of movement that the LTTE elements had enjoyed over the decades of insurgency, bringing the battlefronts within four to five kilometers of LTTE camps. Simultaneously, Special Forces and commandos began to operate in the rear areas of LTTE territory. In the course of my studies, I learned that during World War I, the German army adopted a similar formation that they called "stormtroop" units.[4] These units gave lower-ranking officers the opportunity to form small, agile groups equipped with a wide variety of combat weapons and specialties. Furthermore, the NCOs were involved in the decision-making process and were entrusted with real responsibilities. This improvisation paved the way for the introduction of "Blitzkrieg" at a higher level in World War II and brought success to the Germans in their major offensives.

In the final operation to defeat the Tigers, our professional military leadership and guidance, clear military aims, political leadership, and national will came together, shaping our military strength to meet our need. All three components of the Sri Lankan military's fighting power—conceptual, moral, and physical—had gone through rapid changes to prepare the forces to fight decisively against the LTTE. As for our military strategy, Operation Riviresa was the first time we used a "multi-thrust line" approach rather than fighting on a single front. The LTTE had never seen this maneuver before, and as a result, they had to dissipate their combat power to confront each line, weakening their overall combat cohesiveness and combat synergy. The small-group concepts adapted by our forces were a very effective innovation.



Map 10: Capture of the LTTE Stronghold of Kilinochchi, 2008-09[5]

During the final phase of operations conducted against the LTTE, we maintained constant momentum and the impetus of the offensive by both securing the land we captured from the LTTE and relentlessly carrying out offensives. Due to the paucity of troops, this strategy could not be adopted in earlier offensives, and accomplishing it was another significant factor that contributed to victory. In addition, our navy destroyed 10 LTTE ships (seaborne warehouses) in blue waters and completely cut off the supply route of the LTTE. This turned out to be a pivotal point in the campaign, which, along with the liberation of Jaffna in 1995, aided the Sri Lankan Army's operations on land to bring the majority of Tamils under government control and led to final victory. Without the stronghold of Jaffna, the LTTE could not mobilize the Tamil majority against the government of Sri Lanka as they did in the 1987 Vadamarachchi Operation in eastern Jaffna, when the government had to stop fighting due to pressure from the Indian government.

The Post-Conflict Situation

After completing my assignment to the UN mission in Haiti, I returned to Sri Lanka immediately after the victory over the LTTE. I was appointed commanding officer of the 8th Battalion of the Gemunu Watch (Infantry). My duties were in the war-affected areas, assisting with rehabilitation, resettlement, and reconciliation programs in a post-conflict environment. I worked extensively in civil-military coordination alongside governmental and nongovernmental local and international agencies engaged in development. My duties were sometimes a terrible challenge, because most of the people, victims of the protracted war, were very poor and frustrated. I realized that defeating an insurgency does not bring the conflict to a conclusive end. I had to put all my efforts into managing a post-conflict society for peace building, within a framework called *disarmament, demobilization, and reintegration*. Despite all our work, however, it seems that Sri Lanka is still facing these challenges: pro-LTTE elements continue to make strong attempts to propagate the Tamil separatist ideology and discredit the Sri Lankan government's efforts to bring sustainable peace.

DEFEATING AN INSURGENCY DOES NOT BRING THE CONFLICT TO A CONCLUSIVE END.

To meet these post-war challenges, the Sri Lankan government should double the strength of its intelligence community. I do not, however, see the need to maintain military bases all over the country to stop the reemergence of another separatist movement. Looking back, I believe that "Black July" in 1983, the day on which Sri Lanka had the worst riot in its history, was a turning point for the LTTE, because it gave the separatists a fine opportunity to build support for their movement. Until then, none of these groups, including the LTTE, could muster more than 20 sympathizers at a time. In other words, the Tamil insurgency that waged a 30-year struggle for a separate homeland in Sri Lanka had an accidental birth. A sound intelligence system would have helped us defeat that movement before it grew large enough to be dangerous, and it is what will allow us to launch an operation at any given time to defeat any future threat.

Ruins of Governor's Bungalow, Jaffna, destroyed in 1980s civil war

At the strategic level, we need a central intelligence organization. There is no proper mechanism or body to coordinate the work and exchange of personnel between the various intelligence branches. We need to build a common security and intelligence database, conduct joint training and joint operations, and share technology, expertise, and experience that will enable us to embrace new technological concepts. Further, friendly foreign nations could have a role in this organization to coordinate intelligence. At the operational level, we should design a research and development unit that caters to local intelligence requirements as they evolve to counter the separatist ideology. At the tactical level, we need to institute periodic and extensive training and awareness programs to impart the skills that will allow individuals to identify resistance networks while they are still at an early stage.

Now it is time to forget the bitter past and leave behind the war mentality. We defeated the LTTE in an effort to find a lasting solution to the problem of violent insurgency. If we try to live in the past, then in the years to come, all our sacrifices will have been in vain. The government must take all precautions to avoid the blunders that were made in 1983. We need to win the hearts and minds of the Tamil community and address their core issues. To lessen the mistrust among communities, we must think as Sri Lankans at all levels. ❖

ABOUT THE AUTHOR

COL Sylvester Perera serves in the Sri Lankan army.

Appendix A: Timeline of My Participation in Operations against the LTTE

Srl No	Rank	Appointment	Station/Unit	Location	Duration	
					From	To
1	Cadet	Student	General Sir John Kotelawala Defence University/Sri Lanka Military Academy	Diyathalawa	1990/11/03	1993/10/08
2	2/Lt	Platoon commander	6 Battalion the Gemunu Watch	Trincomalee, Pooneryn, Jaffna, Vavuniya, Killinochchi	1993/10/21	1996/09/26
3	Capt	Company commander	6 Battalion the Gemunu Watch	Jaffna, Kilinochchi Elephant Pass	1996/09/27	1999/07/01
4	Capt	ADC to GOC	52 Division/Overall Operations Command	Jaffna/Colombo	1999/07/01	2001/10/22
5	Maj	Staff officer/ instructor	General Sir John Kotelawala Defence University/Sri Lanka Military Academy	Ratmalana	2001/10/24	2003/12/22
6	Maj	Operations and training officer	6 Battalion the Gemunu Watch	Batticaloa	2004/03/15	2005/01/31
7	Maj	Brigade major	214 Brigade	Vavuniya	2005/12/29	2006/11/02
8	LTC	Directing staff/ adjutant	Sri Lanka Military Academy	Diyathalawa	2006/11/02	2008/08/18
9	LTC	Staff officer, UN MSN Haiti	United Nations Stabilization Mission	Haiti	2008/08/20	2009/08/20
10	LTC	Staff officer I (Posting/Promotions)	Military Secretary's Branch, Army Headquarters	Colombo	2009/09/25	2010/04/15
11	LTC	Commanding officer	8 Battalion the Gemunu Watch	Batticaloa	2010/04/16	2012/01/30
12	LTC	Directing staff	Defence Services Command and Staff College Sapugaskanda	Sapugaskanda	2012/01/31	2015/12/23

NOTES

[1] For a timeline of the Sri Lankan civil war, see "Sri Lanka Profile—Timeline," BBC, updated 9 January 2015: http://www.bbc.com/news/world-south-asia-12004081

[2] In 1999, I was selected to be the aide-de-camp to the general officer commanding, 52nd Division, and later to the overall operations commander, Colombo. Subsequently in 2002, with the rank of captain, I served as staff officer 3 in the training wing of the Kotelawala Defence University in Colombo. I returned in 2004 as a major to the 6th Battalion of the Gemunu Watch, which was deployed in the east, and served as the operations and training officer. The following year, I was selected to follow the Army Command and Staff College course.

[3] The LTTE had cut the water supply to a part of the Eastern Province, and at this point the army launched a full-scale attack to retake the sluice gates and secure the water supply.

[4] Bruce I. Gudmundsson, *Stormtroop Tactics: Innovation in the German Army, 1914–1918* (Westport, Conn.: Praeger, 1989).

[5] This map depicts an important part of the final campaign to defeat the LTTE insurgency. The blue arrows indicate the advance of Sri Lankan military forces along multiple lines of thrust. The place names and dates indicate when and where the SRA captured LTTE-occupied areas.

The Use and Misuse of Influence in Counterinsurgency

MAJ Daniel Pace, US Army

In 2007, the US military was heavily invested in the war in Iraq. Following the initial success against the regular Iraqi army, the American war effort became mired in counterinsurgency operations against the numerous criminal and insurgent groups that rose to fill the power vacuum left in the wake of Iraqi president Saddam Hussein's fall. Faced with the decision to pull out altogether or to double down on US involvement, the George W. Bush administration opted for the latter course and sent an additional 30,000 troops into Iraq, in what was called "the surge." These troops were tasked with establishing security and providing breathing space for the budding government of Iraq to establish control over the country. In March 2007, my platoon—1st platoon, Charlie Company, of the 1st Squadron, 4th US Cavalry, 1st Infantry Division—deployed as part of this effort. Over the course of 15 months, we were able to establish effective security, services, and economic prosperity in our piece of Baghdad, Mahalla 838.[1]

Though our efforts were successful, in hindsight, many of our solutions were ad hoc and achieved only immediate security rather than contributing to long-term stability. In particular, while we succeeded in building influence with the Iraqi people in our area, the influence we built was between the population of Iraq and the US military—represented by my platoon—rather than between the population of Iraq and the government of Iraq. With a more thorough understanding of influence, particularly how it is generated and maintained, the US military could have been more successful in achieving long-term stability in Iraq. This article summarizes my platoon's activities in Iraq and analyzes those activities through the lens of an academic understanding of the concept and application of influence to describe how we built influence with the population of Mahalla 838, what the effects of the influence campaign were, and how counterinsurgency campaigns might improve on our performance in the future.

IN HINDSIGHT, MANY OF OUR SOLUTIONS WERE AD HOC.

Mahalla 838

Mahalla 838 was a heavily Sunni neighborhood in the center of Baghdad. At the time of the US invasion in March 2003, the population was well educated and included many high-ranking technical officials from the Saddam Hussein regime, including the deposed president's cardiologist, the head of the Iraqi Dental Association, and numerous retired senior military officials. The mahalla functioned through a combination of *Gemeinschaft* (the local community)—led by a number of traditionally influential people with strong tribal ties and strengthened by the homogeneity of the Sunni population, which provided a degree of social consensus—and *Gesellschaft* (the larger society), which consisted of the generally rational system of laws constructed and enforced by the Ba'ath party government.[2] Basic necessities in the community were provided by a dual system: partly official and partly unofficial. While the distribution of many important goods was managed by a system of government-issued ration cards, locally owned shops provided the majority of the population's other necessities.

Utilities were provided by the government through a well-developed, government-controlled infrastructure.

Rebuilding the Mahalla

The US invasion upset this balance between the official and the *ad hoc* providers, and unraveled the existing system. Within a few weeks, the Ba'ath party's mechanisms for control of the population vanished. Based on conversations we had with local residents, the basic community-level structure continued to function for a while, but as various insurgent and criminal organizations gained power in Iraq between 2004 and 2006, the community began to break down. Families with the means to leave—often the wealthiest and most influential—did so, and former government employees in a wide variety of fields, from electrical engineers to army generals to dentists, were either banned from further government service by the US de-Ba'athification mandate or fired by the new Shi'a-dominated Iraqi government. US forces patrolled the neighborhood on occasion but lacked sufficient presence and local involvement to gain any influence over the population. Perhaps because the population was largely Sunni, the reorganized Iraqi government mostly ignored the mahalla's needs, except to station a national police unit (entirely Shi'a) at the north end. This police unit spent little time patrolling the area but would fire indiscriminately into the neighborhood whenever they were attacked by the ever-increasing number of hostile Sunni insurgents. Thus, the police had only limited, coercive influence over the population.[3]

AS CRIMINAL ORGANIZATIONS GAINED POWER, THE COMMUNITY BEGAN TO BREAK DOWN.

This was the situation in the mahalla when my platoon arrived in March 2007. Because of a lengthy pre-deployment education program based on the US Army's then-newly published counterinsurgency field manual, the platoon had a basic understanding of population-centric warfare.[4] To secure the mahalla, the platoon first had to connect with the people and separate them from the insurgents. This required an influence campaign.[5] The strategy we used evolved over a few months, but by June it was clear that, if we were to complete our mission, the campaign would have to combine the restoration of essential services, the establishment of security, and intimate knowledge of the population.

But how could this be accomplished? Despite pressure from senior US military leadership to better integrate Sunnis into civil structures, the Iraqi government largely continued to ignore the population of Mahalla 838. Electrical power, which was distributed by the government, was rarely provided to the neighborhood, and government distributions of propane—an essential commodity in Iraq—were suspiciously absent. The mahalla's people had by and large turned to the black market to fill these shortages, which drew them closer to the anti-US and anti-government elements of society. On the one hand, the traditional and rational authority structures were failing and had already lost the ability to influence the population. On the other hand, by exploiting scarcity and the neighborhood's welfare, insurgent and criminal elements were gaining influence over the people.[6] My platoon saw this lack of government support as an opportunity to establish a degree of influence over the population, but in hindsight, we failed to replace or augment the legitimate rational and traditional authority structures. Instead, we destroyed the existing black market organizations and replaced them with a scarcity- and welfare-driven influence organization of our own.[7]

With money from a specially designated fund, we procured and distributed propane and electrical generators. While we made no conscious decision to

During the summer of 2007, Mahalla 838 was dangerous to both US and Iraqi government forces because a number of Sunni insurgents operated freely there. One of the techniques employed against us was the house-borne improvised explosive device (HBIED). While effective at killing coalition forces, the technique alienated many of the people in the mahalla, since they were killed by the attacks more often than we were. As our influence campaign progressed, these attacks became less frequent, and stopped altogether by the winter of 2007/2008.

838 Black Market Electrical Generator

When the government stopped providing electricity to the mahalla after the invasion, Iraqis began setting up their own generators and selling power to the population. The generators were poorly maintained, inefficient, and dangerous, but provided a great deal of influence to the owner. This generator caught fire and burned down during our tour.

US-Purchased, Locally Owned Generator in 838

Recognizing the influence gained by providing essential services, we provided these generators to friendly local entrepreneurs through the microgrant program. This provided the population with electricity and provided us with a friendly, influential, local business owner with a vested interest in keeping the mahalla safe and prosperous.

CERP-Funded Playground

This playground was another Commander's Emergency Response Program (CERP) project. Dr. Mo mentioned that the children of the mahalla had not been able to play anywhere safely for several years and recommended building a few playgrounds. They were very popular. We hired friendly local contractors to do the work.

US-Hired Sunni Security Personnel in 838

As part of the Sons of Iraq initiative, we hired local young men to provide security in Mahalla 838. While our intent was to eventually integrate them into the local Iraqi National Police unit, we were never successful in doing so, since there was resistance to integration from both the local personnel and the government.

Mahalla 838

The general atmosphere of the mahalla

apply Malcolm Gladwell's model of social influence, our funds were naturally channeled through the most effective "connector" in the mahalla, a locally influential man named Dr. Mo.[8] As a connector, Dr. Mo had a knack for understanding who could do what and for connecting us with willing and capable local businessmen, as well as reliable sources of information about local criminals. Over the course of six months and with Dr. Mo's assistance, the platoon induced compliance with our program through a combination of deliberate coercion and enticement.[9] We gained a large degree of influence over key figures in the mahalla, arrested or killed enough local criminals to virtually eliminate attacks, and employed a large percentage of the population in a series of local improvement and security projects.[10] At the time, we regarded this strategy as a success, but in retrospect, there was a trade-off for the gains we made that ultimately undermined stability in our area and insofar as the same strategy was followed elsewhere, in the Sunni areas of Iraq as a whole.

A Post-Surge Vacuum

Due to the difficulty of overcoming sectarian tension between the Sunni population and the Shi'a government, we never integrated the independently functioning community we had developed into the legal Iraqi governmental system. The Shi'a police were nominally involved in security, but in reality, the bulk of the police work was conducted by either the platoon or the Sunni security forces we trained and paid. This undermined one legal method of government population control. Additionally, by creating local Sunni sources of scarce, traditionally government-supplied products, we removed the government's second means of gaining influence over the population: the provision of welfare.[11] Removing these links to the government ensured that when US forces departed, we left an influence gap.

TO SECURE THE MAHALLA, THE PLATOON FIRST HAD TO CONNECT WITH THE PEOPLE.

Faced with the reality of an often hostile Shi'a government and left suddenly without US forces to serve as a source of influence and stability, the population of Mahalla 838 likely felt abandoned and isolated. It is not difficult to imagine, especially given the presence of an internally loyal Sunni security force, that a large number of residents would have been willing to abandon the Iraqi government for an organization with more cultural overlap, such as the Islamic State (ISIS). It is possible that some of the residents of Mahalla 838 are fighting with ISIS today.

In retrospect, it is clear that the members of my platoon should have used our ability to create influence differently. Given the initial hostility between the population and the new government, it was necessary for us to secure influence over the population ourselves, but in the last six months of the deployment, with security and prosperity largely restored, we should have made a concerted effort to strengthen the mahalla's ties to the government. Restoring the link between the Sunni leaders of the mahalla—both the traditional sources of authority and the new managers of scarcity that we created—and the legal Iraqi government would have worked toward long-term stability rather than against it.[12] By tying the economic structures we developed to corresponding structures at the regional level, we could have enabled the local elements of the Iraqi government to use welfare as a source of influence, and by tying our security structure directly to the national police, we could have enabled the Iraqi government to begin the long process of encouraging first compliance and then conversion to its point of view in our small piece of Iraq.[13] Had our unit been more successful at this process, and had the hundreds of other US units conducting the same mission across Iraq achieved a similar kind of success, it is possible we could have helped prevent the current Iraqi civil war.

A Lesson to Be Learned

In future counterinsurgency campaigns, the US military must learn from these mistakes. When working through a partner-nation government, US military leaders must remember that while gaining influence over the population is important, *the source of the influence is equally important*. Influence built between US forces and the population is not the same as influence built between the population and the government, and long-term stability in a fragile country requires the latter, not the former. In the future, US policymakers and commanders must ensure that the partner-nation government is seen as the primary provider of security, economic opportunity, and welfare, especially in areas where the population does not initially support the government or its policies.[14] Conducting these influence campaigns will be difficult, but numerous scholars have studied this problem and written useful works about their findings and recommendations.[15] During the conduct of the campaign, metrics must be developed to track government influence over the population, and commanders must be willing to accept the immediate tactical risk inherent in the relatively long process of allowing the partner-nation government to develop influence, rather than the commanders' developing unilateral influence themselves. While maintaining unilateral influence makes operations easier for US forces in the short term, it ultimately undermines US interests in the region. Without influence, the partner-nation government will be unable to effectively control its population, an outcome that discourages regional stability and will ultimately result in future conflicts. ❖

ABOUT THE AUTHOR

MAJ Daniel Pace serves in the US Army Special Forces.

NOTES

[1] A *mahalla* is the Iraqi word for a subsection of the city, equivalent to a district. The mahalla is used by the Iraqi government as a unit of population division, and the number is included on all official census, identification, and ration card documents.

[2] Francis Fukuyama, *The Great Disruption: Human Nature and the Reconstitution of Social Order* (New York: Free Press, 1999); Max Weber, *The Theory of Social and Economic Organization* (New York: Free Press, 1947), 325–58.

[3] The facts presented in this paragraph come from my personal experience in Mahalla 838. Over the course of 15 months, I interviewed hundreds of citizens of the area, including the members of the police unit itself, during census data collection and other counterinsurgency operations. This paragraph represents an aggregate of the information gathered during those interviews.

[4] Headquarters, Department of the Army, *Counterinsurgency*, FM 3-24/MCWP 3-33.5 (Washington, D.C.: HQ, Dept. of the Army, December 2006): http://usacac.army.mil/cac2/Repository/Materials/COIN-FM3-24.pdf

[5] An influence campaign is a series of planned actions to affect the behavior of a target population with the intent of causing that population to support the influencer's political objectives. See Kim Cragin and Scott Gerwehr, *Dissuading Terror: Strategic Influence and the Struggle against Terrorism*, MG-184-RC (Santa Monica, Calif.: RAND Corporation, 2005), 14: http://www.rand.org/pubs/monographs/MG184.html

[6] Anthony R. Pratkanis, "Social Influence Analysis: An Index of Tactics," in *The Science of Social Influence: Advances and Future Progress*, ed. Anthony R. Pratkanis (New York: Psychology Press, 2007), 56.

[7] Alexus G. Grynkewich, "Welfare as Warfare: How Violent Nonstate Groups Use Social Services to Attack the State," *Studies in Conflict and Terrorism* 31, no. 4 (2008): 350–70.

[8] In his model, Gladwell refers to personality archetypes as *connectors, mavens,* and *salesmen*, which work together to spread ideas throughout a population. The connectors, through their internal networks and innate likability, tie people together; the mavens investigate and share information on the topics that interest them; and the salesmen identify individuals' needs and persuasively recommend helpful ideas. According to Gladwell, this system spreads ideas quickly and effectively. Malcolm Gladwell, *The Tipping Point* (New York: Little, Brown, and Co., 2000), 33–88.

[9] Dr. Mo (a pseudonym) became very wealthy during our tour. From information I saw in 2011, he still seemed to be doing quite well.

[10] *Compliance*, in this case, is the objective of an influence campaign, which aims to alter a population's behavior without regard to its beliefs. See Cragin and Gerwehr, *Dissuading Terror*, 15–16.

[11] Grynkewich, "Welfare as Warfare"; Pratkanis, "Social Influence Analysis," 56.

[12] Weber, *Theory of Social and Economic Organization*, 325–58.

[13] *Conversion* is the influence objective that seeks to produce the desired behavior in a population by changing its underlying beliefs. See Cragin and Gerwehr, *Dissuading Terror*, 19.

[14] Grynkewich, "Welfare as Warfare." The fact that the United States needs to carefully evaluate whether the government of a post-conflict partner-nation will be willing to or capable of governing in a manner that supports US interests is another matter entirely. While the answer is essential to the outcome of a US influence campaign, this issue is outside the scope of this paper.

[15] A few of the most practical recommendations are Grynkewich's "Welfare as Warfare" for the use of welfare to win popular support; Pratkanis's index of tactics on influence in "Social Influence Analysis"; and Gladwell's *The Tipping Point* on connectors, mavens, and salesmen.

The Dark Side of Drones: Implications for Terrorism

CPT Benjamin Seibert, US Army

In recent years, rapid advancements in drone technology have raised questions, not only at the tactical level but also at the academic level, about the potentially revolutionary ways drones will affect how terrorists operate and what such technology will be capable of. As historian Walter Laqueur warned, "Society has … become vulnerable to a new kind of terrorism, in which the destructive power of both the individual terrorist and terrorism as a tactic are infinitely greater."[1] This article discusses some of the likely effects that drones will have in this world of postmodern terrorism by analyzing the capabilities of drones, their appeal to terrorists and terrorist organizations, and the way drones can achieve the psychological impact that terrorists desire.

Drone Capabilities

Before discussing what drones are capable of, it is first necessary to define what is meant by the term *drone*. The word is not an accurate representation of the machines, but it has been adopted in mainstream communications to broadly denote a constantly changing form of mobile technology. For example, the word *drone* has been used by the media to refer to airplanes, rotary-wing aircraft, boats, and wheeled vehicles when these machines are unmanned and remotely operated. More commonly, however, the word *drone* refers to unmanned aerial vehicles, or UAVs. These are any aircraft, fixed- or rotary-wing, capable of operating without a pilot on board. Fixed-wing UAVs range from the recreational model airplane to larger military reconnaissance and attack aircraft. The Predator and Reaper UAVs used by the United States are two examples of this latter military craft. Rotary-wing UAVs range from the small, lightweight quadcopter to a full-sized helicopter operated by remote control. Quadcopters are commercially available and are most commonly used to take aerial photographs, while larger unmanned helicopters have a wide variety of industrial, commercial, and military applications. For the purpose of this article, the word *drone* is used specifically to refer to these fixed- and rotary-wing UAVs.

What are these drones capable of? A foiled 2011 terrorist plot to attack the US Capitol building and the Pentagon provides an example of a model airplane's capabilities. Analyst Marc Goodman writes that the planner of the attack, Rezwan Ferdaus, "wanted to use 1/10 scale models of the F-4 Phantom fighter aircraft in the attack, noting that they can be purchased fully assembled with Global Positioning System (GPS) navigation equipment, were capable of traveling up to 160 mph, and could carry a payload of 10 to 12 pounds."[2] Goodman goes on to note that some model airplanes are capable of carrying up to 33 pounds and that bombing capabilities are also commercially available.[3] "For only $16.95 anyone can buy the Chinese-made Quanum 'bomb' drop system for remote control aircraft—either fixed- or rotary-wing. This 23.5 centimeter long case splits open to release a 103 gram payload of the user's choice."[4] The system is available for purchase on Amazon today, and although the weight capacity is small, the technology is simple and can be upgraded to accommodate larger aircraft with

"FOR ONLY $16.95 ANYONE CAN BUY THE CHINESE-MADE QUANUM 'BOMB' DROP SYSTEM."

heavier payloads. This recalls the infamous quote from the 1966 film *The Battle of Algiers*, when the captured terrorist leader Ben M'Hidi is questioned about the morality of using baskets to deliver explosives. He responds, "Of course, if we had your airplanes, it would be a lot easier for us. Give us your bombers, and you can have our baskets."[5]

Thus, the presumed technological limitations of terrorist organizations are becoming increasingly irrelevant, and weapons that were the monopoly of advanced militaries are becoming accessible to anyone. Although significant limitations remain, the technology is catching up at an alarming rate. Ferdaus is not the only recent example. In 2013, German officials conducted a raid on a group of individuals thought to have been radicalized by Islamic extremism and discovered model airplanes that were reportedly capable of carrying enough explosives to destroy a commercial building.[6]

The Payload

The problem of acquiring and preparing explosives for use remains a gap between the desire and the deed, however, and the astute observer will note that in these previous two examples, the would-be terrorists possessed drones capable of delivering explosives, but not the explosives themselves. Marc Sageman of the Foreign Policy Institute remarks that although instructions for creating explosives are available online, the actual production of them is extremely dangerous.[7] Sageman warns, "Law enforcement authorities should not become complacent; the number of wannabe terrorists remains large, and by the law of averages some are bound to be smart and bold enough to pull off an attack."[8] The 2013 Boston Marathon attack and the 1995 Oklahoma City bombing are two examples from the United States in which terrorists did beat the law of averages and carried out lethal attacks using commercially available resources. Regulating the sale of commercial components after they have been successfully used, as was done with chemical fertilizers after the Oklahoma City bombing, however, will not prevent future attacks that use different means. As psychologist John Horgan notes, "Easily accessible components are the primary ingredients of today's terrorist bombs."[9] Terrorists will continue to adapt and create explosives with what is available to them, and the internet will continue to provide innovative techniques to assist in the process. Sageman goes on to warn that "these new [terrorist] groups ... become dangerous when they hook up with a trained bomb maker."[10] Joining forces with an experienced bomb maker no longer has to happen in a distant terrorist training camp but can now be as simple as downloading an instructional video from the internet, and anyone dedicated enough to risk it can use this knowledge to create his own explosives. It becomes clear that terrorists, especially those working in countries where explosive components are not tightly regulated, are able to acquire all the necessary ingredients to carry out a bomb attack, with drones as the delivery vehicles.

Rotary-Wing Aircraft

Among modern drones, helicopter-style drones deserve special attention due to their extreme maneuverability. A video posted on YouTube by a group of researchers from the University of Pennsylvania demonstrates the impressive aerial maneuvers of quadcopter drones (called *quadrotors* in the video). These quadcopters do midair flips, fly through rectangular openings with a clearance of less than 3 inches on each side, and attach to fixed surfaces (by means of Velcro pads).[11] Combined with GPS technology to guide the aircraft to within one meter of a target and laser range-finder devices that instantly identify precise grid coordinates from over 3,000 feet away, one could potentially land a quadcopter almost anywhere. This technology could be used for high-profile attacks such as assassinations of leading government officials. In 2013, for example, an activist group was able to land a quadcopter drone directly in front of German Chancellor Angela Merkel as she spoke before a large crowd in Dresden. The entire video of this event can be seen on YouTube.[12] The

most alarming aspect of the event is that the ground-based security forces were completely helpless to prevent the drone from landing in front of the podium where Merkel was speaking. The chancellor herself seemed uncertain as to what actions should be taken. Despite a small lift capacity, commercially available quadcopters can carry enough explosives to seriously harm or kill a person. The incident in Dresden clearly demonstrates both the ability of drones to bypass traditional security measures and the unpreparedness of security forces to counter such a threat.

Another video posted by the University of Pennsylvania research group demonstrates the ability of 20 quadcopters to fly in formation to create a swarming effect.[13] While one explosive-laden quadcopter might not reach its target or might cause only minimal damage, a swarm of the aircraft could cause serious harm. Even without explosives, a swarm of quadcopters could be aimed at the engines of a commercial airliner and cause it to crash. Flocks of birds are already known to cause serious harm if they are sucked into a jet engine, but the metal of a quadcopter drone would be much more devastating. The quadcopters in the University of Pennsylvania videos are state-of-the-art UAVs with proprietary software operating in a controlled laboratory setting, and could not currently be used outdoors with the same precision. But the technology to move these quadcopters out of the lab is being developed, and we should expect commercial drones to have these capabilities in the near future. What is more, as with all technology, costs and prices will fall dramatically as the devices are commercialized.

GPS technology allows for attacks against stationary targets, but technology is available to accurately strike moving targets as well. The Google Lily is an autonomous quadcopter drone—currently being marketed to skiers, surfers, and extreme sports enthusiasts—that uses GPS technology to record video of someone who is wearing a synchronized tag in an armband.[14] Its current range from camera to tag is only 100 feet, but a commercially available antenna could greatly increase this distance. In addition, the Google Lily drone does not require line-of-sight with the tag to operate. Someone with violent intent could surreptitiously place one of these tags, which are small, inconspicuous, and undetectable by current security measures, on the intended target, and the drone, carrying a timed or remote-controlled explosive, could then be programmed to fly to the location of the tag. This would effectively turn a drone with Google Lily technology into a guided missile. If the tag is carried onto an aircraft, the drone could have the same effect as a surface-to-air missile, most potentially during takeoff or landing (to mitigate the greater speed of the airliner). This is one example of how commercially available products are further bridging the gap between the previously inaccessible technologies of modern militaries and the assets available to terrorist organizations.

Appeal to Terrorists and Terrorist Organizations

Up to this point, the discussion has focused on the tactical capabilities of drones and how they could be used to conduct terrorist attacks—information that is relevant to those with the day-to-day responsibility of defending against and preventing terrorist attacks. This section looks at why the use of drones is appealing to terrorists and terrorist organizations.

The Benefits of Precision

Precision targeting, made possible through the use of GPS, is appealing to terrorist organizations for the same reason it is appealing to any military: it not only allows the attacker to precisely hit the intended target, but assuming accurate targeting intelligence in the first place, also equally prevents an accidental strike on an unintended target. Just because a terrorist organization uses violent means against civilian targets does not mean that it is immune from the backlash that results when the wrong

people are killed. Horgan comments that "a myth about terrorist violence in the popular media is that it is often uncontrolled, frenzied, and vicious. While terrorism is often vicious, it is rarely frenzied and uncontrolled; when it is, it runs the risk of losing significant support."[15] The history of the Irish Republican Army (IRA) provides two examples, both from 1993. In the first incident, as the IRA escalated its attacks against increasingly aggressive British Loyalists, an IRA cell targeted some local paramilitary leaders who were believed to be meeting on the upper floor of a commercial fish shop on Shankill Road in Belfast.[16] The attackers intended to plant a bomb with a timed fuse at the location of the meeting, but it detonated prematurely and killed nine civilians. In the second incident, a bomb that detonated in a Cheshire shopping area killed "two young boys and prompted significant protest in England and Ireland."[17] These botched attacks brought widespread condemnation down on the IRA during a time when gaining public support was vital to the organization. The attacks failed for two reasons: the unpredictability of the explosives and the inadequate means the group used for delivering the explosives to the intended targets. The exact reason why the explosive on Shankill Road detonated prematurely is unknown, but it was probably due to the use of a timed fuse—a common tactic of the IRA. Programming a bomb to detonate based on exact GPS location coordinates instead of relying on a timer creates a more reliable precision weapon and avoids the backlash that results from killing unintended targets.

DRONES ARE MUCH EASIER TO ACQUIRE AND TRANSPORT THAN CONVENTIONAL WEAPONS.

Another reason why drones appeal to terrorists and terrorist organizations is that they are much easier to acquire and transport than conventional weapons. If a dedicated individual can overcome the obstacle of creating a reliable explosive component, then a terrorist attack can be conducted almost anywhere. A major strength of the US intelligence network has been its ability to intercept terrorists as they attempt to acquire conventional weapons. This was demonstrated by a 1982 FBI sting operation that uncovered an IRA weapons smuggling ring (whose shipment, incidentally, included a remote-controlled model airplane),[18] as well as multiple operations since the 9/11 terrorist attacks in which FBI agents posed as arms dealers to bring down terror cells in their infancy.[19] As a result, conventional military-grade weapons have been difficult for terrorists in the United

States and Western Europe to acquire. Drones, on the other hand, are already available online, with more advanced models appearing every year.

Finally, drones allow attacks to be conducted anonymously and therefore increase the probability that an attacker will not only survive the attack but also avoid capture. This lessens the recruitment burden for terrorist networks, allows attackers to perfect their tactics by participating in multiple attacks, and appeals to those who prefer to pursue violence as a lifestyle choice rather than as a sacrificial duty. A drone provides this anonymity because it takes the burden of delivering the explosives away from the attacker, who otherwise risks being filmed by security cameras or identified by witnesses, or is expected to die, and places it on a machine. In addition, a drone could be launched from a concealed location by means of a timer and then fly to its intended target using GPS, long after the perpetrators have left the area. It is possible that an attacker would have enough time to fly to a foreign country and watch the results of the attack from abroad. The explosive could even be configured to detonate once the drone reaches a pre-configured grid coordinate. This process would require slightly more technical expertise but is well within the capabilities of many amateur hobbyists.

Regulation Lags behind Technology

The lack of effective government regulation is another appealing aspect of using drones to conduct terrorist attacks. Currently, fixed-wing drones can be modified by amateur hobbyists to carry heavier payloads like explosives, but they are not as effective as rotary-wing drones at precision targeting. The rotary-wing drones available to the public are still relatively small and would require significant upgrades to increase their lift capacity. While hobbyists have gained a lot of experience working with fixed-wing drones, rotary-wing technology is still beyond the skills of most amateur enthusiasts. Larger rotary-wing models, however, are being widely developed in the commercial sector and include drones with a lift capacity of up to 70 pounds.[20] The use of such drones is still heavily regulated, but corporations are actively lobbying to expand their use. This lobbying has already resulted in a presidential memorandum, issued in February 2015, that called for "a plan to safely integrate civil UAS [unmanned aircraft systems] into the National Airspace System by September 30, 2015."[21]

"MUCH OF THE RUSH TOWARD DRONE ADOPTION IS HAPPENING IN THE SHADOWS."

In reality, this regulation is already behind the times. Many US companies have been experimenting with the technology without waiting for Federal Aviation Administration (FAA) approval. "The FAA's ban on commercial drone use means that much of the rush toward drone adoption is happening in the shadows."[22] Furthermore, "because the FAA lacks the manpower to police the entire national airspace at all times, many companies get away with flying their commercial drones until someone brings it to the agency's attention, at which point a cease-and-desist letter goes out."[23] This cumbersome progression toward FAA regulation brings up two alarming aspects of the spread of commercial drone use. The first is that, in the absence of regulation, the use of these aircraft has already fostered a secretive distribution network that could allow a large rotary-wing drone to be sold to terrorist organizations either directly or through intermediaries. The second point is that the slow pace of FAA approval for commercial drone use has brought to light the agency's inability to effectively monitor the country's vast domestic airspace. Even if full coverage were possible, many of these aircraft are still small enough that radar technology might mistake them for large birds or miss them entirely.[24]

The United States is not alone in this struggle to regulate its airspace. The Birmingham Policy Commission of the United Kingdom published a report in 2014 noting that, "in the wrong hands, RPA [Remotely Piloted Aircraft] could become a dangerous and destabilizing delivery system. We doubt how far the proliferation of the various enabling technologies ... can be controlled."[25] Findings from this report stress the urgent necessity to regulate RPA use, publicize and enforce existing laws, and alert the Ministry of Defence and law enforcement agencies of the potential use of RPAs for criminal or terrorist activity. The report also emphasizes that the United Kingdom is not in a position to influence the international regulation of RPAs, due to their widespread proliferation on the global market.[26]

India is another country that has had considerable difficulty regulating the use of drones. Similar to the slow progress made by the FAA in the United States, India's Directorate General of Civil Aviation (DCGA) has not effectively regulated the use of small recreational or commercial drones. Analyst Nidhi Singal writes that "the long wait for the DCGA to issue guidelines has not helped ... as drones have become a common sight despite the ban."[27] If countries with established institutions for the regulation of airspace are incapable of regulating drone use, then it is easy to imagine that areas of the world racked by terrorist violence, such as Nigeria, Syria, or the Levant, are highly susceptible to the threat of drone terrorism. Even without the technical expertise required to turn a drone into an explosive-carrying aerial platform, the devices could still be used non-lethally to conduct aerial reconnaissance. Terrorist groups such as Boko Haram, for instance, would greatly benefit from deploying drones to learn for certain whether security forces were present before the group conducted an attack, or to give an early warning of attacks against its own sites.

THE INTERNET PROVIDES A FORUM ON THE TECHNICAL REQUIREMENTS FOR DRONE ATTACKS.

Online Expertise

The internet provides an excellent, anonymous forum for instructing would-be terrorists on the technical requirements for drone attacks. Sageman elaborates on the growing trend of instructing terrorists online: "The growth of the Internet has dramatically transformed the structure and dynamic of the evolving threat of global Islamist terrorism by changing the nature of terrorists' interactions. ... The average age of terrorists arrested in Europe and Canada from 2005 onward has dramatically decreased."[28] According to terrorism specialist Alan Krueger, "88% of the time, terrorist attacks occur in the perpetrator's country of origin," and "the perpetrators tend to be middle class or upper middle class."[29] These characteristics are ideal for recruiting someone who would be inclined to use a drone for a terrorist attack. A teenager or 20-something who is already comfortable learning from the internet could learn to configure a drone, and many youth are already interested in and excited about recreational drone use. Most importantly, the recruit could live and work in proximity to the target, and all of the necessary equipment is available for purchase and affordable to anyone in the middle or upper classes. Sageman also notes that, as demonstrated by al Qaeda, the trend of recruitment also favors the use of the internet: "The prospective mujahed took the initiative rather than waiting for someone to ask him to join the jihad. Instead of a top-down process of the terrorist organization trying to recruit new members, it was a bottom-up process of young people volunteering to join the organization."[30]

The desired end of this process is to have such groups or individuals act independently, using their own resources to conduct terrorist attacks in line with the overall goals of the organization. Jason Burke, an investigative journalist, describes the dangers of this recruitment strategy in his analysis of the 2004 Madrid terrorist attacks. "The attackers were not experienced Al-Qaeda operatives parachuted in from overseas as initially suspected, but were first-generation Moroccan and Tunisian immigrants who had been living in Spain for some time. ... Spanish intelligence and police investigators concluded that the bombers were acting largely on their own."[31] Two of the most disturbing aspects of the Madrid attacks are that the targets were chosen without the approval of the central al Qaeda leadership and that the attacks were not controlled to meet the goals of the organization. This statement may seem ludicrous considering the violent nature of al Qaeda and the nature of its historical targets, but as Burke writes, "Killing crowds of ordinary commuters on their way to work was far harder to sell to potential sympathizers and thus risked delegitimizing the cause as a whole."[32] He also notes that the bombers did not embrace the traditional martyrdom favored by al Qaeda.[33] These attackers would likely have conducted follow-on attacks if they had not been quickly detained. The implication is that while al Qaeda is bad, individuals who become self-radicalized and choose targets at random have the potential to be much worse and even more difficult to stop. Armed with drones, these self-radicalized groups or individuals would have the capacity to conduct extremely lethal attacks, evade capture, and carry out additional attacks essentially at will.

The Psychological Impact of Drones

This article has discussed the potential effectiveness of using drones to conduct terrorist attacks, but their effectiveness alone does not make them appealing. Drone strikes must also achieve the desired psychological goals of the terrorist organization or individual. Horgan writes, "When we consider Al-Qaeda's additional expectations of political destabilization and galvanization of extreme Islamic sentiment against Western interests, the allure of terrorism as a psychological strategy and psycho-political tool to otherwise disenfranchised extremists becomes apparent."[34] Although al Qaeda is only one terrorist organization among many, the group's psychological goals are generally similar to other terrorist groups throughout history; only the ideology and opponent change. Therefore, Horgan's comments are relevant to the question of whether drones achieve the goals of terrorist organizations in general.

WITH DRONES, SELF-RADICALIZED GROUPS WOULD HAVE THE CAPACITY TO CONDUCT EXTREMELY LETHAL ATTACKS.

Achieving Political Destabilization

The most effective tactics used by terrorists—aside from the unprecedented use of hijacked airplanes as guided missiles on 9/11—have largely been ground-based. They have involved attacks with small arms, infiltration to emplace concealed explosives, and suicide missions in which explosives were carried either on an individual or in a vehicle. The targets for many of these attacks have been public places where, seemingly, the victims were randomly selected and had no connection to the police, military, or government. Horgan explains why such attacks are highly effective at achieving the psychological goals of terrorists.

> The fact that the apparently random victim of this kind of violence is arbitrarily selected to die shocks and sickens people, and this unexpectedness leads to personalization of events even at an individual level. It is seen as terrible and unjust, the way in which anyone, particularly non-combatant bystanders, can be at the wrong place at the wrong time and be killed in the name of some cause that the victim has possibly never even heard of.[35]

"Terrorist violence," Horgan points out, "is predicated on the assumptions that apparently random violence can push the agenda of the terrorist group onto an 'otherwise indifferent public's awareness,' and that, faced with the prospect of a prolonged campaign of terrorist violence, the public will eventually opt for an acceptance of the terrorists' demands."[36]

To date, al Qaeda and other radicalized Islamist organizations seem to have achieved many of their psychological aims. They have conducted horrific attacks and awakened public awareness of their existence, but they have not yet achieved their overall goal to, as former US deputy national security advisor (and current CIA director) John O. Brennan described it, "terrorize us into retreating from the world stage."[37] Horgan suggests why this goal has not been met: "That a constant state of dread cannot be maintained forever is illustrated through a slow habituation of the terrorist audience to the situation. For the terrorist, audience acclimatization poses problems: if the audience adapts to tactics, the terrorist's influence diminishes."[38] This readiness to adapt is where the Western public currently stands with regard to terrorism. Due to the persistent ground-based threat, security measures have been upgraded in response. For example, a 2008 Government Accountability Office (GAO) report lists several physical security measures that US embassies have implemented in recent years, as seen in figure 1.[39]

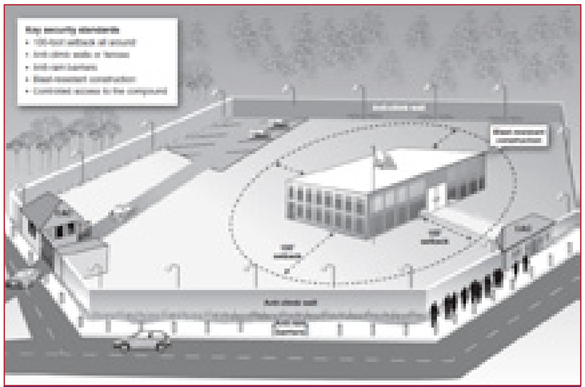

Key security standards
• 100-foot setback all around
• Anti-climb walls or fences
• Anti-ram barriers
• Blast-resistant construction
• Controlled access to the compound

Figure 1: Key security measures at a notional embassy compound

These include placing buildings at a specified "standoff" distance from main roads, anti-climb walls, anti-ram barriers, and blast-resistant building construction that includes shatter-proof glass. The GAO has also recommended that US embassies be relocated from dense urban areas to areas on the outskirts of capitals that can accommodate the recommended security measures. In this regard, the psychological aim of al Qaeda to reduce US influence abroad has been effective. Instead of occupying a prominent place in the center of foreign political power, many US embassies have adopted a bunker-like mentality that serves as a symbolic limitation to their international prestige and a physical limitation to American personnel's interactions with the public. This overly cautious approach paints the United States as being fearful and out of touch with both foreign politics and daily life.

THE PSYCHOLOGICAL AIM OF AL QAEDA TO REDUCE US INFLUENCE ABROAD HAS BEEN EFFECTIVE.

Nevertheless, al Qaeda and similar Islamist terrorist groups have not achieved all of their psychological goals because the "audience acclimatization" that Horgan described is ongoing. Prominent domestic sites in the United States and other Western countries have adopted similar precautions to those found protecting embassies in domestic defense of terrorist attacks. As a result, people in major Western countries are regaining the sense of security that they lost on 11 September 2001, 11 March 2004, and 7 July 2005, because their perception of security is reinforced every day as they navigate through metal detectors, bag searches, anti-ram barriers disguised as decorative flower pots, and a myriad of other defensive measures. Whistleblower revelations concerning the US National Security Agency's highly intrusive surveillance of private citizens should be alarming to a liberal democracy, but instead the revelations have further reinforced many Americans' sense of security and thereby reduced the psychological influence of terrorism.[40] To regain the initiative, terrorists must conduct a successful attack that bypasses these security measures in such a way that the public will no longer feel they are protected from seemingly random acts of violence.

Drones may provide the means for terrorists to regain the initiative and reach their psychological goals of destabilizing Western societies. The glaring gap in all of the above-mentioned ground-based security measures is that they do not provide protection from aerial attacks by anything smaller than a manned conventional aircraft, a weakness easily exploited by drones. This problem was publicly demonstrated in two separate events in early 2015, when a piloted gyrocopter and a rotary-wing drone embarrassed the US Secret Service by landing on the White House lawn.[41] As technology improves, it is likely that the semblance of security that has been recreated through expenditures of vast resources and time will be destroyed the moment a successful drone attack forces the public to realize, once again, that they are not as safe as they thought they were.

Galvanizing Extreme Islamist Sentiment

Perhaps nothing has been more controversial in the United States' current fight against radical Islamist terrorism than the use of drone strikes. Political scientist Avery Plaw writes that "between June 2004 and the end of 2011, the CIA is widely reported to have carried out 300 covert drone strikes in Northwest Pakistan that have killed more than 2000 people, some of whom were civilians."[42] In recent years, this program has been extended and drones have now been used in Somalia, Afghanistan, Pakistan, Yemen, and most recently, in the fight against ISIS. Plaw describes the parallel narratives that characterize the US drone program. On the one hand, John Brennan said regarding the US drone program in Pakistan, "For the past year there hasn't been a single collateral death because of the exceptional proficiency and precision of the capabilities that we've been able to develop."[43] The narrative adopted by the Pakistani press, on the other hand, is much different, as Plaw makes clear.

> The Pakistani daily, *Dawn,* reported in January 2010 that "of the 44 predator strikes carried out by US drones ... over the past 12 months, only five were able to hit their actual targets ... but at the cost of over 700 innocent lives. ... For each al-Qaeda and Taliban terrorist killed by US drones, 140 innocent Pakistanis also had to die."[44]

Whether the Pakistani press's numbers are correct is irrelevant. The Pakistani public and wider regional audience will undoubtedly believe local sources over statements made by Western officials. Claims of civilian casualties have also been made outside of South Asia and the Middle East. Social anthropologist Jeffrey Sluka commented that "the drone strikes have already caused well over a thousand civilian casualties, have had a particular affinity for hitting weddings and funerals, and appear to be seriously fueling the insurgency."[45]

DRONES HAVE BEEN CITED AS A MOTIVATION FOR TERRORISM BY THE ATTACKERS THEMSELVES.

The use of drones by the United States and the United Kingdom has also been cited as a motivation for terrorism by the attackers themselves, including the foiled 2010 Times Square bomber, Faisal Shahzad, a US citizen of Pakistani heritage.[46] US drone strikes have been a source of humiliating defeat for members of al Qaeda and other Islamist terrorists, but they have also been a source of great anger within the international Muslim community—an anger that terrorists can exploit. "Given the controversial use of drones by the US and UK in many parts of the Muslim world, the ability to strike at the homeland with such a device must be very attractive to many terrorist groups as the ultimate expression of a paradoxically symmetrical asymmetric warfare."[47] If terrorists could use drones against targets in the West, it would provide a psychological victory for their members and serve as a recruitment tool aimed at the citizens of countries targeted by drones. In addition, by citing US drone strikes as the reason for retaliation, such attacks might force apathetic Western populations to pay attention to the problems in their own governments' drone programs—and potentially motivate homegrown terrorists to take action.

To many people, the idea of drones as weapons may seem futuristic and within the grasp of only the most technologically advanced militaries of the world. Therefore, if a terrorist organization could effectively use drones, it would achieve instant legitimacy. Hezbollah has already realized this and began to incorporate drones into its arsenal as early as 2004. In 2012, Hezbollah operatives launched a drone from Lebanon that flew 35 miles into Israel and was shot down near the town of Dimona—the site of an Israeli nuclear complex.[48] This incursion into Israeli airspace was clearly a psychological victory for Hezbollah because it exposed the vulnerability of Israel's primary source of military power over its neighbors—its nuclear weapons. Although the Hezbollah drones lag behind those of Israel and the United States in sophistication, they do provide a powerful psychological tool for Israel's enemies. The rapid technological evolution of drones in the commercial market may greatly reduce this gap in capability between the drones of Hezbollah and the drones of the West in the very near future.

A TERRORIST ORGANIZATION THAT EFFECTIVELY USED DRONES WOULD ACHIEVE INSTANT LEGITIMACY.

Final Thoughts

This article describes the capabilities of drones, how they could be used to conduct terrorist attacks, and how they may become the ideal platform for terrorists to achieve their psychological goals. The question remains, however, whether it will take a successful drone attack before Western security agencies implement the changes necessary to counter this threat.

> While the challenge presented by drones as potential terrorist weapons is real and growing, this does not mean that nothing can be done to counter it. Various measures have been suggested as defenses against drone attacks, such as electromagnetic jamming, deeper perimeter defense of airports, physical barriers on buildings, and even high-powered fiber optic laser guns, but such measures will only be implemented if the threat from drones is acknowledged, debated, and acted upon.[49]

The article does not cover appropriate defenses against drone terrorism. Its purpose is to make clear that the use of drones is rapidly growing, their technological capacity is increasing, and the threat that they will become a tool for terrorism is real. Burke writes that prior to 11 September 2001, "no one had imagined terrorists ever using tactics like those that the hijackers were to adopt."[50] The intelligence community, he notes, admitted that "the nature of the threat was not 'understood' at the time ... 'due to a failure of imagination.'"[51] This failure of imagination continues to be a lethal weakness that will be exploited by terrorist organizations, which will constantly seek out new and more effective methods of attack. The rapid proliferation and technological improvement of drones may profoundly change the way terrorists conduct attacks and what they will be capable of accomplishing. ❖

ABOUT THE AUTHOR

CPT Benjamin Seibert currently serves as a foreign area officer in the United States Army.

NOTES

[1] Walter Laqueur, “Postmodern Terrorism: New Rules for an Old Game,” *Foreign Affairs* 75, no. 5 (1996): 35.

[2] Marc Goodman, “Attack of the Drones: Terrorist Use of Remote Controlled Aircraft,” *Jane’s Intelligence Review* 23, no. 4 (2011) (available by subscription): 1.

[3] Ibid.

[4] Ibid.

[5] *The Battle of Algiers,* directed by Gillo Pontecorvo (Italy: Rizzoli, 1966).

[6] “Islamist Raids: German Police Shoot Down Model Plane Terror Plot,” *Spiegel Online International*, 25 June 2013: http://www.spiegel.de/international/germany/german-police-suspect-remote-controlled-airplane-terror-plot-a-907756.html

[7] Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008), 140–41.

[8] Ibid., 141.

[9] John Horgan, *The Psychology of Terrorism*, rev. 2nd ed. (New York: Routledge, 2014), 18.

[10] Sageman, *Leaderless Jihad*, 140–41.

[11] “Aggressive Maneuvers for Autonomous Quadrotor Flight,” YouTube video, 1:26, posted by “TheDmel,” 21 May 2010: https://www.youtube.com/watch?v=MvRTALJp8DM

[12] “Merkel’s Dresden Drone Close Encounter: Drone Crashes in Front of German Chancellor Angela Merkel,” YouTube video, 1:00, posted by JewishNewsOne, 15 September 2013: https://www.youtube.com/watch?v=qKV6g47hgRs

[13] Alex Kushlayev, Daniel Mellinger, and Vijay Kumar, “A Swarm of Nano Quadrotors,” YouTube video, 1:42, posted by “TheDmel,” 31 January 2012: https://www.youtube.com/watch?v=YQIMGV5vtd4

[14] David Pierce, “Throw This Camera Drone in the Air and It Flies Itself,” *Wired*, 12 May 2015: http://www.wired.com/2015/05/lily-robotics-drone/

[15] Horgan, *Psychology of Terrorism*, 24.

[16] Jonathan Tonge, *Northern Ireland* (Cambridge, UK: Polity Press, 2006), 57.

[17] Ibid.

[18] For the story of the IRA weapons ring, see Warren Richey, “Roller Skates and Rifles: How IRA Group Tried to Sneak Arms out of US,” *Christian Science Monitor*, 18 January 1985: http://www.csmonitor.com/1985/0121/anor5.html

[19] Jessica Zuckerman, Steven P. Bucci, and James Jay Carafano, *60 Terrorist Plots since 9/11: Continued Lessons in Domestic Counterterrorism*, Special Report (Washington, D.C.: The Heritage Foundation, 22 July 2013): http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism

[20] “Our Unmanned Aerial Vehicle (UAV) Platforms,” Homeland Surveillance & Electronics LLC UAV, n.d.: http://www.hse-uav.com/platforms.htm

[21] “Presidential Memorandum: Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems,” The White House, Office of the Press Secretary, 15 February 2015: https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua . On 19 October 2015, the FAA announced plans to require all recreational drone operators to register their machines and said an online registry would be in place before Christmas. Craig Whitlock, “Federal Regulators to Require Registration of Recreational Drones,” *Washington Post,* 19 October 2015: https://www.washingtonpost.com/world/national-security/federal-regulators-to-require-registration-of-recreational-drones/2015/10/19/434961be-7664-11e5-a958-d889faf561dc_story.html

[22] Clay Dillow, “Get Ready for ‘Drone Nation,’” *Fortune,* 27 October 2014: http://fortune.com/2014/10/08/drone-nation-air-droid/

[23] Ibid.

[24] *Editor’s note*: For more on the practical limitations of radar in airspace defense systems, see Jamal Hussain, “The Phantom Raid,” in this issue of *CTX.*

[25] Birmingham Policy Commission, *The Security Impact of Drones: Challenges and Opportunities for the UK* (Birmingham: Institute for Conflict, Cooperation, and Security, University of Birmingham, 2014), 13: http://www.birmingham.ac.uk/Documents/research/policycommission/remote-warfare/final-report-october-2014.pdf

[26] Ibid., 77–78.

[27] Nidhi Singal, “Game of Drones,” Yahoo Finance India, 7 May 2015: https://in.finance.yahoo.com/news/game-drones-123524432.html

[28] Sageman, *Leaderless Jihad,* 109, 111.

[29] Alan B. Krueger, *What Makes a Terrorist: Economics and the Roots of Terrorism* (Princeton: Princeton University Press, 2008), 71, 77.

[30] Sageman, *Leaderless Jihad,* 110.

[31] Jason Burke, *The 9/11 Wars* (London: Penguin, 2011), 160.

[32] Ibid.

[33] Ibid.

[34] Horgan, *Psychology of Terrorism,* 12.

[35] Ibid., 14.

[36] Ibid., 12–13.

[37] “Remarks of John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, on Ensuring al-Qa’ida’s Demise—As Prepared for Delivery,” The White House, Office of the Press Secretary, 29 June 2011: https://www.whitehouse.gov/the-press-office/2011/06/29/remarks-john-o-brennan-assistant-president-homeland-security-and-counter

[38] Horgan, *Psychology of Terrorism,* 22.

[39] Government Accountability Office, *Embassy Security: Upgrades Have Enhanced Security, but Site Conditions Prevent Full Adherence to Standards*, GAO-08-162 (Washington, D.C.: GAO, 2008), 7: http://www.gao.gov/new.items/d08162.pdf

[40] According to a poll by the Pew Research Center, "a majority of Americans—56%—say the National Security Agency's program tracking the telephone records of millions of Americans is an acceptable way for the government to investigate terrorism." "Majority Views NSA Phone Tracking as Acceptable Anti-Terror Tactic," Pew Research Center, 10 June 2013: http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

[41] Faine Greenwood, "Man Who Crashed Drone on White House Lawn Won't Be Charged," *Slate*, 18 March 2015: http://www.slate.com/blogs/future_tense/2015/03/18/white_house_lawn_drone_the_man_who_crashed_it_there_won_t_be_charged.html ; Julie Zauzmer and Mike DeBonis, "Gyrocopter Lands on Capitol Lawn; Pilot Is Arrested," *Washington Post*, 15 April 2015: https://www.washingtonpost.com/news/local/wp/2015/04/15/a-gyrocopter-just-landed-on-the-capitol-lawn/

[42] Avery Plaw, "Counting the Dead: The Proportionality of Predation in Pakistan," in *Killing by Remote Control: The Ethics of an Unmanned Military*, ed. Bradley Jay Strawser (Oxford: Oxford University Press, 2013), 126.

[43] Ibid., 132.

[44] Ibid., 127–28.

[45] Jeffrey A. Sluka, "Death from Above: UAVs and Losing Hearts and Minds," *Military Review,* May–June 2011: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20110630_art012.pdf

[46] David Hastings Dunn, "Drones: Disembodied Aerial Warfare and the Unarticulated Threat," *International Affairs* 89, no. 5 (2013): 1243.

[47] Ibid.

[48] Milton Hoenig, "Hezbollah and the Use of Drones as a Weapon of Terrorism," *Public Interest Report* 67, no. 2 (2014) : 2–3: http://fas.org/wp-content/uploads/2014/06/Hezbollah-Drones-Spring-2014.pdf

[49] Dunn, "Drones," 1246.

[50] Burke, *9/11 Wars,* 31.

[51] Ibid., 44.

Countering Extremist Groups in Cyberspace: Applying Old Solutions to a New Problem

LTC Robert Schultz, US Army

Finding ways to counter an adversary that is not physically observable poses a significant challenge, especially when that adversary is operating within the vast domain of cyberspace. For various extremist groups that promote hatred and violence, cyberspace provides a virtual safe haven where they can promote their causes, raise funds, communicate, and grow. Based on the increasing number of extremist websites, it appears that the considerable efforts to degrade these online operations have had little overall effect. This outcome points to the need for innovative strategic solutions to counter these extremist groups in cyberspace.[1] Rather than creating new strategies that require a tremendous amount of brainpower, manpower, and money, however, new forms of two old operational concepts from land and naval warfare over the last few centuries could work in tandem to counter the cyberspace strategies of extremist groups.

The first concept is called a *false-flag operation*, a deceptive maneuver that allowed a navy's ships to approach enemy vessels and launch a surprise attack at close quarters. A virtual false-flag maneuver could be used in cyberspace to disguise operations intended to undermine an adversary's web-based operations. Second is the high-risk and deceptive concept of *pseudo operations*, in which an agent infiltrates an adversary's physical location and poses as a member of the target group for the purposes of gathering intelligence and disrupting operations. These two operational concepts are provocative because they have sometimes been associated with the use of "dirty tricks," especially in cases where sponsorship and oversight were haphazard.[2] This article therefore also suggests a legal framework for executing these operations feasibly and legitimately, by reinvigorating the age-old practice of issuing letters of marque and reprisal.

NEW FORMS OF TWO OLD OPERATIONAL CONCEPTS COULD COUNTER THE CYBERSPACE STRATEGIES OF EXTREMIST GROUPS.

The Need for Novel Solutions

What makes extremist groups a unique threat in cyberspace is that the majority of them cannot be tied to a recognizable or accountable body, such as a nation-state. It was easy for the United States and its allies to tie provocative behavior to the Soviet Union during the Cold War, and even easier to identify the "bad guys" during the transparent struggle for world domination with Nazi Germany and imperial Japan in World War II. Today, most extremist groups are acephalous—composed of dispersed organizations and individuals and lacking any clear command structure—which makes them even more difficult to identify and target using conventional military power.[3] To be successful, they must be able to instill loyalty among their members through near-constant communications, and in this regard, their lack of a centralized structure has made them true beneficiaries of cyberspace. Utilizing websites and social media outlets, extremist groups enjoy unparalleled global reach with which to organize and conduct operations such as recruiting, fund-raising, and training.

In light of increasing illicit activities in cyberspace by a multitude of extremist groups, the United States and its allies should acknowledge that tools for the application of offensive cyberspace operations against these threats are needed. Before turning to new strategies, however, the extremists' opponents might look to some old concepts to meet these new threats.

The advent of web-based information technology has made it possible for many governments to carry out their own covert operations and create new opportunities in cyberspace to counter extremists.[4] Few extremist groups that currently operate in cyberspace, despite being equipped with various degrees of information technology and a cybersecurity infrastructure, have the capability to detect their opponents' counter activities. This is due, in part, to the loose organizational structure of most extremist groups, which does not support the training and resources required to detect and counter hackers, viruses, or false personas. With these favorable conditions, it is time to encourage the integration of offensive capabilities such as false-flag operations, pseudo operations, and the issuance of letters of marque and reprisal into cyberspace counterterrorism strategies.

False-Flag Operations

False-flag operations are secret or disguised operations intended to deceive an adversary into believing the operations are being executed by groups or states other than those that actually planned and implemented them.[5] The term *false flag* originated in naval warfare. A warship would attempt to deceive an enemy vessel's crew by hiding its flag or replacing it with one that looked like a friendly flag, in order to maneuver close enough to launch a surprise attack and destroy or capture the target before being fired upon. This tactic, although rarely used in modern times, has long been legally acceptable under the US Law of Armed Conflict, which permits the wearing of enemy uniforms prior to engaging in combat.[6] The use of false-flag operations largely faded away in the mid-1800s (with the important exception of the German Navy Raiders during both World Wars). Many nation-states maintained that these operations were being carried out without proper oversight or governmental control, primarily by pirates whose atrocities were then wrongly blamed on other nation-states.[7] This of course would not be the case for these operations carried out under official auspices in cyberspace. Such deceptions are, in fact, legitimized at the international level under Articles 37–39 of the Geneva Convention, which state,

> Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law.[8]

FEW EXTREMIST GROUPS HAVE THE CAPABILITY TO DETECT THEIR OPPONENTS' COUNTER ACTIVITIES.

Used in cyberspace, a false-flag operation could disguise deceptions in a similar manner. Additionally, where traditional false-flag operations used a disguise to approach the enemy, the interaction between the deceiver and the deceived is reversed in cyberspace. The target must actively choose to visit the false-flag website for the deception to work. Because posting web-based content is far different from engaging in physical combat, any requirement to eventually reveal the identity of the sponsor remains a question for legal scholars. Web-based false-flag operations thus are more akin to "black" or covert deceptions in which the sponsor's attribution remains hidden.[9]

False-flag operations in cyberspace involve developing websites, blogs, and chat rooms that mirror a targeted extremist group's ideology. The first steps are for cyber-deceivers to develop web-based content that is consistent with the targeted group's narrative and then to redirect the group's followers to the false site. Skilled coders could, for instance, execute seamless redirections from targeted websites to false-flag sites. Next, as readership and membership grow, the content on the false-flag sites gradually changes. Over time, the narratives shift subtly, to influence the audience into believing the target group's ideology is corrupt, for instance, or so devious and untrustworthy that supporters feel compelled to terminate their online association with the extremist group.[10]

For example, the recent trend of using online radicalization to fill the ranks of ISIS could be countered through the use of false-flag operations that deliberately undermine the bond of trust between those who may want to join the cause and the extremists. False-flag websites could highlight the group's atrocities, against Muslims in particular, and thus help delegitimize the movement. Alienating extremist groups like ISIS from the international Islamic community through false-flag operations would not only degrade such organizations in the short term but also potentially discredit their online activities over the longer term.

AS READERSHIP GROWS, THE CONTENT ON THE FALSE-FLAG SITES GRADUALLY CHANGES.

Implications of False-Flag Operations

There are three effects we can expect to see if false-flag operations are successful in undermining the bonds of trust between targeted online extremist groups and would-be supporters. First, because false-flag operations target the legitimacy of the extremists, we would expect to see measurable changes in online activity, such as decreases in membership, fund-raising, blog postings, and chats, as well as increases in the antagonistic and denunciatory messages posted on false-flag websites. Second, we would see targeted extremist groups begin to police or even attack other like-minded websites they did not directly manage as they came to question the veracity of the others' ideology or suspect rivals of being the source of their websites' problems.[11] Finally, we would also expect to see an overall change in the extremists' use of cyberspace, as they and their supporters—even if they detected the false flag—felt less free to operate openly in the virtual medium.

False-flag tactics are already being used to some extent to counter online extremism, but only in a defensive manner or to collect intelligence. The concept of false-flag operations presented here is unique because it applies deception as an *offensive* tool to counter extremist activity online.

Pseudo Operations

Another effective deception based on an operational concept used previously against insurgent and terrorist organizations is the pseudo operation. Pseudo operations traditionally used disguised military forces to infiltrate an adversary's area of operation in order to gain targetable intelligence.[12] Historically, the British have had the most experience and success with pseudo operations, which they utilized in the anticolonial insurgencies of the post–World War II period, such as the Mau Mau uprising in Kenya (1952–1960).[13] The British first developed the concept as early as the Boer War (1899–1902), however, as part of their counterinsurgency strategy against Afrikaner guerillas.[14]

In cyberspace, a pseudo operation may be used to infiltrate an extremist group's virtual area of operations through websites, blogs, and chat rooms for the purposes of gathering intelligence and disrupting its online operations. By targeting the organization's existing online members, pseudo operations could be used to weaken the bonds of trust between the extremist group's leadership and its virtual community. Unlike false-flag operations, which focus on audiences that are not already members of the targeted extremist group, such as potential recruits and donors, pseudo operations in cyberspace work to get inside the targeted extremist group, gather information, and disrupt the organization from within. Conceptually, web-based pseudo forces could "role play" as active members and supporters in order to gain access to the inner workings of a targeted extremist group's online operation. Once inside, the pseudo force would begin collecting intelligence on group members and their activities. As specific targets within the online organization were developed, the pseudo force would begin exploiting rifts between members and groups within the organization through the use of misinformation and similar tactics. Ultimately, the bonds of trust between loyal supporters and the extremist group's leadership would be undermined to the point that the group would lose many of its members or even disintegrate.

Identifying the right selection criteria for the personnel who would conduct web-based pseudo operations is critically important. To mitigate the chances of compromise, the first step would be to recruit team members for these operations from various organizations, to keep their association with each other sufficiently vague and help mask the team from the internal security apparatus of a targeted extremist group. History has also proved that the best executors of pseudo operations are those who enjoy adventure rather than those who are or once were extremists themselves, or those who could be swayed by peer pressure. The adventure seekers and risk takers were much more reliable and easier to retain for future operations.[15] With the explosion of online gaming over the past 20 years, finding motivated individuals who enjoy the excitement of role playing and are comfortable in the relatively secure and low-cost environment of cyberspace will likely be easy.

The effectiveness of pseudo operations is also proportional to the level of approval and support provided by senior civilian and military leadership. Cyberspace, in effect, helps alleviate concerns about risk and the danger of compromise because of its inherent anonymity and the ability to operate with minimal risk of physical consequence. Incorporating pseudo operations into future counterinsurgency strategies will leverage the powerful effects that can be brought to bear against extremist groups in cyberspace.

Implications of Using Pseudo Operations

If pseudo operations are effective, we would expect to see three observable effects. First, since pseudo operations directly attack the internal workings of an extremist group's online operation, we should see a decrease in the group's overall cyber operations and an increase in security measures at targeted sites. The need to improve security would also increase the operating costs for the extremist group's cyber presence. Signals of increased security might include more frequent notifications for members to change their passwords or the use of image credentialing to verify user identification. Second, since an important aspect of pseudo operations is to create and exploit rifts between members of the extremist group's online community, we would expect to see the group splinter or even disappear altogether. Third, pseudo operations by design induce dissent and distrust within the organization, and the anonymity of cyberspace only exacerbates these types of fissures. Trust among its members is vital to the strength of any illicit organization, and members of the extremist group—who would already be on alert because of heightened site security—would grow distrustful of each other in regular online activities such as chatting and blogging. Members' trust in the organization's leadership would diminish, along with the group's ability to recruit and carry out operations.

Whether it is the potential for operators to be compromised or the implications of associating itself with former insurgents, the United States has not had a doctrinal concept on pseudo operations, nor has it used pseudo operations as part of a military strategy—certainly not in cyberspace.[16] With the advent of cyberspace as a global common domain and the precipitate rise in extremist messaging online, however, there is a new opportunity—and need—to reinvigorate pseudo operations as an operational concept.

Letters of Marque and Reprisal

False-flag and pseudo operations in cyberspace require a domestically and internationally acceptable policy, a legal framework that justifies their use, and a recognized necessity for their continued practice. For the United States, these requirements can be found in its Constitution, which states that the US Congress has the power "to declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water." [17]

In the days before the United States possessed a strong naval force, and for individual states without strong navies, letters of marque and reprisal offered an alternative method of defending interests on the high seas. The issuance of these letters became the strategy of choice at a time when many governments found themselves short on both revenue and naval vessels.[18] Rather than have to pay for naval operations against an enemy, the government simply granted private ship owners, commonly known as "privateers," the legal authority to conduct naval warfare, raid ship-borne commerce, and seize adversaries' ships.[19] In return, the privateer was paid with a portion of whatever goods he captured, which served as an incentive to capture as much of the opponent's shipping as possible. The English crown used this concept, known as privateering commissions, as early as the thirteenth century: private individuals would be commissioned to infiltrate an adversary's territory for the purposes of retaliation or retribution against specific people believed to have committed offenses against the king.[20] In 1765, the concept of letters of marque and reprisal was written into the Commentaries on the Laws of England, which state,

> These letters are grantable by the law of nations, whenever the subjects of one state are oppressed and injured by those of another; and justice is denied by that state to which the oppressor belongs. In this case letters of marque and reprisal (words in themselves synonymous and signifying a taking in return) may be obtained, in order to seize the bodies or goods of the subjects of the offending state, until satisfaction be made, wherever they happen to be found. Indeed this custom of reprisals seems dictated by nature herself; and accordingly we find in the most ancient times very notable instances of it.[21]

Simply put, a *marque* is a pledge to someone or something. *Reprisal* is retaliation for perceived violations or harmful actions. A reprisal could be the seizing or destruction of property or persons, and could range from a small-scale attack to major operations against the adversary.[22] Therefore, a letter of marque and reprisal would authorize a private entity or person to conduct reprisal operations anywhere in the world or—in the case of cyber operations—outside of it.

The situation today is not dissimilar, as extremist groups operate virtually unopposed in cyberspace, while many governments find themselves falling short in their efforts to confront them. Hence the value of letters of marque and reprisal, which would enable governments to deploy a private army of hackers, or cyber privateers, to legally and legitimately execute cyber activities like false flags and pseudo operations. The US military, having fought conflicts in Afghanistan and Iraq for the past 14 years, finds itself in a conundrum of diminishing funds, resources, and people. Recent budget measures have dictated cuts in defense spending that limit the military's ability to create new capabilities and formations. At the same time, the use of cyberspace by extremist groups is growing to the point where cyber warfare is a daily and continuous fight that must be won. Issuing letters of marque and reprisal to build a force of cyber privateers without the use of tax dollars could help limit the reach of extremists in cyberspace while legally justifying offensive cyber capabilities.

THE GOVERNMENT GRANTED "PRIVATEERS" THE LEGAL AUTHORITY TO CONDUCT NAVAL WARFARE.

To build these capabilities, letters of marque and reprisal could be issued to any number of the private organizations or individuals that have expressed a willingness to counter extremist groups in cyberspace.[23] History has several examples, such as the Abraham Lincoln Brigade in the Spanish Civil War, of privately-funded forces that fought for idealistic principles. Today, like-minded private organizations could recruit socially concerned and tech-savvy individuals to conduct false-flag and pseudo operations from their personal computers.[24] For this concept to work, however, each letter of marque and reprisal would need to articulate in detail the parameters of the privateers' activities, as well as economic incentives, if any. For example, the letter could prohibit conducting cyber attacks solely as retaliation for attacks against individual privateers. Additionally, the letters would need to define the financial incentives for cyber raids against an opponent's exploitable data, such as personal and financial information. An appropriate incentive for a privateer would be the use of bank account data, or a portion of funds that may have been donated to a targeted online extremist group and confiscated by the cyber privateer. With the proper legal oversight, these prizes, or some portion of them, would be the privateer's to keep. Potential cyber privateers have already shown interest in conducting offensive operations in cyberspace for these purposes. For example, following the deadly attacks on the French satirical publication *Charlie Hebdo*, outraged tech-savvy individuals and groups launched private cyber attacks on jihadist websites in an attempt to shut down their online propaganda.[25] Imagine the outcome if these attacks were grounded in law, controlled by proper oversight, and incentivized with profit?

In addition to false-flag and pseudo operations, cyber privateers could be issued letters of marque and reprisal to fill specific military requirements that the state's military cannot or will not immediately meet. Fueled through the incentive of profit, the privateers could expeditiously begin cyber operations as stipulated under the letter.[26] In the past, privateers have achieved mixed results while supporting state militaries, whether it was because they operated beyond the scope of their contracts or because they fostered the perception that they existed solely for profit, and so such operations have yet to establish a positive reputation in national defense.[27] To help correct this perception, governments can draw on a 200-year-old mechanism for providing legal oversight of privateers: prize courts. Historically, representatives of a sponsoring government's prize courts ensured privateers were not rewarded beyond the scope or the authority outlined in the specific letter of marque and reprisal.[28] A prize court could make rulings on the sale or destruction of seized items and the distribution of any proceeds, or order the return of seized property or funds if the seizure was deemed unlawful. The same judicial concept could be applied today without the need to expand the size or scope of a state's legal system.[29] Under current law in the United States, for example, federal district courts throughout the country have exclusive jurisdiction in prize cases. No prize cases have been heard in the United States since the current statutes were adopted in 1956 because no letters of marque and reprisal have been issued in that time, but the system to provide judicial oversight already exists.[30]

THE LETTERS WOULD NEED TO DEFINE THE FINANCIAL INCENTIVES FOR CYBER RAIDS.

Understanding the circumstances and conditions in which a letter of marque and reprisal could be issued with regard to cyberspace is very important. Unlike land and naval warfare, targets in cyberspace are not physical and can be disguised with false identifications and internet protocol (IP) addresses. The burden of proof to determine whether to issue a letter of marque and reprisal to disrupt, corrupt, influence, destroy, or deceive a targeted extremist group in cyberspace remains the same. These actions should be characterized by clear thresholds of legal action: first, officials would have to show probable cause to initiate offensive cyber operations, and second, the government would be required to demonstrate evidence of a crime beyond a reasonable doubt before a letter of marque and reprisal would be issued.[31]

Implications of Letters of Marque and Reprisal

Perhaps the best part about the strategic use of letters of marque and reprisal is that they are completely legal under current international law and US constitutional law. The US Constitution gives Congress the authority not only to declare war but also to issue these letters, as an alternative to engaging in costly physical warfare. This alternative also empowers private citizens to work on behalf of the US government in a military capacity. Opponents to letters of marque and reprisal often point to the Paris Declaration Respecting Maritime Law, ratified by 55 countries in 1856, which bans signatory nations from commissioning privateers.[32] The United States, however, was not a signatory to this declaration, which pertains only to the letters' use in naval warfare. To date there are no other international laws pertaining to privateering that would preclude the United States from using these letters for cyberspace operations.[33]

Nevertheless, attempts in 2001 and again in 2007 to introduce new legislation in Congress that would have authorized the issuance of letters of marque and reprisal to counter al Qaeda fell on deaf ears and were quickly dismissed.[34] By recruiting and regulating talented cyber privateers to carry out false-flag and pseudo operations, the United States and its allies could implement a cost-effective campaign against extremist groups operating in cyberspace.[35]

Considerations for the Use of New Solutions in Cyberspace

With the legal backing of letters of marque and reprisal, false-flag and pseudo operations could be successfully integrated into a strategy for countering extremist groups in cyberspace. The following points, however, must be considered.

1. **Feasibility.** Maintaining transparency between these operational concepts and the civilian authorities and laws that govern their use is much easier to do in cyberspace than in the physical domain. A cyber privateer operating under legal authority and supervision would have a much harder time hiding clandestine activity than would the captain of a ship on the open ocean. Letters of marque and reprisal, with their attendant legal infrastructure, make it less likely that a poorly constructed false-flag operation would be tied to or enable an actual terrorist attack, or that a pseudo operation would target a group that is only exercising its right to free speech.
2. **Suitability.** Normally, these operational concepts come with a limited shelf life because of their deceptive nature. Adversaries in the physical domain would eventually catch on to methods such as infiltration by an undercover agent or disinformation operations.[36] In cyberspace, by contrast, time could be on the side of the implementer. Although these operational concepts may take longer to be effective, the vastness and anonymity of cyberspace allows the false-flag and pseudo operators, supported by the issuance of letters of marque and reprisal, to continue to adjust methods, techniques, and timing. In terms of targeting extremist groups in cyberspace, operational concepts and overarching strategies of this nature work best when their aggregated effects are achieved over time.
3. **Risk.** Operations in cyberspace can be difficult to control. The risk of compromise should, however, be an acceptable part of doing business. Those who carry out these new solutions should assume their efforts will be compromised; it might be just as advantageous to the operators, however, if the targeted extremist group does detect these offensive cyber operations. The extremists would be forced to adjust their online presence, and members and potential recruits would question the security of "trusted sites." Additionally, in the event of compromise, false-flag and pseudo operators need merely to take the operation off-line and reconfigure, and then reappear under another persona, avatar, or website. Finally, and perhaps most obviously, cyber operations of this nature assume less physical risk compared to their historical forerunners. Cyberspace should prove to be a forgiving environment that continually allows for renewed innovation without the associated operational risk of loss of life and collateral damage. Regardless, common sense dictates that governments should not ignore any of these low-cost and relatively safe tools that can help them achieve their goals of countering extremists in cyberspace with greater effectiveness and efficiency.

Conclusion

Rapidly emerging cyber technologies, which have connected every corner of the world, are being used quite efficiently by extremist groups for recruitment and fundraising. Concepts such as false-flag and pseudo operations can be instrumental in developing strategic solutions that are legally reinforced by letters of marque and reprisal to counter extremist operations in cyberspace. Numerous defensive cyber-security tools—often of dubious effectiveness—have been developed and implemented, but more offensive capabilities are needed in cyberspace to counter emerging threats in the twenty-first century. When it comes to countering extremist groups in cyberspace, false-flag operations, pseudo operations, and letters of marque and reprisal can provide myriad creative options from which to choose. ❖

ABOUT THE AUTHOR

LTC Robert Schultz is a US Army information operations officer.

NOTES

[1] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C.: US Institute of Peace, 2006), 15.

[2] Dirty tricks are unethical or illegal tactics employed to destroy or diminish the effectiveness of opponents. See Lawrence E. Cline, *Pseudo Operations and Counterinsurgency: Lessons from Other Countries* (Carlisle, PA: Strategic Studies Institute, 2005), 20: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=607

[3] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, MR-1382-OSD (Santa Monica, Calif.: RAND Corporation, 2001), 241: http://www.rand.org/pubs/monograph_reports/MR1382.html

[4] Charles A. Fowler and Robert Nesbit, “Tactical Deception in Air-Land Warfare,” *Journal of Electronic Defense* 18, no. 6 (1995): 50.

[5] Geraint Hughes, *The Military’s Role in Counterterrorism: Examples and Implications for Liberal Democracies*, Letort Paper (Carlisle, Pa.: Strategic Studies Institute, May 2011), 105.

[6] Headquarters, Department of the Army, *The Law of Land Warfare*, FM 27-10 (Washington, D.C.: HQ, Dept. of the Army, 18 July 1956), note 15, para 54.

[7] Hughes, *Military’s Role in Counterterrorism*, 105.

[8] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Art. 37–39: https://www.icrc.org/ihl/INTRO/470

[9] W. Thomas Smith, Jr., *Encyclopedia of the Central Intelligence Agency* (New York: Facts on File, 2003), 31.

[10] Mark E. Stout, Jessica M. Huckabey, and John R. Schindler, *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movements* (Annapolis, Md.: US Naval Institute Press, 2008), 122; David B. Moon, “Cyber-Herding and Cyber Activism: Countering Qutbists on the Internet” (master’s thesis, US Naval Postgraduate School, December 2007), 5–18.

[11] Additional research into the psychology behind these dynamics is needed to design false-flag operations to be as effective as possible.

[12] Cline, *Pseudo Operations and Counterinsurgency*, 1.

[13] For more information on pseudo gangs during the Mau Mau Uprising, see Wunyabari O. Maloba, *Mau Mau and Kenya: An Analysis of a Peasant Revolt* (Bloomington: Indiana University Press, 1993).

[14] Ibid., 2.

[15] Frank Kitson, *Gangs and Counter-Gangs* (London: Barrie and Rockliff, 1960), 126.

[16] Paul Melshen, *Pseudo Operations* (Newport, R.I.: US Naval War College, February 1986), 2.

[17] US Const., art. 1, § 8.

[18] Ian Rice and Douglas Borer, “Bring Back the Privateers,” *The National Interest* (22 April 2015): http://nationalinterest.org/feature/bring-back-the-privateers-12695

[19] C. Kevin Marshall, “Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars,” *The University of Chicago Law Review* 64, no. 3 (Summer 1997): 960–61. See also Theodore M. Cooperstein, “Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering,” *Journal of Maritime Law and Commerce* 40, no. 2 (2009): 224–29.

[20] Kelly Gneiting, “A Constitutional Alternate to War, Marque and Reprisal,” Independent American Party, 18 October 2013: http://www.independentamericanparty.org/2013/10/an-constitutional-alternate-to-war-marque-and-reprisal/

[21] William Blackstone, *Commentaries on the Laws of England* (1765–1769), Section I, 249.

[22] Fred E. Foldvary, “Letters of Marque and Reprisal,” Progress, 8 October 2002: http://www.progress.org/tpr/letters-of-marque-and-reprisal/

[23] Rice and Borer, “Bring Back the Privateers.”

[24] “Spanish Civil War: The Abraham Lincoln Brigade and the Spanish Civil War,” Abraham Lincoln Brigade Archives, n.d.: http://www.alba-valb.org/history/spanish-civil-war

[25] David Goldman and Mark Thompson, “Anonymous Blocks Jihadist Website in Retaliation for Charlie Hebdo Attack,” CNN, 12 January 2015: http://money.cnn.com/2015/01/11/technology/security/anonymous-charlie-hebdo/

[26] Rice and Borer, “Bring Back the Privateers.”

[27] William Young, “A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal,” *Washington and Lee Law Review* 66, no. 2 (March 2009): 10.

[28] Rice and Borer, “Bring Back the Privateers.”

[29] Marshall, “Putting Privateers in Their Place,” 961–63.

[30] 10 US Code § 7681—Reciprocal privileges to cobelligerent.

[31] Michael Todd Hopkins, “The Exceptionalist’s Approach to Private Sector Cybersecurity: A Marque and Reprisal Model” (master’s thesis, George Washington University, 2011).

[32] Donald A. Petrie, *The Prize Game: Lawful Looting on the High Seas in the Days of Fighting Sail* (Annapolis, Md.: US Naval Institute Press, 1999), 143.

[33] In addition to false-flag and pseudo operations, these letters could refresh other operational concepts such as spoofing attacks, which would provide counterterrorist operators with an even greater strategic advantage in cyberspace. Spoofing effects falsify online data and images in order to influence and/or deceive online users to surrender their own data. See Dorothy E. Denning, *Information Warfare and Security* (New York: Addison-Wesley, 1998).

[34] Gneiting, “A Constitutional Alternate to War.”

[35] Jeremy A. Rabkin and Ariel Rabkin, *To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict* (Stanford, Calif.: Hoover Institution, 19 January 2012): http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf

[36] James Adams, *The Next World War: Computers Are the Weapons & the Frontline Is Everywhere* (New York: Simon & Schuster, 2001), 286.

The Comprehensive Approach: A Silver Bullet or the Loch Ness Monster?

LTC Sándor Fábián, Hungarian Army

The way militaries understand what constitutes a threat to security has gone through a significant transformation since the end of the Cold War. Single peer-on-peer military threats of the past have given way to complex forms of violence and upheaval that simultaneously threaten both national and global peace and security. The natural consequence of this transformation is a fundamental change in the way nations approach crisis management, a role that has radically expanded over the course of recent conflicts in terms of tasks, timelines, and the number of actors involved.[1] By the beginning of the twenty-first century, both individual states and international organizations had painfully learned that their traditional, sequenced crisis management procedures did not deliver the results they expected.[2] Despite "on-paper" success in many crisis areas, the world has seen numerous seemingly resolved conflicts relapse into violence since the early 1990s.

Many scholars, supported by research that has explored the recent failures in crisis management, argue that the fundamental problem is due to "poor coordination and collaboration between the actors involved," which has led to "wasted resources, poor effectiveness, and lack of sustainability."[3] The concept of a comprehensive approach (CA) to crisis management was born out of these discussions, and the term came to be widely used among both national and international crisis management professionals. Now CA is cited everywhere from the lowest to the highest levels of decision makers and practitioners as if it were a silver bullet for solving contemporary conflicts. But is it?

NO SINGLE, UNIVERSALLY AGREED DEFINITION OF THE COMPREHENSIVE APPROACH EXISTS.

What Is a Comprehensive Approach?

As a result of the shortcomings of crisis management in recent conflicts, a number of international organizations, including the United Nations, the European Union, and NATO, along with individual states, have taken significant steps to improve the efficiency, effectiveness, and sustainability of their crisis management efforts. These initiatives have "resulted in the development of a range of concepts for acting comprehensively."[4] Although these concepts share some common ground, in the end all of them have been fundamentally shaped by the national and organizational contexts in which they were developed. No single, universally agreed definition of CA exists. Given this fact, it seems more appropriate to think about CA as a cluster of concepts rather than as one common concept. There are at least three identifiable categories of CA, based on the bureaucratic levels at which CA is implemented: national, intra-agency, and interagency.[5]

CA at the National Level

A number of countries, especially those involved in recent crisis management efforts, "have been experimenting with improving coherence between their own ministries or governmental departments, with a view to improve the national management of domestic challenges as well as international operations."[6] Different terminologies inevitably arose to describe the application of CA at the national level, including the whole-of-government approach;[7] DIME, a US concept that refers to the four types of power a government can bring to bear (diplomatic, information, military, and economic); PMESII (political, military, economic, social, information, and infrastructure systems), a US military acronym from systems analysis; and the Canadian 3D approach (defense, diplomacy, and development), to name a few prominent examples. It does not matter what name is used—all of these concepts aim to harmonize the policies and actions of various governmental departments around a certain issue to achieve greater effectiveness. These approaches include the coordination of the "departments and agencies responsible for defence, foreign affairs, and international development issues," a grouping that is sometimes stretched to include other departments or ministries, such as trade, finance, or justice.[8] The concepts are based on the assumption that more meaningful and sustainable effects can be achieved in crisis management "when the various government departments involved pursue a common strategy, [and] have a shared understanding of the problem, a common theory of change, and an agreed plan for implementing such a strategy."[9]

It must be admitted that many of these national approaches have had some promising results, including putting "mechanisms in place for regular meetings to exchange information" and coordinate actions;[10] the establishment of integrated offices; the development of joint funding mechanisms; and the development of a joint national strategy with regards to specific crises. While the implementation of CA on a national level may be useful for creating consistent national policies, it is not sufficient to address contemporary international crises. National approaches are developed mostly in a vacuum, where the focus is on national interests and concerns. If a country's CA policy fails to consider the strategies, interests, and abilities of the other actors and organizations involved in an international crisis, it will be more difficult for that country's agencies and personnel to effectively interact with others in the field—especially because the national agencies' hands will already be tied by national interests when they arrive in the conflict zone. These agencies will also be less flexible and adaptable in a foreign environment. Last but not least, national approaches in general seem to be too "state-centric"; in other words, they fail to properly consider the roles of civil society, the private sector, and international organizations in crisis management.

Intra-Agency Concepts of CA

International organizations have their own intra-agency concepts for CA as well, and like the national ones, there are significant differences among them. Three of the many ideas developed in recent years are particularly relevant to this discussion.

The United Nations' Integrated Missions concept

> refers to a type of mission where there are processes, mechanisms and structures in place that generate and sustain a common strategic objective, as well as a comprehensive operational approach among the political, security, development and human rights sectors and, where appropriate, humanitarian UN actors at the country level.[11]

The European Union's Civil-Military Coordination Concept

> seeks to ensure and guide a Comprehensive Approach particularly at the political-strategic level, ranging from the planning phase to execution of a mission. The "Crisis Management Procedures" as well as the "Crisis Management Concept," which is developed individually for each operation, are geared towards ensuring that the Comprehensive Approach concept is applied in the EU's crisis management activities.[12]

Finally, NATO's Comprehensive Approach

> is NATO's planning blueprint. This is to be achieved by expanding its approach for military planning to include all civilian and military aspects of a NATO engagement. … [NATO's] approach primarily seeks to improve the external cooperation with civilian actors and other international organizations.[13]

Although the very existence of these approaches is a significant step forward in international crisis management, all of these organizations have a long way to go to develop coherent policies that will make the concepts work. As of now, all of these approaches "suffer from internal, institutional and interagency rivalry," and even more from disagreement and fragmentation among the organizations' member states, which have consistently failed to speak with one voice.[14] Furthermore, it seems that the intra-agency approaches face an "ideological gap between the political/military actors on the one side and humanitarian actors on the other."[15] Although this is a problem for both the UN and the EU, it most severely affects NATO and could potentially block the alliance's efforts to bring humanitarian partners on board with CA. Last but not least, the most challenging problem for international organizations is to develop a model for cooperating among themselves and synchronizing their differing approaches.

Inter-Agency Approaches to CA

The third category of CA concepts, the inter-agency approach, is best described as a whole-of-systems approach:

> Instead of seeking coherent and complementary approaches between governmental actors or within one organisation, CA, at this level, addresses the relationships and structures that exist among and between the plethora of international and local actors and organisations engaged in a given context.[16]

The inter-agency approach arose from the context of concept development and experimentation, such as the Multinational Experiment series. This approach addresses "the relationship between actors both at a strategic level as well as in the field. The pre-conditions for acting comprehensively in these different contexts vary significantly."[17] Recent crisis management operations have in fact tended to expose the lack of a unified strategy, which makes the implementation of CA in the field no more than an attempt to coordinate the activities that derive from various existing strategies.[18] The inter-agency approach has never been effectively operationalized because it is inherently complex and "there are only a few strategies or suggested working methods that concretise CA at this level."[19]

CA IS A MIND-SET. "IT INCLUDES RECOGNITION OF ONESELF AS PART OF A SYSTEM."

It seems obvious that despite CA being used so frequently in crisis management, there is no universal agreement about what CA entails or even how it should be defined. The different CA approaches "exist because they fulfil different functions, use different resources and have varying goals and ambitions."[20] One common denominator can, however, be identified: CA is a mind-set. "It includes recognition of oneself as part of a system and an understanding that effectiveness, efficiency and sustainability can be achieved if the interdependencies that exist within this system are responsibly managed."[21] There have been numerous attempts to concretize and implement CA, which usually have "resulted in the establishment of structures and processes for coordination and collaboration. How these structures or processes are outlined depends on the nature of each system and what possibility there is to direct and coordinate the system."[22]

As long as CA is used as a highly conceptual, singular term, without understanding "how the various interpretations vary and what effect each of them has on how CA should be implemented, assessed and prepared for," the approach will never be a blueprint for effective crisis managment.[23] A number of questions need to be answered. How will the dependencies (e.g., resources and action timelines) be managed? What incentives are needed to ensure coordination and cooperation? How will the harmonization of actions and goals occur? How will key leaders be trained? How do participants ensure that the necessary capabilities are developed? Until everyone agrees on the answers, CA will not be a silver bullet for crisis management, but only a myth like the Loch Ness monster: lots of people talk about Nessie, some may even believe it exists, but no one has ever been able to prove its existence beyond a doubt. ❖

ABOUT THE AUTHOR

LTC Sándor Fábián is a Special Forces officer in the Hungarian Army.

NOTES

[1] Christian Mölling, "Comprehensive Approaches to International Crisis Management," *CSS Analyses in Security Policy* 3, no. 42 (October 2008): 1: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-42.pdf

[2] In traditional crisis management operations, peacekeeping and peace building were considered to be sequential steps. Peace building naturally followed peacekeeping, and development initiatives would begin only after a sufficient level of "peace" and stability had been established. Experiences from operations in recent years, however, show that recognizable points where peacekeeping might naturally transition into peace building are difficult to find. Cecilia Hull, *Focus and Convergence through a Comprehensive Approach: But Which among the Many?* (Stockholm: Swedish Defence Research Agency, 2011), 3: http://www.dodccrp.org/events/16th_iccrts_2011/papers/088.pdf

[3] Ibid., 3–4.

[4] Ibid., 4.

[5] Ibid., 7–8.

[6] Ibid., 8.

[7] "'Whole of Government Approaches' usually aim at improving inter- and intra-ministerial cooperation in view of assuring a nationally consistent approach. They respond to the experience that incoherencies in domestic actors' positions and policies obstruct not only a coherent national strategy but also constitute a major stumbling block for an internationally accepted and coherent crisis response." Mölling, "Comprehensive Approaches," 2.

[8] Hull, *Focus and Convergence*, 8.

[9] Cedric de Coning, Helge Lurås, Niels Nagelhus Schia, and Ståle Ulriksen, *Norway's Whole-of-Government Approach and Its Engagement with Afghanistan*, NUPI Report (Oslo: Norwegian Institute of International Affairs, Department of Security and Conflict Management, 2009), 5: http://www.oecd.org/dac/evaluation/dcdndep/47107380.pdf

[10] Hull, *Focus and Convergence*, 8.

[11] Kristiina Rintakoski and Mikko Autti, *Comprehensive Approach: Trends, Challenges, and Possibilities for Cooperation in Crisis Prevention and Management* (Helsinki: Ministry of Defence/Crisis Management Initiative, 2008), 13: http://www.defmin.fi/files/1316/Comprehensive_Approach_-_Trends_Challenges_and_Possibilities_for_Cooperation_in_Crisis_Prevention_and_Management.pdf

[12] Mölling, "Comprehensive Approaches," 3.

[13] Ibid.

[14] Rintakoski and Autti, *Comprehensive Approach*, 17.

[15] Ibid.

[16] Hull, *Focus and Convergence*, 9.

[17] Ibid., 10. "The Comprehensive Approach concept for MNE 5 [Multinational Experiment] describes the overarching framework in which various nationally sponsored concepts (or focus areas) are being evaluated for their individual practicality and for the critical integration linkages between focus areas to support effective and efficient coalition operations. MNE 5 has aimed to provide capabilities through which concerned nations and organisations can harmonise potentially divergent views and interests in order to respond to a crisis in a unified manner." Rintakoski and Autti, *Comprehensive Approach*, 16. For more on the MNE series, go to the Multinational Experiment website: https://wss.apan.org/s/MEpub/default.aspx

[18] Hull, *Focus and Convergence*, 10.

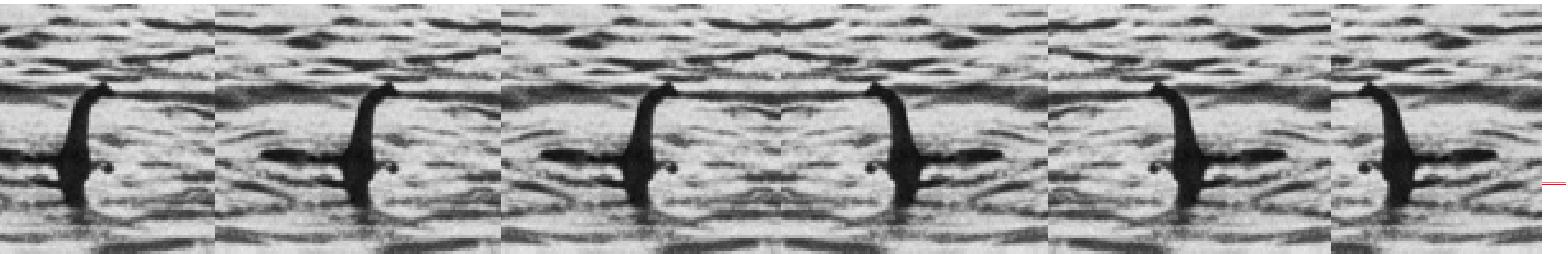
[19] Ibid., 9.

[20] Ibid., 14.

[21] Ibid.

[22] Ibid.

[23] Ibid.



THE CTAP INTERVIEW

Dr. David Kilcullen, Caerus Global Solutions

Interviewed by Dr. Doug Borer, US Naval Postgraduate School

This interview is taken from the collection of the Combating Terrorism Archive Project (CTAP).[1] On 13 August 2015, Dr. Doug Borer sat down with counterinsurgency expert Dr. David Kilcullen to talk about current trends in counterinsurgency planning and operations, and the fight against ISIS.[2] Dr. Kilcullen's books include *The Accidental Guerrilla* (2009), *Counterinsurgency* (2010), and *Out of the Mountains* (2013).[3]

DOUG BORER: Dave, I would first like to address your own experience as someone at the center of counterinsurgency, in theory and in practice, over the last decade or so. What are the greatest improvements you have seen in that time, in terms of both the conceptual thinking and practice of counterinsurgency?

DAVID KILCULLEN: That's a great question. These days we have an incredibly high degree of both familiarity and competence on the part of US military combat units operating in a real warfare environment that really didn't exist 15 years ago. I would put US forces today up against any force on the planet in the last 100 years in terms of their ability to conduct this kind of unconventional warfare operation. We have also seen vast improvements in US capabilities. There are capabilities available to your average line infantry battalion or artillery battalion today that only existed in Special Operations Command back in 2001. Capabilities that only existed in Hollywood in 2001 are now regularly applied by high-end, tier-one special mission units.

CAPABILITIES THAT EXISTED ONLY IN HOLLYWOOD IN 2001 ARE NOW REGULARLY APPLIED.

While the military's conceptual understanding of counterinsurgency has dramatically improved, however, the United States, as a nation, has failed to close the gap between military success on the ground and a range of political reconciliation, stabilization, and economic development issues. The military has repeatedly created the conditions to achieve a political outcome, only to watch political organizations fail to follow through. That's not to shift blame from the military to somebody else; it's just to say that the improvements in military capability haven't necessarily been matched by improvements on the civilian side of government.

BORER: When you served as an advisor to coalition forces and saw these capabilities shift over time, where did you see the line of friction between providing security and order in these environments, and actually developing the local institutions of governance in, say, Iraq or Afghanistan?

KILCULLEN: I would argue that this issue is partly why we have seen, at best, a mixed outcome in both countries. If you put military guys—who have their own people out in harm's way—in charge of the overall mission, then of course you are going to find that force protection becomes a high priority. There is a negative element of force protection, which is bunkers and blast walls and so on. But there is also a positive element of force protection, which is getting out and destroying the enemy before it can close in and destroy you. Either way, you end up with a fairly heavy emphasis on kinetics and on the intelligence side, what I would call “force protection risk,” as distinct from mission risk. In other words, the distinction is between things that can hurt the force and things that can undermine the success of the mission. You tend to find yourself committed to a structure of dependency, where the local actors depend on your presence. You create a safe environment, and you improve the situation to a dramatically better level than the locals can, because you have all these resources. At that point, it becomes really difficult to let go and allow failure.

One of the Afghans I engaged with in 2009 said it best. He said, “Look, there is no question that if the US military fights the Taliban, the US military is going to win. That’s not the issue now. The issue is, what about the Afghan military? How do we get the Afghan military to the point where it can win, initially with support from the US military, but then subsequently without them?” So, the outcome of each individual combat engagement eventually turns out to be less important than institution-building. The trick is to recognize that tipping point. When is it no longer crucial to win every engagement, but crucial to get the locals themselves out on the ground? The other question is, how do you get the people who have been responsible for stabilization up to this point to say, “We have made things really good. Now we’re going to let the situation go back to the way it was temporarily, because that’s the path we have to take to get the locals up to speed”? That’s tough.

YOU TEND TO FIND YOURSELF COMMITTED TO A STRUCTURE OF DEPENDENCY.

Iraq is a good example. We went in with three objectives that were actually incompatible: we wanted to democratize, we wanted to stabilize, and we wanted to create a new economy. The dictatorship was a completely state-based economy. The problem was, back in 2005–2006, we democratized before the country was stable, and then we surrendered control over the new leadership to the Iraqi people. But too many Iraqis had no intention of working with those leaders to achieve a stable outcome. You have to think about sequencing those different objectives carefully, because you are always going to have objectives that are incompatible and parameters that are hard to optimize. It’s a classic design problem, and there is no getting around it. I think our big mistake in Iraq, and to some extent, Afghanistan, was to surrender control over a lot of the tasks that needed to be done to keep the country stable before stability had really been reached, in the name of democracy. It is extraordinarily hard to get that control back. Then, in fact, we never did.

BORER: Do you think it’s possible for a Western country to get involved in these types of conflicts without projecting itself as the role model—as in, “You have to become a democracy if we are involved”?

KILCULLEN: I do think it’s possible. There are even a few historical cases, like the British in Amman, Jordan, in the 1960s and 1970s, or possibly El Salvador, where the United States has only a light footprint. The influence is more indirect, with the implication that the local government is in charge of its own destiny and we are just there to help it execute that. But as soon as you have a US general officer and a satellite dish on the ground, things change. Somebody starts talking back to Washington, and people’s careers begin to build up around a certain outcome. The fundamental role of the embassy shifts significantly, and it becomes very difficult to avoid a kind of commitment trap where you want it more than they want it. And then it’s impossible for you to disengage because you end up doing all of the hard work.

Looking at our experiences in Afghanistan and Iraq, I think it's a bit of a cop-out to say that stabilization and democratization didn't go well because Western countries just can't do this. Maybe they can but just didn't do a good job. Right? I don't think we know the answer to that yet. I would argue that neither Iraq nor Afghanistan is a fair test of concepts if you didn't plan to execute the concepts in the first place. I have had this discussion with people around counterinsurgency theory. There are many great critiques of counterinsurgency theory, but it's not a fair critique to say, "It didn't go well in Afghanistan, so that proves counterinsurgency doesn't work." It would be like treating someone who is sick with half the recommended dosage of antibiotics and then saying the drug doesn't work. You didn't follow the plan. I think that's the case in Afghanistan. We did the job halfway and then let the Afghans handle it. Whether counterinsurgency works is an unanswered question, in my view, but this particular case is not a definitive answer to that question.

BORER: But will this be a case of history repeating itself? For instance, after Vietnam, the US military wanted to avoid these types of wars. But we just keep reinventing the same old counterinsurgency wheel, because the organizational construct goes back to what it does best—which is breaking things.

KILCULLEN: Yes. You mentioned the way bureaucracy operates. There are institutional pathways within the US government that mean we always do things a certain way. And while the Balkans are not like Iraq, and Iraq is not like Afghanistan, Americans are still who we are, so in each of those cases, at least half the equation is the same. There is certainly a tendency within the armed forces, at the political level, to say we want to avoid ever getting into a counterinsurgency environment again, and we want to avoid ever again having to do what we did in Iraq and Afghanistan. People are shying away from a lot of lessons learned. I think that's a very understandable human reaction, but it's not necessarily the best pathway to a better outcome next time. There are painful lessons that we really need to understand. It's as wrong to say Iraq and Afghanistan prove that counterinsurgency works as it is to say those conflicts prove counterinsurgency can never work. We're paid to be smarter than that. Until we figure out what actually happened on the ground, it's going to be hard to come to any kind of judgments.

AS SOON AS YOU HAVE A US GENERAL OFFICER AND A SATELLITE DISH ON THE GROUND, THINGS CHANGE.

The issue, of course, is also obscured by politics, with Democrats blaming Bush for invading Iraq in the first place and Republicans blaming Obama for leaving Iraq and allowing ISIS to return. A similar discussion is now brewing around Afghanistan. I think it behooves those of us who are professionals to set aside all the political bullshit, for lack of a better term, and really look at the facts.

BORER: There is a presumption that small countries can reproduce what the United States is doing. Do you have any thoughts on that, based on your experience in the Western coalition?

KILCULLEN: I think it's a classic error to believe that our capabilities can be replicated by a partner or by certain members of our coalition. One example you see is people copying drones and trying to field their own drone programs because that is what they think they should be doing. People also try to copy and replicate the time-sensitive targeting cycle. It's a lot like saying, "I want to be a high-end cardiac-thoracic surgeon in an operating theater" when, in reality, you are a bush doctor in a village somewhere. Without the right resources, you are worse than useless, because you've structured yourself around the expectation that you'll have certain information at certain periods, certain communications tools, and certain reaction mechanisms that you may not actually have. I think there is a real danger in trying to copy something that seems sexy and useful without any real ability to accomplish it.

That said, I think that we have often also failed by neglecting to look at what is working on the ground and then creating something similar but not exactly the same—something designed to work in that specific environment. A classic example would be village stability operations in Afghanistan. Initially, it was about helping the Afghans, who already knew how to fight, determine ways to build legitimate, local-level political authorities so they could attack the Taliban from a political and governmental standpoint. Within six months, it became the formation of local Afghan militias to fight the Taliban. In other words, we went from something that was fundamentally an armed propaganda and political agitation activity designed to help local populations organize local governance, to putting an SF team on the ground to deal with infiltration. This is a typical pathway, where you take something that is small and works, and then rapidly pump it up into something much bigger to replicate that success. And then you find that there was something magical about the way it was done originally that just doesn't survive the transition to a large project—and it all falls apart. That's the tragedy of a lot of what we do. We go in and pump money into something that works, just to watch it break.

WE GO IN AND PUMP MONEY INTO SOMETHING THAT WORKS, JUST TO WATCH IT BREAK.

The counterexample, which I think is a positive one, is what we have seen in Colombia. The Colombians have really gained ownership and taken control of what is going on there, and they have designed a series of equipment solutions and procedural solutions that work for them. They have listened to our advice, they have thought about it, and then in many cases respectfully said, "That's great, but we are going to do it another way instead." The result is a set of locally appropriate technologies that suit their needs and are, by definition, affordable and legitimate. It's not a matter of Americans coming in and trying to apply a template of something that works for us in a radically different environment. The Philippines is another example where it has worked, but the Balikatan exercise structure is fairly unique to the Philippines.[4] And in the case of Colombia, there is a remarkable pool of talent on the Colombian side. The human capital is dramatically better than what we saw in Iraq or Afghanistan, where people have come out of 30 years of war and 40 years of dictatorship, and naturally need a period of recovery before they can get back on their feet.

Military police, Bogotá, Colombia

BORER: To an outside observer, it might seem that insurgents put far more emphasis on information operations [IO] than counterinsurgency operators do. Can you speak to the importance of information operations in both insurgency and counterinsurgency strategies?

KILCULLEN: The answer to that depends on what you mean by information operations. I think insurgents often decide what their information strategy is going to be and then structure all their operations—including communications and kinetic operations—around achieving that particular goal. The classic example would be the Taliban in 2006 and 2007, when you saw a Taliban commander on Al Jazeera doing interviews. One of the things he did was issue general information directives, and then local commanders would design operations to support that message. In other words, they decided on the message first and then planned the operation to support it. We take the opposite approach, designing the operation first and then deciding how to sell it. This becomes the IO plan. IO is literally an afterthought for US operators. For the Taliban, if that statement the commander made on Al Jazeera was an operations order, the order itself would be the IO plan, and all of the supporting appendices would be the physical operations that were carried out to fulfill the plan. So the insurgents completely flip the way that they approach IO and kinetic operations.

This strategy was short-lived in the case of the Taliban. After their spokesman [Taliban commander Dadullah] Akhund was killed, they adopted a completely new and less effective model. So that is my other point: sometimes the best way to achieve an IO goal is to shoot the right person in the head. Sometimes it's a kinetic action that is going to have the IO impact you were hoping for. It may be that your strongest messaging is not leaflet drops and radio and the internet, but just removing a key player from the battlefield. There are plenty of examples of this effect in Iraq and Afghanistan, where enemy activity in a given sector drops off to zero. And it's not because of any particular change in ideology but just because you managed to wipe out the right guy.

SOMETIMES THE BEST WAY TO ACHIEVE AN IO GOAL IS TO SHOOT THE RIGHT PERSON IN THE HEAD.

Some research shows that whether a population supports a particular group ideologically or subjectively has very little to do with the degree of cooperation with that group. It's much more about who is creating a set of rules and sanctions that make the population feel safe by bringing predictability to their lives. I argue in one of my books that you can characterize that as "competitive control." Hearts and minds, at least insofar as getting people to like you, are much, much less important than we like to think. Behavioral change tends to follow incentives that you correct through a normative system. Some of those are through communication, but a vast majority of them are administrative.

BORER: Maybe you can come back around to that again as it relates to ISIS. In your recent article, "Blood Year," you describe ISIS as a state-building enterprise, but you stop short of calling it a state.[5] Yet you seem to be uncomfortable with Audrey Cronin's calling it a pseudo-state.[6] Have your thoughts evolved since you published that article?

KILCULLEN: Yes, they have, and I am in the middle of turning that article into a full-length book. The environment has dramatically evolved since I finished writing that article. The United States is a signatory to the 1933 Montevideo convention, which says that there are four criteria an entity must meet to be considered a state in international law.[7] First, you have to have a territory—a permanent territory that you control. Second, you have to have a stable population within that territory; it can't be nomadic or transient. Third, you have to have a government that claims authority over that population. And fourth, you have to be capable of contributing to relationships with other states. The convention says explicitly that you don't actually have to be recognized by other states to have relationships; you just have to be able to participate in relationships.

If we apply those four criteria to ISIS, we can see that it controls territory—it's about the size of Israel, or even a little larger now. It also controls a permanent population about the size of Norway's. ISIS has its own economy, with roughly $600 million in revenue per year. And while that is small for a state, it's large by terrorist standards—bigger than almost any other insurgent group in history. So it has an economy. Third, it has a government that exercises a degree of control over the population. We may not like that government or agree with its methods or even consider it to be effective, but it is a government. And finally, ISIS sells electricity and water to the Syrian government, and it trades oil on the black market, and it has the ability to enter into international relations.

ISIS IS NOT AN INSURGENCY. IT IS RUNNING A CONVENTIONAL FIGHT, CONTROLLING CITIES.

So I disagree with Dr. Cronin, but only because she calls ISIS a pseudo-state—which technically means a fake state, like it's pretending to be a state when it's not. I think it is a para-state—that it's almost there. It's on the verge of meeting, or is already meeting, all four of those key criteria.

This is not to suggest that we should recognize ISIS as a state. I think that would be a significant mistake. For example, people who challenged Australia to support ISIS are subject to be charged under what's called the Foreign Recruitment Act of 1977. But if you support a state and travel to join the armed forces of that state, you have a defense under that act. As soon as we declare ISIS a state, those people who support ISIS can defend their actions under that act.

So, on the one hand, there are good legal and political reasons not to call ISIS a state. But on the other hand, we do need to treat it as a state-like entity for targeting purposes. This is not a counterinsurgency environment; ISIS is not an insurgency. There is actually no danger that we will be sucked back into a counterinsurgency, because it's not an insurgency. ISIS is running a conventional fight, controlling cities. It's a state—a state-like entity. Yes, it's a revolutionary state that is trying to overthrow the state system, but that's not unique to history. The Soviet Union before 1924, or China after 1949, or the Islamic Republic of Iran after 1979—these are all now states, part of the international state system, but all of them started off with the goal of overthrowing the entire system and then creating something better. It's unlikely, but not impossible, that ISIS will follow a similar path.

BORER: In the article, you also note that there is a lack of political will today to treat the conflict with ISIS as a state, or state-like, fight. Under what conditions could you foresee a change in that attitude?

KILCULLEN: That, to me, is the most important critique of what I write in "Blood Year." Dr. Cronin's critique—and it might be true—is that there's no way at this point that the current US administration or the American people will support a full-scale, conventional fight against ISIS. I think she might be right about that.

We've seen two major changes in just the last month, and we have yet to learn the outcome or the impact of those changes. One of them is Turkey's entry into the war, which has not only significantly increased the pain ISIS is suffering but also brought the Turks into direct conflict with some of the Kurds who are fighting most effectively. The other is the Iran nuclear deal. And while personally I'm not convinced that the deal will prevent Iran from obtaining a nuclear weapon in the long term, I do think it may create the basis for some form of collaboration between Iran and the United States for stabilizing both Iraq and Syria. That may have been the real geopolitical reasoning behind the administration's push for the deal. Frankly, I am not confident that it will work, because it would severely alienate—and already has alienated—the vast majority of our allies in the region. We need to ask ourselves, "What am I trading here, and am I getting more than I'm giving away by pissing off the Israelis and the Saudis and everybody else for the sake of getting the Iranians on board?"

It might come down to Syria. I don't think there is any hope that we can stabilize Iraq or solve its problems until we reach some kind of resolution in the Syrian civil war. We are not going to get a political resolution until we can convince the majority of armed actors that they are better off negotiating than continuing to fight. That's the military role: to do enough damage—much like in Kosovo—to the Syrian Arab Republic, to ISIS, and to others, to convince them that the better option is negotiation. I will also repeat something I have heard a lot from Syrian peace activists in the last six months, which is that ISIS needs to go, Assad needs to go, but the regime needs to stay. We need some kind of framework to allow for a long-term political resolution. This is where the Iranian nuclear deal and other factors may start to lay the foundation for a collaborative approach. Until we do that, we can beat back ISIS forever in Iraq, but it's not going to make a long-term difference.

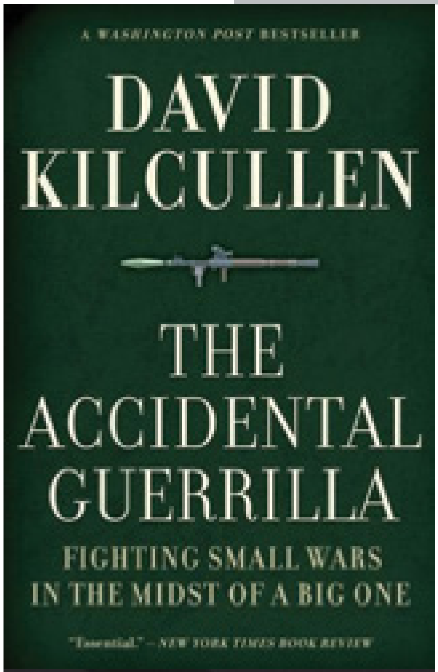
BORER: Going back to *The Accidental Guerrilla*, which seems to have launched your public career, do you think that term—the "accidental guerrilla"—and the concepts embedded in the book could help us understand the phenomenon of the lone-wolf terrorist?

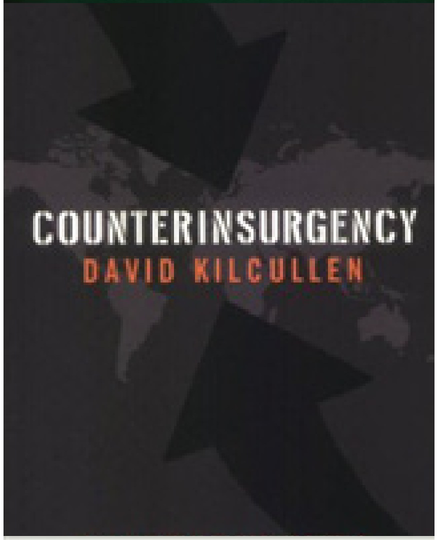
KILCULLEN: Yes, I do. Let me say up front, though, that I think the idea of an accidental guerilla is, at some level, an easy insight. Obviously, when you send a large expeditionary force into somebody's home turf, you are going to piss off a lot of people, and some of those people are going to take up arms against you.

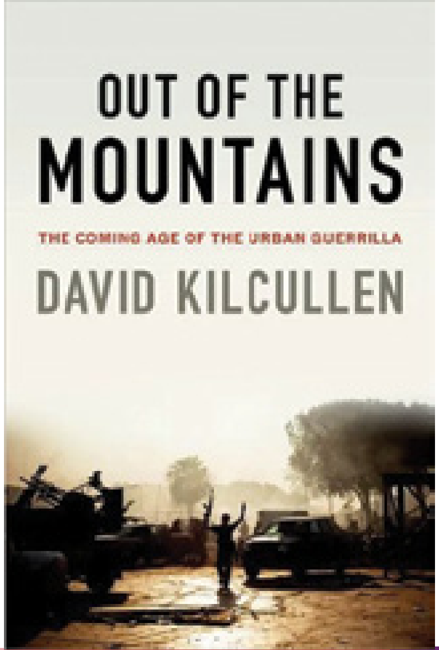
The point I was trying to make in *The Accidental Guerrilla* is that "radical" is not the start of any insurgent group's life cycle. They tend to emerge on the side of law and order, clean government, or identity. They gain a lot of support initially. And then they outlive their welcome, and they radically piss everybody off, and that's when you start to see the rise of internal opposition. What we did in many cases—Iraq and Afghanistan are both good examples—was intervene in the middle of that life cycle and then turn everybody against us when, in fact, those groups were already losing a lot of support. If we had gone about it in a different way, we may have been able to accelerate the cycle and watch them get kicked out on their ear without having to intervene. That's a great answer, and an argument for what we should have done after 9/11, though nobody involved at the time would have adopted that point of view.

Of course, it's arrogant to say in hindsight, "Oh, that's what we should have done." But you can apply the same idea to the lone-wolf terrorist phenomenon. An analogy I use in the book is this: Imagine that a criminal gang moves into your neighborhood and starts robbing the rich people's houses on the other side of town. If the police come in and start demolishing houses in your neighborhood and running checkpoints to find the bad guys, that will just turn everybody in the neighborhood against the police. That's the accidental guerilla syndrome. And it has actually happened to a lot of people in Muslim-minority communities in the West since 9/11.

In my view, there are three really negative dynamics from what Western countries have done. One is that exact phenomenon, the accidental guerrilla. Guys from Manchester start bombing in London, and suddenly there is this massive security crackdown on a bunch of young blokes in Manchester and the Midlands. And soon you end up with another crop of guys who are thinking differently about the British state.


A WASHINGTON POST BESTSELLER
DAVID KILCULLEN
THE ACCIDENTAL GUERRILLA
FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE
"Essential." —NEW YORK TIMES BOOK REVIEW





The second outcome is within the Muslim communities in our own societies—the United States, Australia, France, Britain—after 9/11. These Muslim communities established their own contact groups of notables and elders, and the idea was that the government would engage with them and run policies by them so that these communities could police themselves with their own internal security systems. What it actually did, though, was move older, mostly male, religiously and socially conservative elders to the top of the community hierarchy, to act as middlemen for groups of young people who were already pissed off. In essence, it further alienated members of those communities who were already alienated. Now, not only were they feeling disenfranchised and alienated from the parent society, but they also felt cut off from their own society. This is the case particularly with women who join the Islamic State—a kind of double disenfranchisement. It's ironic but true that, in some ways, a young woman is going to win more respect in ISIS than in the Pakistani community in London.

The third issue, along those same lines, is young people. We are seeing a young crowd of people joining ISIS. These recruits are war-on-terror natives; they have grown up in a post-9/11 environment that is, in our view, a temporary aberration but for them is the norm. And their reaction to this "new normal" is a feeling of disenfranchisement and a desire to take action of their own. I think this is a key consideration regarding where the accidental guerilla syndrome has come home to roost domestically since 9/11. Other examples fall under the category of what French philosopher Michel Foucault called "boomerang effects," where you manage a colony overseas a certain way and then turn around and apply the same kinds of techniques to the domestic population. I think we are seeing this already with things like domestic surveillance. Certainly the disenfranchisement and alienation of Muslim communities in the West is a great example of the accidental guerilla syndrome as well.

WE SEE A YOUNG CROWD OF PEOPLE JOINING ISIS. THESE ARE WAR-ON-TERROR NATIVES.

BORER: When you look back at history, is there any period—the Thirty Years' War, for example—from which we can draw parallels that might help us make sense of what is going on today?

KILCULLEN: You mentioned the Thirty Years' War in Europe. The former prime minister of Iraq made that comparison more than once. What he is talking about is the emergence of a region-wide Sunni-Shi'a proxy conflict in the Middle East. One of the key lessons there is to realize the West's limited potential to influence the situation. If this is another Thirty Years' War, then within that analogy the United States probably plays the same role as the Ottoman Empire. Imagine if the Ottoman sultan had tried to make peace in the middle of the Thirty Years' War. It would never have happened, right? In fact, many of the European state systems involved eventually unified *in opposition* to perceived threats from the East, from the sultan. In some ways, the West creates a unifying effect, but it's a unification by opposition to other people. As soon as we try to influence the situation or play the role of mediator, we run up against the fairly sharp limits of what we can do.

Another example is one we touched on earlier while discussing Audrey Cronin. She wrote a really useful paper, almost 10 years ago now, about what she called the electronic *levée en masse*.[8] She was looking at the period immediately following the French Revolution, when this massive explosion of printing technology, literacy, and the ability to build bridges between people with the written word led to significant shifts in the patterns of warfare. You went from small, professional armies that fought for a personal sovereign for a defined number of months per year in accordance with very specific rules to recruiting these mass armies motivated by public propaganda issued through print communications. What we are seeing now is, I think, the effect of a massive explosion in electronic connectivity, particularly in the developing world, since the year 2000. My go-to quote is that, in the year 2000, there were 30,000 phones in the whole country of Nigeria. Today there are 113 million. That's a 280,000 percent increase in just over a decade. And we are seeing similar rates of increase in many of the countries affected by the Arab Spring, in Eastern Europe, in sub-Saharan Africa, and in Latin America. The result is a radical shift in the information environment, and in the ability of non-state actors to organize action, transmit messages, and share information.

Dr. Cronin wrote that paper well before most of this happened, so it's very prescient in that respect. The nine years since that paper came out have reinforced her point: What is new about the current operation environment is not the weaponry, and it's not the tactics, and it's not the types of actors. It's the opponent's ability to communicate and share information and organize in near-real time, enabled by this massive explosion of connectivity. That's something we want to think about carefully when considering where our capabilities need to go next.

BORER: I usually like to end with the "king for the day" question. If we could make you king for the day—if you were the next US president, and you had the ability to bypass Congress and do one important thing for US national security, what would you do?

KILCULLEN: Wow, that's a great question. This is going to sound weird, but I think the solution to many of our military problems over the last 15 years lies

Hundreds of thousands of Bahrainis taking part in march of loyalty to martyrs

in a complete restructuring and revamping of civilian capability. We often leave the military hanging by asking them to do something that is not their job, that is actually the job of another agency, only to find that that agency just doesn't have the capacity, or the capability, or the political willingness to go out on the ground and do it. I would focus most of my efforts during my one day, then, on enabling civil agencies in the US government to partner effectively with military forces on the ground. There are lots of factors involved, but most important is making people understand that it's not acceptable to just leave everything to the military. There is a whole-of-nation requirement here, and if you are unable to execute your side of the operation, you will continually put the military in an unwinnable situation. It will only be able to achieve its goals halfway and then fail to close the gap to the desired political outcome. This is a big lesson for us from the last 15 years. But the very fact that you have to frame the question hypothetically means that it will never happen, right? So, knowing this, we have to think about what we should do next, and when.

BORER: On behalf of the school and the Department of Defense Analysis, I want to thank you for this interview. ❖

ABOUT THE INTERVIEWER

Dr. Doug Borer teaches in the Defense Analysis department at the US Naval Postgraduate School, Monterey, California.

NOTES

[1] The Combating Terrorism Archive Project (CTAP) aims to collect and archive knowledge on strategy, operations, and used by military and other security personnel from around the world in the twenty-first–century fight against global terrorism. Collectively, the individual interviews that CTAP conducts will create an oral history archive of knowledge and experience in counterterrorism for the benefit of the CT community now and in the future.

[2] This interview was edited for length and clarity. Every effort was made to ensure that the meaning and intention of the participants were not altered in any way. The ideas and opinions of all participants are theirs alone and do not represent the official positions of the US Naval Postgraduate School, the US Department of Defense, the US government, or any other official entity.

[3] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009); *Counterinsurgency* (Oxford: Oxford University Press, 2010); *Out of the Mountains: The Coming Age of the Urban Guerrilla* (Oxford: Oxford University Press, 2013).

[4] The annual Balikatan exercises bring together members of the US and Philippine armed forces to undertake joint humanitarian projects throughout the Philippines. See the Marine Corps website: http://www.marforpac.marines.mil/Exercises/Balikatan.aspx

[5] David Kilcullen, "Blood Year: Terror and the Islamic State," *Quarterly Essay* 58 (2015) (subscription required).

[6] Audrey Kurth Cronin, "ISIS is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat," *Foreign Affairs* (March/April 2015): https://www.foreignaffairs.com/articles/middle-east/2015-02-16/isis-not-terrorist-group

[7] See article 1 of the Convention on Rights and Duties of States (Inter-American), 26 December 1933, T.I.A.S. 881: http://avalon.law.yale.edu/20th_century/intam03.asp

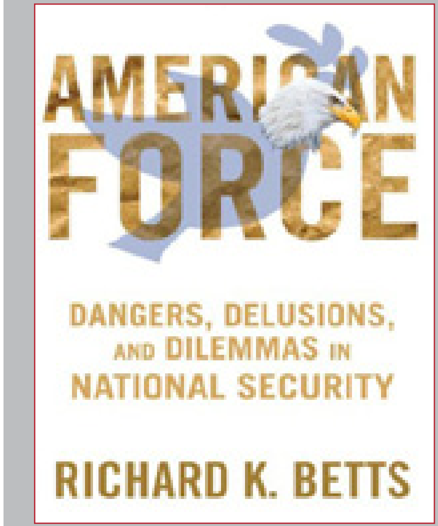
[8] Audrey Kurth Cronin, "Cyber-Mobilization: The New *Levée en Masse*," *Parameters* (Summer 2006): 77–87: http://spgia.gmu.edu/wp-content/uploads/PDFs/Audrey_Kurth_Cronin/cybermobilization.pdf

THE WRITTEN WORD

American Force: Dangers, Delusions, and Dilemmas in National Security

Reviewed by MAJ Bradley J. Krauss, US Army

A lengthy absence from the academic world can make returning to graduate school an intimidating proposition. Those of us who have been military practitioners more than theorizers over the past decade have found it necessary to push aside introspective thought in favor of preparing for the current or next challenge. When the time finally comes to make the leap back into academia and expand our minds' ability to think critically about the world, we inevitably face some start-up costs: recalling and dusting off long-forgotten theories, catching up on domestic and international events and their consequences, recalling the lessons of history that apply to current realities, and thinking critically about where we stand as citizens and professionals. If I could recommend one book to a friend who is preparing to embark on a graduate-level study of national security in general or defense analysis in particular, Richard K. Betts's *American Force: Dangers, Delusions, and Dilemmas in National Security* would be that book.[1]



American Force: Dangers, Delusions, and Dilemmas in National Security

by Richard K. Betts

New York: Columbia University Press, 2012
Paperback: US$22.00
367 pages

This collection of essays, some not previously published and others recently revised, focuses on the United States' role as the sole post–Cold War superpower and the current threats to its continued peace and security. Betts's dedication of the book to a young Army officer killed in Iraq at the height of the surge in 2007 may initially lead the reader to think that *American Force* is an overall condemnation of American interventionism and militarism, typified by the second invasion of Iraq in 2003. This assumption would be only partly true. While Betts is highly critical of the invasion of Iraq under false pretenses, he does not oppose the general principle of using military force to achieve political objectives. He does favor using the military decisively in circumstances where it can genuinely further US national interests. Betts also notes that not every adversity requires military force and not every upheaval is truly a threat. In sum, *American Force* seeks to both define the national security landscape and lay out options for those charged with maintaining it.

In "Part I: The Post–Cold War Hiatus," Betts describes how the United States effectively built the NATO alliance as an extension of American power and influence to deal with the Soviet Union. This strategy proved effective: it brought about the USSR's collapse, ended the Cold War, and ushered in an era of US unipolarity. With the end of the persistent threat of large-scale nuclear war, the United States no longer feared a debilitating attack from a single near-peer competitor but began to suffer unexpected lesser pinpricks from smaller developing states and non-state actors. No longer hindered by the need to confront communism and the Soviets at every turn, the United States was free to intervene wherever it saw fit. What US leaders must do more effectively, Betts argues, is first determine the criteria for intervening militarily and once the decision to intervene is made, fully commit to resolving the crisis—and avoid jumping only halfway across the ditch.[2] Additionally, while the threat from weapons of mass destruction (WMD) is still very real, today we expect them to arrive under the radar, in the hands of a rogue actor instead of atop a state's intercontinental ballistic missiles. Betts contends, however, that the United States still relies too heavily on using its nuclear capability to deter states; those actors most likely to use WMD do not have a return address against which states can retaliate.

"Part II: History Strikes Back" tackles the difficulties and challenges facing the United States in the post-9/11 world: terrorism, military interventions ranging in scale from covert action to outright war, China's rise, and Russia's resurgence. In most cases, Betts notes, terrorism offers a high psychological impact compared to the relatively minor physical damage it imparts, and so will remain a popular tool for those who oppose the United States' global primacy but are ill-equipped to match its military might. For those instances in which the United States does consider confronting an identifiable opponent with force, Betts argues that the US military must maintain a minimum spectrum of capabilities, from deterrence to counterinsurgency to conventional superiority. This will ensure that the US effort will be both effective (the policy objectives are achieved) and efficient (success comes at the lowest possible cost in blood and treasure). Despite the fact that neither China nor Russia can rival raw US military power and professionalism, China's continued rise as a regional hegemon in the western Pacific and Russia's attempt to reassert power against NATO represent the only true threats to unipolarity. Betts advises that both should be countered through either a multilateral approach, the reassertion of Western hegemony, or a balance of power. He underlines this entire discussion on the use of force with an argument that the preemptive use of force has validity in international law, while wars of prevention are in essence acts of unprovoked aggression.[3] In the twenty-first century, one of the more tempting preventive measures is air strikes. Betts warns that when weighing the merits of such a strike ahead of time, decision makers should consider not only what they know the strike might destroy but also what might be hidden from them and left intact.[4]

THE PENTAGON SHOULD AVOID FRIVOLOUS SPENDING ON THE PURSUIT OF NEW CAPABILITIES AT THE EDGE OF THE "REALM OF THE POSSIBLE."

Finally, in "Part III: Decision and Implementation," Betts questions how accurate Samuel Huntington's models of civil-military relations are today, given the drastic changes in the geopolitical environment since *The Soldier and the State* was published in 1957.[5] Betts notes that although most democracies' civil-military relations tend to lie somewhere between the extremes of outright hostility and perfect harmony, the system works as long as senior military leaders don't become political appointees and the military and political leaders can openly discuss their views with each other. He then seeks to answer the question of whether even a well-crafted strategy—a necessary preparation for waging war—can tie political objectives to military outcomes in a meaningful way. To do so, he outlines 10 critiques of how well strategies (and by extension, strategists) predict the best way to link policy with operations to achieve victory.[6] To avoid sounding like a pessimist regarding the importance of aspiring to good strategy, Betts provides a rebuttal to each critique. He concludes that for strategy to be effective, the use of force should generate significantly more benefits than costs; strategies should be kept as simple as possible; and policy makers need a strong understanding of the military tools they seek to deploy.

Before concluding this section, Betts takes on a topic that tends to be a lightning rod in discussions of this nature: defense spending. He notes that US defense spending today is at about the same level it was (adjusted for inflation) during the Cold War, even though the United States no longer faces a near-peer enemy like the Soviet Union. The Pentagon, he concludes, should focus on emerging threats and avoid frivolous spending on individual services' pet projects or the pursuit of new capabilities at the edge of the "realm of the possible."

Now that I'm in the second quarter of my graduate studies, I find that *American Force* offers an informative perspective on many of our class discussions. Betts has something valuable to say for anyone who needs to get the juices of critical thinking flowing or generate some original thought in class. For instance, his discussion of the military interventions in Kosovo and Bosnia were directly relevant to our studies of peacekeeping operations in a class called "Joint Military Operations," and his critiques of strategy would have made for lively discussions in the Naval War College's "Strategy and Warfare" course. Betts's explorations of nuclear deterrence, China's rise, just war theory, and civil-military relations would be useful background for deterrence studies. Finally, the material he covers on "big small wars," terrorism, cyber warfare, and military interventions is centrally relevant to studies of conflict in the information age.

One area where Betts could have provided a more in-depth analysis concerns US options for dealing with the rise of militant Islam. He gives cursory attention to radical Islamism within the context of his chapter on "Terrorism" but suggests that terrorism is a reaction within the Muslim world to US hegemony and the worldwide propagation of Western media, politics, and popular culture. In fact, Betts gives fewer than four pages to addressing the root causes of violent jihad, and even fewer to evaluating whether terrorism is simply a tactic chosen to pursue broader political objectives. He may have done this intentionally to avoid getting bogged down in an unsolvable argument over motives and intentions. Instead, he emphasizes that because the actual risk of becoming a victim of Islamist terrorist violence within the United States is so ridiculously low (and will remain low, unless a group like al Qaeda gets its hands on WMD), there is little need to waste time and energy worrying about solving the underlying issues. He seems to propose that the United States should resign itself to the ire of the Muslim world because, on the one hand, it won't back down from its obligations and commitments in the Middle East and on the other hand, the prospects that the United States will be able to effectively recast itself as a benign force for good in the region are very low. Interestingly, one danger that Betts does acknowledge is a future war, not against sub-state Islamist actors but "against a coordinated international coalition of revolutionary Islamist regimes."[7] If the rise of ISIS over the past year represents the beginning of such a movement, perhaps Betts will reconsider his position and entertain the notion that the United States should devote greater energy to understanding and addressing the underlying motivations of jihadist violence instead of trying to simply bomb these groups into submission.

THE UNITED STATES SHOULD RESIGN ITSELF TO THE IRE OF THE MUSLIM WORLD.

One other small point of contention I have with *American Force* is its imprecise use of the term "unconventional warfare" (UW). For special warfare practitioners, like me, this term has a very specific meaning that involves using an auxiliary, underground guerilla force to disrupt, overthrow, or coerce a government. *American Force* first addresses "unconventional warfare" in the introduction with the claim that "unconventional, irregular, or asymmetric warfare ... takes place in the midst of civilian populations and collateral damage is usually extensive—and it is unconventional warfare that is most common in the unipolar world."[8] UW practitioners would argue that, by our definition, unconventional warfare is uncommon, especially from a US perspective. Furthermore, unconventional warfare itself is not inherently violent, though it can use violence as a tactic. In chapter five, Betts refers to Iraq and Afghanistan as "unconventional wars" and also claims that "technological substitution for manpower gives the modern American military its edge, but it cannot be applied very well in unconventional warfare."[9] I believe the confusion is unintentional and that Betts uses "unconventional warfare" interchangeably with "asymmetric warfare" or even "counterinsurgency" to describe the characteristics of a given war, rather than using the professional definition of it as a method for waging a specific type of warfare. Only readers like me, with specialized knowledge, will take issue with such an imprecise use of terms. If *American Force* is truly meant to appeal to the national security practitioner, however, then Betts should pay more attention to the precision of his terminology.

In the preface to *American Force*, Betts worries that readers who are practitioners of national security may find *American Force* glib, arrogant, or inhumane. To the contrary, I found his arguments to be insightful, thought provoking, relevant, and devoid of partisan rhetoric. *American Force* is a well-rounded exploration of US national security policy and the use of military force that is a must-read, not only for experienced and aspiring practitioners but also for the average reader who is interested in understanding current US activities abroad. ❖

ABOUT THE REVIEWER

MAJ Bradley J. Krauss is a US Army Special Forces officer and graduate student at the US Naval Postgraduate School.

NOTES

[1] Richard K. Betts, *American Force: Dangers, Delusions, and Dilemmas in National Security* (New York: Columbia University Press, 2011).

[2] Betts, *American Force,* 12. Betts quotes from Carl Von Clausewitz's famous treatise, *On War*: "A small jump is easier than a large one, but no one on that account, wishing to cross a wide ditch, would jump half of it first." Betts returns to this metaphor several times to highlight instances where a military objective is known but the commitment to achieving it is half-hearted or incomplete and leads only to failure. For the original quote, see Book VIII, chapter 4 of Carl von Clausewitz, *On War*, Clausewitz.com, n.d.: http://www.clausewitz.com/readings/OnWar1873/BK8ch04.html

[3] People are sometimes confused about the difference between the terms *preemptive* war and *preventive* war. One side starts a preemptive war when it receives or perceives a credible, active threat of aggression from an opponent and chooses to act first. International law upholds the right of a state to preempt an imminent attack. A preventive war, by contrast, is launched by one side against a perceived opponent with the intention to prevent a possible future threat from arising. International law does not recognize a right to launch preventive war.

[4] Betts, *American Force*, 139.

[5] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge: Harvard University Press, 1957).

[6] See Betts, *American Force*, chapter 10: "Plans and Results: Is Strategy an Illusion?"

[7] Ibid., 286.

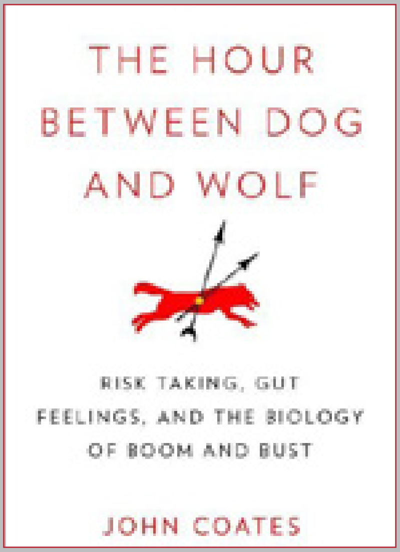
[8] Ibid., 13.

[9] Ibid., 153.

THE WRITTEN WORD

The Hour between Dog and Wolf

Reviewed by LT Adam Karagouz, US Navy



THE HOUR BETWEEN DOG AND WOLF

RISK TAKING, GUT FEELINGS, AND THE BIOLOGY OF BOOM AND BUST

JOHN COATES

The Hour between Dog and Wolf: Risk Taking, Gut Feelings, and the Biology of Boom and Bust

by John Coates

New York: Penguin Press, 2012
Paperback: US$15.07
339 pages

> The hour between dog and wolf, that is, dusk, when the two can't be distinguished from each other, suggests a lot of other things besides the time of day. … The hour in which … every being becomes his own shadow, and thus something other than himself. The hour of metamorphoses, when people half hope, half fear that a dog will become a wolf. The hour that comes down to us from at least as far back as the early Middle Ages, when country people believed that transformation might happen at any moment.
>
> —Jean Genet, *Prisoner of Love*[1]

Is there a relationship between the biological processes of the human body and our decision-making ability? According to John Coates, author of *The Hour between Dog and Wolf: Risk Taking, Gut Feelings, and the Biology of Boom and Bust*, the answer is an emphatic yes. Coates, a former derivatives trader turned neuroscientist, uses a fictionalized vignette of a Wall Street trading house to highlight the drastic changes in body chemistry that humans undergo during stressful events, in particular decision making under conditions of uncertainty.[2] The vignette reveals how corporate cultural incentives blend with the biological stew of chemicals and hormones circulating inside the average 20- to 40- year-old male trader to create the ideal conditions for irrational exuberance during market upswings and "excessive pessimism" during downticks. Coates refers to the latter condition as "learned helplessness," a state in which the traders feel that they have no control over their lives, and exuberance is replaced by withdrawal and depression.

Coates traces Western thought about human behavior back to Aristotle, on whom he bestows the title of "first biologist."[3] According to Coates, Aristotle did not draw such a stark mind/body distinction as philosophers who came after him—he viewed human beings as holistic systems in which perfect reason was impossible to attain due to the nature of emotion. Today, scientists are slowly warming up to the holistic approach as they learn more about the role that chemicals in the body play in how humans both perceive reality and make decisions.

Coates cites research indicating that three situational factors cause a spike in cortisol (the hormone associated with stress) in the human body: novelty, uncertainty, and uncontrollability.[4] The presence of one or more of these factors has a marked effect on decision making. With the spike in cortisol comes a lowered appetite for risk. Coates highlights advances in sports psychology that reveal that training can make it possible to adapt to these stress factors in much the same manner that muscles are conditioned by physical exertion.[5] Advances in our understanding of mind and body can be incorporated into training scenarios to improve both performance and resilience. This has interesting implications for efforts within the military and law enforcement to develop more resilience in their personnel—a process sometimes termed "stress inoculation." Coates also describes the toxic effects of chronic stress on the human body and cutting-edge attempts to mitigate it, in particular a method called "mental toughening." This is a field of inquiry involving physiology, neuroscience, and sports medicine that investigates how humans react to novelty.

In another fascinating passage, Coates points to the presence of a "testosterone feedback loop" in male primates as a contributing factor to irrational exuberance in market performance (a majority of traders are male).[6] He describes research that shows that the bodies of two competing males experience a surge of testosterone in preparation for an imminent conflict. The winner of the contest receives an additional spike in the hormone, while the loser's hormone surge quickly dwindles away. This is also known as the "winner effect," a well-documented outcome of perceived victory in some sort of competitive endeavor between male primates: the winner gets increased testosterone, the loser increased cortisol. Likewise, as male Wall Street traders execute profitable trades, their confidence and aggression are heightened by the flush of additional hormones triggered by success. In an organizational construct that rewards short-term profits and bold action, this is a recipe for disaster.

COATES POINTS TO THE PRESENCE OF A "TESTOSTERONE FEEDBACK LOOP" IN MALE PRIMATES.

The main point Coates is making is to warn about the dangers of overconfidence and how the biological processes within the human body can foster overconfidence. This observation has concrete applications to the special operations world. SOF leaders regularly face decisions about whether to launch an operation under suboptimal conditions, for instance, with minimal intelligence or at the edge of environmental limitations for a given mobility platform. For example, perhaps an assault force learns from tactical questioning while on target that the targeted individual is several city blocks away but about to depart the area. The ground force commander must quickly weigh many competing variables, such as asset and force availability and conditions on the ground, before deciding whether to move to another location. Excessive aggression or overconfidence in these situations can lead to mission failure, as some have learned the hard way.

In one section, Coates alludes to the benefits of "thermal stress" for increasing resilience and mental toughness in human beings. If true, it would seem to confirm that there are added and unforeseen benefits to SOF training, with its emphasis on arduous environmental conditions. He writes:

> One type of toughening [regimen] is especially intriguing, and that is exposure to cold weather, even to cold water. Scientists have found that rats swimming regularly in cold water develop the capacity to mount a quick and powerful arousal, relying on adrenaline more than cortisol, and to switch it off just as quickly. When subsequently exposed to stressors they are not as prone to learned helplessness. Some tentative research has suggested that much the same thing occurs in humans. People who are regularly exposed to cold weather or who swim in cool water may have undergone an effective toughening [regimen] that has made them more emotionally stable when confronted by prolonged stress. It is surmised by some researchers that the exercise itself, coupled with acute thermal demands, provides these people with an enviable pattern of stress and recovery. Perhaps the same effects could result from the Nordic practice of a sauna followed by a cold plunge.[7]

Coates points out that women and older men (roughly defined as over 50) are not subject to the same fluctuations of testosterone as young men, and he advocates that such individuals be included in teams that are involved in high-risk decision making.[8] Men experience a slow decline in testosterone from their mid-20s onward, and for this reason become gradually less susceptible to its influence. I am reminded of a quote attributed to the ancient Greek philosopher Plato regarding the "passion" of emotions that youth experience (and that we now know are caused by hormones such as testosterone):

> In particular I may mention Sophocles the poet, who was once asked in my presence, How do you feel about love, Sophocles? Are you still capable of it? To which he replied, "Hush! If you please: to my great delight I have escaped from it, and feel as if I had escaped from a frantic and savage master." I thought then, as I do now, that he spoke wisely. For unquestionably old age brings us profound repose and freedom from this and other passions.[9]

Women produce one-tenth the amount of testosterone that a man of similar age does and generally take longer than men to make decisions. Women are not necessarily more risk-averse, Coates points out; it's just that their time horizon is different.[10] He cites a 2001 study that followed thousands of male and female traders over a six-year period. The women in the study outperformed the men by 1.4 percent, and some researchers point to the fact that they traded their accounts with much less frequency than the men. Thus, while the women in the study may have taken longer to make decisions, they did take risks and did so in a more long-term, strategic manner than the men. Coates asserts that a more even balance of men and women working in financial markets "could not possibly do any worse than the system we have now" and that the inclusion of different types of risk evaluation would create a more stable market.[11] Missing from Coates' analysis, however, is the effect of hormones on women—in particular how fluctuations in their chemistry and the aging process may alter their perceptions and decision making in a manner different from their male counterparts.

THIS FINDING IS A THOUGHT-PROVOKING, HORMONE-BASED TAKE ON THE CONCEPT OF "GROUPTHINK."

This finding that the varying biological processes of young men, women, and older men can produce different risk evaluations across the groups is a thought-provoking, hormone-based take on the concept of "groupthink," in which a desire for conformity and group cohesion overrides critical analysis. It also has relevance to the current debate regarding the inclusion of women on special operations teams. According to Coates, their presence would have a positive effect on decision making. The inclusion of women and older men would provide a more hormonally balanced team that would be better able to evaluate risk versus gain in an ambiguous environment and thus prevent biologically induced groupthink from prevailing. This is a credible argument, and I agree with Coates, but improved decision making is only one facet of including women in SOF teams. Other aspects of this issue, such as unit cohesion and a myriad of second- and third-order effects, remain questions to be answered. Also, how the nuances of women's biology will influence their performance in a SOF setting is an area that requires further study and analysis.

In this thought-provoking book, Coates urges readers to follow the age-old adage to "know thyself" and reminds his readers that an integral part of self-knowledge is an understanding of the chemistry swirling inside the body. This chemistry has a marked impact on perception, resilience, and importantly, how humans evaluate risk. He advocates a return to the Aristotelian holistic conception of the body and mind, rather than conventionally held philosophies that separate the two. Finally, Coates recommends having a diversity of ages and genders on teams to add stability to high-risk decision-making and temper the pull of body chemistry on reason and rationality. ❖

ABOUT THE REVIEWER

LT Adam Karagouz is a US Naval Special Warfare officer.

NOTES

[1] Jean Genet, *Prisoner of Love*, trans. Barbara Bray (New York: New York Review Books Classics, 1986), quoted in John Coates, *The Hour between Dog and Wolf: Risk Taking, Gut Feelings, and the Biology of Boom and Bust* (New York: Penguin Press, 2012), 1.

[2] Coates, *The Hour between Dog and Wolf*, 10.

[3] Ibid., 35.

[4] Ibid., 217.

[5] Ibid., 240.

[6] Ibid., 180.

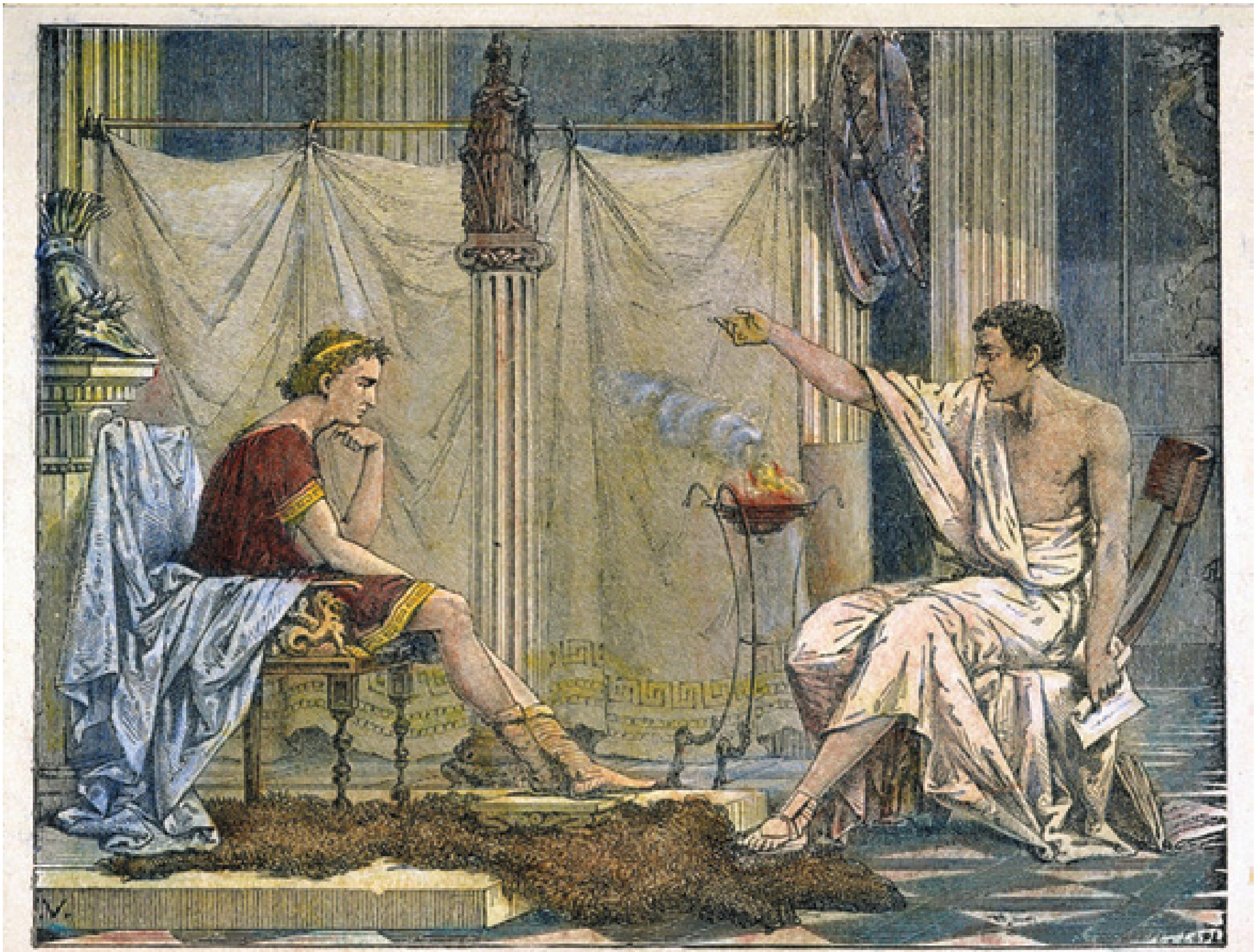
[7] Ibid., 252.

[8] Ibid., 275.

[9] Plato, *Republic* 329c.

[10] Coates, *Hour between Dog and Wolf*, 166.

[11] Ibid., 275.



ARISTOTLE AND HIS PUPIL, ALEXANDER.

THE MOVING IMAGE

Turn: Washington's Spies: A History Lesson on Irregular Warfare

Reviewed by Ian C. Rice

If you are interested in learning about one of the most important irregular warfare campaigns in American history, AMC's American Revolutionary War television series, *Turn: Washington's Spies*, is a great place to start.[1] Based on historian Alexander Rose's book *Washington's Spies: The Story of America's First Spy Ring*, *Turn* combines drama, suspense, and intrigue to bring to life the spies of the Culper Ring—relatively unknown yet important and audacious actors in early American history.[2] For those readers who have more than a casual interest in the dynamics of insurgencies and counterinsurgency operations, *Turn* also offers some thought-provoking reminders that population-centric conflicts may be more similar than they are unique—a consideration that merits continued investigation in our modern era of persistent irregular conflict.

In the year 1776, the British are pressing General George Washington's army on the battlefield, and the Continentals (as the colonial forces were called) need more human intelligence if they are going to change the course of the war in their favor. Continental officers Major Benjamin Tallmadge (Seth Numrich) and Lieutenant Caleb Brewster (Daniel Henshall) devise a scheme to recruit Americans to collect information on British military activities near New York City. To their surprise, Abraham "Abe" Woodhull (Jamie Bell), an old childhood friend from their hometown village of Setauket on Long Island, is their first—albeit reluctant—recruit. After Abe is arrested for smuggling cabbage across the Long Island Sound to British-held New York, Ben and Caleb soon convince him that spying for the American cause is preferable to jail. And so, with the help of another childhood friend, Mrs. Anna Strong (Heather Lind), Abe begins collecting intelligence for Washington's army. As Rose describes it, colonial Setauket was a typical small community where "everyone knows each other."[3] Thus, establishing a spy ring in such a community required confidence in one's close associates as well as knowledge of who might reveal the spies to the occupying British. For Abraham Woodhull and the Culper Ring, operations on Long Island were even more challenging because the area was well behind British lines and traditionally had a strong loyalist support base.[4]

Though Abraham and Anna, as the rebellion's operatives in Setauket, are the focal characters of the series, *Turn* also showcases many of the other historical figures who play prominent parts in Rose's book. Most notably, General George Washington (Ian Kahn), Major General Benedict Arnold (Owain Yeoman), Major John André (JJ Feild), and Major Robert Rogers (Angus Macfadyen) follow plotlines that build on their large roles in American history. This additional character development helps breathe some life into these legendary figures, who are often remembered only for their most famous deeds (or in some cases, their infamous misdeeds).

THE SPIES OF THE CULPER RING WERE IMPORTANT AND AUDACIOUS ACTORS IN EARLY AMERICAN HISTORY.

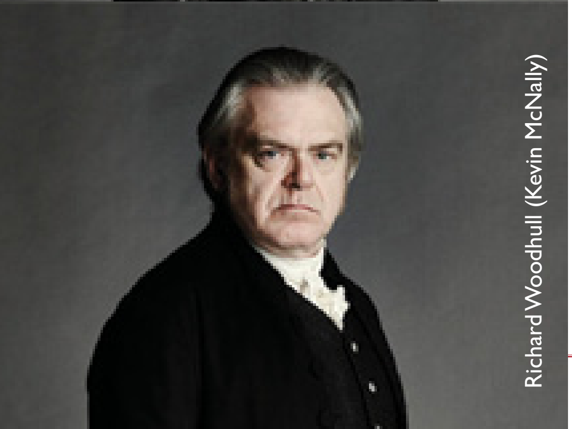
Although *Turn* offers interesting glimpses of eighteenth-century American life, including realistic-looking costumes, some creative use of blue-screen backdrops, and of course, many scenes filmed in the beautifully preserved town of Colonial

Abraham Woodhull (Jamie Bell)

Ben Tallmadge (Seth Numrich)

Anna Strong (Heather Lind)

Caleb Brewster (Daniel Henshall)


Richard Woodhull (Kevin McNally)

Williamsburg, Virginia, the plot is slow to develop, especially for a television spy series. This slow build-up of characters and plot follows Rose's account, however, and should be expected from a historically-based spy story. An actual covert spy ring needs significant time to build itself and develop channels for collecting useful information, all while staying hidden. To prevent the story of the Culper Ring from being boring television, therefore, *Turn*'s writers have predictably spiced up the characters and added some additional plotlines, just as they might for any television crime or spy drama. *Turn* has three love stories—and two of these are even love triangles! These side plots are endowed with enough colorful and suggestive content to keep cable viewers entertained. Across the first two seasons, the challenge for *Turn* seems to be how to skillfully interweave the main plotline of the Culper Ring's spying exploits and the overall history of the war with the numerous interpersonal dramas so that viewers stay engaged.

Is *Turn* historically accurate? Not exactly. But while *Turn*'s writers have not kept the plot historically pristine, Rose's historical account provides the inspiration for the series. For instance, some episodes deviate from the chronological order of certain historical events to help build the subplots and support character development. In one case, the central agent of the Culper Ring, Abraham, is credited with reporting to General Washington on the Hessian garrison in Trenton. This report then becomes the catalyst for Washington's famed surprise attack on that mercenary force on 26 December 1776.[5] In reality, Woodhull was not recruited as an agent until the spring of 1778, well after this important American victory.[6] There are other minor inaccuracies scattered throughout the episodes, but they do not detract from the overall storyline, and they add some interesting color to a television series that is trying to distill a large amount of historical material into an already short season of 10 one-hour episodes. Thus, *Turn* may not be the best source for studying the American Revolutionary War, but it is a great starting point for those who are interested in investigating the real history behind this television series.

Though *Turn* takes creative license with some historical details of the American Revolutionary War, the series writers have done their homework when it comes to depicting irregular warfare. The first two seasons sustain recurring themes that remind us that, regardless of the time and location, population-centric conflicts are often similar. The first theme, which runs through season one, can best be described as "The Battle for Setauket," in which the tiny British garrison struggles to keep the favor of the Setauket residents. Unfortunately for the soldiers, the British command manages to anger the people of Setauket through a series of arrogant missteps intended to improve the garrison's fortifications. Prior to this, many of the townspeople appeared tolerant, if not supportive, of the British garrison, but the soldiers' disrespectful treatment of the elders and traditions of the town turns American opinion from tacit support to overt antagonism. This kind of situation is not unique to eighteenth-century Setauket, but has played out in countless other villages with many different occupiers, whether in Afghanistan, Algeria, Iraq, Northern Ireland, or Vietnam, to name only a few examples. In irregular conflicts, the population remains the decisive terrain to win. The arrogant choices of the British garrison in Setauket lost it the small foothold it had among the people.

Turn's writers have also nicely crafted a conflict between the British garrison commander, Major Edmund Hewlett (Burn Gorman), and his aggressive subordinate, Captain John Graves Simcoe (Samuel Roukin). To the casual viewer, this is just a classic conflict of supervisor versus conniving subordinate. As the two men struggle for power, their disagreements over style and demeanor become more clear. Anyone who studies irregular warfare, however, will recognize that at the core of this interpersonal rivalry are quite different understandings of how to best ensure that Setauket and its people stay under the heel of British authority. On one side stands Hewlett, who relies on his intellect and legal authority as the town's military government representative to maintain order. Although Hewlett is portrayed as an overly educated, quirky, and paranoid military commander, he is convinced that the best way to "tame" the colony is by "winning hearts and minds" in Setauket. With their invocation of this Vietnam-era cliché, *Turn*'s writers have typecast Hewlett as a strategist who prefers counterrevolutionary methods that do not immediately require the use of military force.

Juxtaposed to Hewlett, Captain Simcoe is temperamentally imposing and physically intimidating—clearly a leader you want on your side in a fight. Simcoe sees himself as a loyal subject of the British Crown and as such, empowered to use all means necessary, especially brutal intimidation and violence, to ensure the Empire's subjects understand their place. Simcoe is more than just a bully, however. He is a tactically capable military leader, as we learn across the series' first two seasons: skilled in single combat as well as conducting operations to root out the American rebels—though perhaps he enjoys administering his brand of authority a little too much. Because he is driven equally by violence and ambition, Simcoe is often shortsighted in how he selects options to deal with the colonial subjects of the crown. In one scene, Simcoe shows his disdain for all American colonists, loyalist or rebel, when he reminds one rebel of who actually owns the town of Setauket.

> Except it isn't your town, is it? It belongs to our king. By rights. It's the arrogance of the colonies that you forget this. That's why I joined the Royal Army. To remind you in Guiana, the Caribbean, and now New York. I have enjoyed reminding you all over the world.[7]

Turn also reminds us that human intelligence operations are integral to winning population-centric warfare, whether the spy is a hidden insurgent biding her time to strike or a counterinsurgent perpetually visible as a symbol of order and authority.[8] This theme is apparent throughout the first two seasons of *Turn*: the paranoia of secret agents is everywhere, whether in sleepy Setauket, bustling New York City, or even in Washington's own camp.

In colonial New York, there were spies, and there were also spy catchers, just as today there are networks of insurgents and terrorists and those who hunt and attack those networks. This aspect of irregular warfare is also not lost on the writers of *Turn*. They remind us that one of the greatest heroes of the American colonial period, renowned for his daring feats of bravery and endurance, was also a feared British mercenary who stalked and captured the young rebel spy Captain Nathan Hale.[9] To this day, Major Robert Rogers (of Rogers' Rangers fame) is revered in the United States military as a guerrilla

Edmund Hewlett (Burn Gorman)

John Graves Simcoe (Samuel Roukin)

John André (JJ Feild)

Mary Woodhull (Meegan Warner)

Robert Rogers (Angus Macfadyen)

fighter, although he actually fought against the young United States during the Revolution and remains more legend than fact.[10] There is not even an authenticated likeness to associate with his exploits.[11] His duplicity is accurately depicted in the series: Rogers is not only a villain to the Americans; he is equally despised by his British masters because of his brutal tactical methods and his use of "Negroes, Indians, Mulattos, and Rebel prisoners" to fill the ranks of his irregular troop called the Queen's Rangers.[12] Rogers recruited men for their tracking and fighting abilities rather than for their social status and trained them in unconventional tactics to conduct raids and ambushes in support of British intelligence efforts against a sometimes equally unconventional enemy. His skills as a raider and a spy hunter, both in fact and as portrayed in *Turn*, were not all that different from today's special operations forces that attack networks of agents, couriers, financiers, bomb makers, and safe houses.

As I noted at the beginning of this review, *Turn* is entertaining television if one does not mind slow plot development and a few historical inaccuracies. More importantly, for those who analyze and study irregular conflicts, *Turn* can be a haunting reminder of the timeless nature of population-centric warfare. Although the places and players may change, the dynamics of this type of conflict often remain the same. The first two seasons are available through a variety of online vendors for your binge-watching enjoyment. Once you are hooked on the series and have caught up, you'll be happy to know that season three will premiere in the spring of 2016 on AMC.[13]

George Washington (Ian Kahn)

Peggy Shippen (Ksenia Solo)

Benedict Arnold (Owain Yeoman)

Robert Townsend (Nick Westrate)

Nathaniel Sackett (Stephen Root)

NOTES

[1] For the US Army's official definition of irregular warfare, see Headquarters, Department of the Army, *Insurgencies and Countering Insurgencies*, FM 3-24/MCWP 3-33.5 (Washington, D.C.: HQ, Dept. of the Army, 2014), 1-1: https://fas.org/irp/doddir/army/fm3-24.pdf

[2] Alexander Rose, *Washington's Spies: The Story of America's First Spy Ring* (New York: Bantam Dell, 2006).

[3] Ibid., 80.

[4] Ibid., 81. Historians typically estimate that 20 percent of the population in the American colonies were loyalists when the revolution broke out. Robert Middlekauff, *The Glorious Cause: The American Revolution, 1763–1789* (New York: Oxford University Press, 1982), 550.

[5] Middlekauff, *The Glorious Cause*, 357–60.

[6] Rose, *Washington's Spies*, 82–87.

[7] *Turn*, "Who by Fire" episode 2, (originally aired 13 April 2014). Also see the episode script at "Turn (2014) Episode Scripts," *Springfield! Springfield!*, n.d.: http://www.springfieldspringfield.co.uk/view_episode_scripts.php?tv-show=turn-2014&episode=s01e02

[8] See Kalev I. Sepp, "Best Practices in Counterinsurgency," *Military Review* (May-June, 2005): 10; and HQ, Dept. of the Army, *Insurgencies*, 4-13.

[9] Rose, *Washington's Spies*, 27–32.

[10] See John R. Cuneo, *Robert Rogers of the Rangers* (New York: Richardson & Steirman, 1988).

[11] Ibid., 281–83.

[12] Ibid., 275.

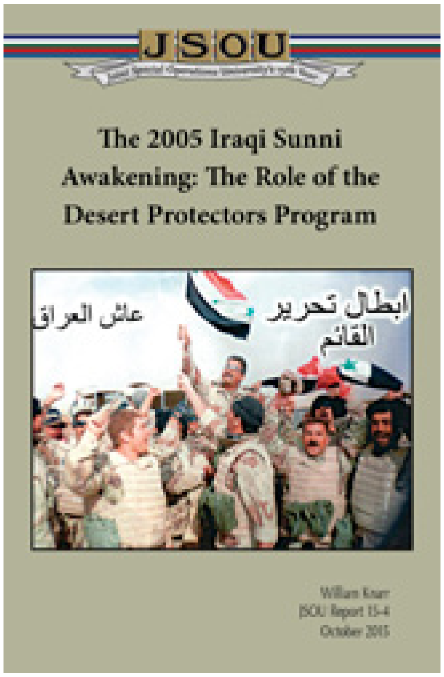
[13] Cynthia Littleton, "'Turn: Washington's Spies' Renewed for Season 3 by AMC," *Variety*, 15 July 2015: http://variety.com/2015/tv/news/turn-amc-renewed-season-3-1201541056/

JSOU PUBLICATIONS

These new JSOU Press publications are available electronically on the JSOU Library Management System website: https://jsou.libguides.com/jsoupublications

Special Operations Research Topics 2016
Issue Date: June 2015

The JSOU Special Operations Research Topics 2016 publication presents a list of SOF-related topics that are recommended for research by those who desire to provide insight and recommendations on issues and challenges facing the SOF enterprise. As in the past several years, this list is tailored to address priority areas identified by USSOCOM. There are five SOF priorities: Ensure SOF Readiness; Help Our Nation Win; Continue to Build Relationships; Prepare for the Future; and Preserve Our Force and Families. This publication also includes the Key Strategic Issues List (KSIL) developed and maintained by the USSOCOM J5–Strategy, Plans, and Policy Directorate. These topics reflect a consensus of the SOF experts who participated in the Special Operations Research Topics Workshop as being particularly worthwhile for addressing immediate SOF needs and building future capacity for emerging challenges. Topics may be narrowed or otherwise modified as necessary to suit school writing requirements or maximize individual interests and experiences.



The 2005 Iraqi Sunni Awakening: The Role of the Desert Protectors Program
by William Knarr
Issue Date: October 2015

Dr. Knarr tells the story of Al Sahawa, the Awakening, in Iraq from a perspective that is different from most narratives. Many associate the beginning of the Awakening with Sheikh Sattar Abu-Risha's 14 September 2006 proclamation in Ramadi, where he coined the term *Al Sahawa*. However, Dr. Knarr contends that the Anbar Awakening, as a movement, started in the northwest of Al Anbar 16 months prior to the sheikh's proclamation, with the Albu-Mahal tribe in Al Qaim District along the Syrian/Iraqi border. The Albu-Mahal realized that they could not fight Al Qaida in Iraq (AQI) on their own and pleaded for help from the coalition and the government of Iraq in what would become a fight for survival. The foundation for developing that partnership was a little known program called the "Desert Protectors." The development of the Desert Protectors and the Awakening movement in 2005 has tremendous lessons for today as a newly formed coalition organizes to fight the Islamic State of Iraq and the Levant (ISIL), an outgrowth of AQI.

IMAGE CREDITS

Page 5: US Government work/public domain
Pages 6–7: by Russell Watkins/Department for International Development. Licensed under the Creative Commons Attribution 2.0 Generic license. https://commons.wikimedia.org/wiki/File:Tacloban_Typhoon_Haiyan_2013-11-14.jpg
Page 8: Courtesy of the author.
Pages 10–11: by Eoghan Rice—Trócaire/Caritas. This file is licensed under the Creative Commons Attribution 2.0 Generic license. https://commons.wikimedia.org/wiki/File:Tacloban_Typhoon_Haiyan_2013-11-14.jpg
Page 18: US Navy photo by Petty Officer 1st Class William John Kipp, Jr. US Government work, public domain.
Page 19: by Pete Souza, White House photographer. US Government work, public domain.
Page 20: Photographer unknown, US Government work, public domain. http://georgewbush-whitehouse.archives.gov/news/releases/2006/03/images/20060304-2_d-0293-1-515h.html
Page 21: CNN screen capture downloaded from http://www.washingtonian.com/blogs/capitalcomment/media/recent-seymour-hersh-interviews-ranked.php.
Pages 25–33: Maps courtesy of the author
Pages 34–35: by Adam Jones via Flickr. Licensed under CC BY-SA 2.0 via Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Ruins_of_Governor%27s_Bungalow_1,_Jaffna.jpg#/media/File:Ruins_of_Governor%27s_Bungalow_1,_Jaffna.jpg
Pages 39–40: Courtesy of the author
Pages 44–45: by Steve Lodefink, licensed under Creative Commons. http://www.finkbuilt.com/blog/fpv-quadcopter-shot-down-by-radar/
Page 46: by Fribbler, licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license. https://upload.wikimedia.org/wikipedia/commons/a/a2/Shankilltroubles.jpg
Page 50: Courtesy of the author.
Page 54: by Michael Kaczorowski via Flickr. https://www.flickr.com/photos/arselectronica/8584777128/in/photostream/
Page 64: “Hoaxed photo of the Loch Ness monster,” photographer unknown. Licensed under fair use via Wikipedia. https://en.wikipedia.org/wiki/File:Hoaxed_photo_of_the_Loch_Ness_monster.jpg#/media/File:Hoaxed_photo_of_the_Loch_Ness_monster.jpg
Page 70: US Army Photo by Staff Sgt. Teddy Wade/Released. US Government work, public domain.
Page 75: by Lewa'a Alnasr, licensed under Creative Commons Attribution-Share Alike 3.0 Unported license. https://commons.wikimedia.org/wiki/File:Hundreds_of_thousands_of_Bahrainis_taking_part_in_march_of_loyalty_to_martyrs.jpg
Page 84: Engraving by Charles Laplante, a French engraver and illustrator. Public domain via Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Alexander_and_Aristotle.jpg
Pages 86–90: Publicity photos via http://www.amc.com/shows/turn

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 www.GlobalECCO.org/journal/ and click on the "Submit to CTX" link.

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**

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 consent from anyone whose pictures, videos, or statements you include 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).
- Any kind of submission can be multimedia.

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: no PDFs, please.)

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

Ready to Submit?

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

Submit to
CTXSubmit@GlobalECCO.org

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

Terms of Copyright