Col. G. I. Wilson, USMCR, Sgt. John P. Sullivan, LA County Sheriff's Dept., & Lt. Col. Hal Kempfer, USMCR

Fourth-Generation Warfare

It's Here, And We Need New Intelligence-Gathering Techniques For Dealing With It

Our world and the nature of conflict are changing. The ways we wage war and protect the public are also rapidly changing. The now-and-future conflict is transnational and global; it includes the American homeland and cyberspace and attacks on civilians.

This "fourth-generation warfare" is manifesting itself in highly compartmentalized, cellular, predatory adversaries operating in networks outside the framework of traditional nation-states.

Urban operations, crime, and terrorism are now part of the same operational environment. We are witnessing them emerging and mutating into new forms of warfare, blurring distinctions between crime and war. Fourth-generation warfare (4GW) moves beyond terrorism, suggesting that terrorism will take advantage of that type of warfare's three main characteristics: the loss of the nation-state's monopoly on war; a return to a world of cultures and nation-states in conflict; and internal segmentation or division along ethnic, religious, and special-interest lines within our own society.

On 11 September 2001, an unthinkable fourth-generation idea moved from the realm of the potential into the realm of reality. In a surprisingly graphic, coordinated, nearly simultaneous attack on the World Trade Center in New York and the Pentagon in Washington, DC, the scourge of global networked terrorism brutally assaulted the American homeland.

These attacks mirrored the rage of criminals who use violence with perceived impunity to secure political and social ends. Distinctions between military and civilian were suspended as a result of the nature of targets chosen by al Qaeda. We now face a fourth-generation opponent without a nation-state base.

On 11 September 2001, an unthinkable fourth-generation idea moved from the realm of the potential into the realm of reality. In a surprisingly graphic, coordinated, near-simultaneous attack on the World Trade Center in New York and the Pentagon in Washington, DC, the scourge of global networked terrorism brutally assaulted the American homeland. These attacks mirrored the rage of criminals who use violence with perceived impunity to secure political and social ends. Distinctions between military and civilian were suspended as a result of the nature of targets chosen by al Qaeda. We now face a fourth-generation opponent without a nation-state base.

Our new adversaries are diverse and linked in unfamiliar ways. Loose coalitions of criminal actors, guerrillas, and insurgents who operate outside the nation-state now challenge national security capabilities that were designed to operate within a nation-state framework. Beyond that framework, our traditional structures have great difficulties engaging such threats.

As Martin van Creveld noted in *The Transformation of War*, throughout most of man's time on earth war has been non-trinitarian. Families waged war, as did clans, tribes, cities, monastic orders, religions, and even commercial enterprises (e.g., the British East India Company). They fought for many reasons other than for the state—croplands, loot, women, slaves, victims to sacrifice to their gods, and even for

The world of today and tomorrow is one dominated by conflict and random violence between the "haves" and the "have nots." Those with a conflicting cultural or religious ideology are likely to challenge our superiority according to their rules, not ours. Their modus operandi blur and will continue to blur the distinctions between crime and war, criminal and civil, combatant and non-combatant. Their actions will seek to exploit the seams of the modern state's internal and external security structures. These emerging challengers will embrace unconventional means not amenable to conventional responses.

the purity of their race. Often there was no formal army with ranks and uniforms set apart from the people; every male strong enough to carry a weapon was a warrior.

CONTINUOUS CONFLICT

War and crime are increasingly intertwined, yielding ethnic enmity, refugees, displaced persons, and opportunities for criminal exploitation. These conflicts are exploited and fueled by crime bosses, gang leaders, tribal chieftains, and warlords supported by non-state soldiers (gangs, clans, and mercenaries). This adds to the complexity of threats, blurring the lines among peace, war, and crime.

These recurring bad actors—criminals, irregular rogue bands, warring clans, and gangs—operate largely at the low end of the technological spectrum, yet, as we are increasingly seeing, they are beginning to exploit technology. The access to technology and cyberspace by bellicose factions is facilitated by money from organized crime.Transnational criminal organizations (TCOs) are networked more than ever and control large sums of money. It is not hard to imagine these entities going beyond their current co-option of governments to actually capturing a state (and its war-making capabilities) to further their goals.

مُجاهدِ اِسلام
اُسامه بن لادن
نورِ خدا ہے کفر کی حرکت پہ خندہ زن
پھونکوں سے یہ چراغ بُجھایا نہ جائے گا

The world of today and tomorrow is one dominated by conflict and random violence between the "haves" and the "have nots." Those with a conflicting cultural or religious ideology are likely to challenge our superiority according to their rules, not ours. Their modus operandi blur and will continue to blur the distinctions between crime and war, criminal and civil, combatant and non-combatant. Their actions will seek to exploit the seams of the modern state's internal and external security structures. These emerging challengers will embrace unconventional means not amenable to conventional responses.

Advanced technologies, once largely the sole domain of highly developed nation-states, are now finding their way into other hands and rogue nations. Technical sophistication is no longer limited to members of nation-states. High-tech applications for waging war—from advanced software simulation and GPS data to high-resolution satellite imagery—are commercially available. Adaptive terrorist tactics are surfacing that are central to fourth-generation warfare.

Post-modern conflict may be so ambiguous and diffuse that the conventional operational environment may all but disappear as a means of describing this setting of conflict. The distinction between "civilian" and "military" continues to erode and may—in many senses—disappear. Actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical, entity. Success will depend heavily on effectiveness in joint and coalition operations in a number of simultaneous theaters of operations, both outside the United States and domestically within the US, as lines between responsibility and mission become increasingly ambiguous.

MULTIPLE OPERATING ENVIRONMENTS

Fourth-generation warfare will be found in a variety of settings, spanning the spectrum of conflict from routine criminal activity and high-intensity crime through low- and mid-intensity conflict. Activities will often converge wherever one finds adversaries operating outside the conventions of the nation-state. For example, peacekeeping and peace-support operations, humanitarian and consequence-management missions, counterterrorism, and counter-infowar missions may overlap, erupting in what former Marine Corps Commandant General Charles C. Krulak described in a prescient 1997 speech to the National Press Club as "Three-Block War."

Where the "three blocks" converge has been and will continue to be complicated by varying degrees of crime. Ethnic conflict is frequently exploited or exacerbated by organized crime and gangs to further their goals. Warlords and terrorists engage in drug trafficking to finance their campaigns. This complex mix places significant challenges and demands on individual military operators and civil police.

Blending civil protection, police, and combat skills demands a high degree of situational recognition and knowledge to understand which response is required and when it is required. Individuals or small units must become adept at this kind of decision-making, which presents large leadership challenges at all ranks. To support the complex range of activities required to navigate fourth-generation conflict, adequate intelligence, surveillance, and reconnaissance (including cultural intelligence and real-time active mapping and sensors) must be available to skilled operators who can adapt their tactics and the activities of small, independent-action forces to a variety of missions and circumstances.

INTELLIGENCE NEEDS

Intelligence is the foundation for determining the kind of war we might be entering and thwarting those who would undermine national and international security. Simply put: Intelligence needs to provide indications and warning (I&W), and human-

As the aftermath of the World Trade Center attack graphically demonstrates, urban settings are extremely complex. The urban battlescape or operational space possesses subterranean, surface, building, and rooftop features. Structures, subway tunnels, enclosed pedestrian bridges, trolley cars and trams with overhead power, roadways, alleys, sewers, tunnels, and parking garages allow multiple avenues of approach, firing positions, and obstacles. Under the best of conditions, lines of sight are diminished, inhibiting sensors and communications capabilities. After a large bombing or collapse of a high-rise building, terrain recognition is further complicated.

source intelligence (HUMINT) needs to discover and discern the plans and intentions of terrorists, gangsters, warlords, and rogue regimes.

Sound intelligence is crucial. It must give us the clearest possible insights into situations, events, players, and hidden agendas, so our leaders can decide quickly how or even if to engage. Intelligence must be able to warn of any potential surprises a warfighter is likely to face.

Lack of situational awareness has long been recognized as a major impediment to executing appropriate courses of action. This shortfall applies not only to fourth-generation warfare and terrorism, but also to crisis and complex-incident management (i.e., peace operations, urban operations, counterterrorism, complex humanitarian emergencies, consequence management, and disaster response). We need to anticipate and understand the dynamics of these issues, having not only knowledge dominance but also, more importantly, dominance in understanding the context of the action, event, or engagement.

Consider the benefits of understanding the context in urban operations. For example, the influence of three-dimensional terrain features and density are vital pieces of information for a commander faced with executing a rescue mission, constabulary operation, or providing humanitarian assistance in a third world mega-city inhabited by gangs, criminal enclaves, and sprawling slums. A world of constant change demands flexibility from intelligence networks after realistic expectations have been established for intelligence-gathering operations. For intelligence personnel, adapting and improvising must be a way of life.

URBAN OPERATIONS

Much of the potential battlespace of the future will be urban. US forces, as well as those of our allies, will conduct urban expeditionary operations against terrorists, paramilitaries, and gangsters linked to internationally networked organized crime. Some of these urban operations will be within the United States, supporting domestic law-enforcement and emergency-response agencies in coalition-type organizational settings.

As history has repeatedly demonstrated, urban operations are complex and brutal. Yet the current and future world landscape—not to mention our adversaries—will make urban operations unavoidable.

As the aftermath of the World Trade Center attack graphically demonstrates, urban settings are extremely complex. The urban battlescape or operational space possesses subterranean, surface, building, and rooftop features. Structures, subway tunnels, enclosed pedestrian bridges, trolley cars and trams with overhead power, roadways, alleys, sewers, tunnels, and parking garages allow multiple avenues of approach, firing positions, and obstacles. Under the best of conditions, lines of sight are diminished, inhibiting sensors and communications capabilities. After a large bombing or collapse of a high-rise building, terrain recognition is further complicated.

In *Heavy Matter: Urban Operations' Density of Challenges*, noted urban operations scholar Dr. Russell Glenn observed that complexity is a feature of all urban operations. Among the factors noted are: compressed decision times, increased operational tempo, and thousands, up to tens of thousands, of inhabitants per "cubic kilometer." These factors promise to degrade command and control, complicate decision-making, and challenge intelligence, surveillance, and reconnaissance efforts. Density, noise, and clutter make accurate, real-time situational awareness an elusive goal.

The military and urban civil protection and emergency services (police and fire service) stand to gain much by working together to better understand the urban environment. As the Russians recently relearned in Chechnya, urban operations are extremely demanding and taxing. The World Trade Center attacks demonstrated the complexity of the urban environment in a modern, western megalopolis. Our military, police, and fire service will have to operate together in this urban environment to protect the public and counter terrorist criminals as the Fourth Generation continues to unfold.

INTELLIGENCE FOR 4GW: "EVERYONE'S BUSINESS"

A new intelligence paradigm needs to be crafted that acknowledges realistic expectations for intelligence-related activities and specifies that intelligence is, in fact, everyone's business. Forging this capability will require a definition of the threat environment, collaboration among the military services and a variety of actors (including the intelligence community and non-traditional players such law-enforcement agencies), experimentation and, finally, implementation.

New tools and approaches are needed to sort pertinent information from noise. In addition, we must illuminate the mission-essential tasks of potential adversaries by exploiting both traditional and nontraditional tools and the information infrastructure through better use of open-source intelligence (OSINT), deception, and development of cyber-intelligence (CyberINT). HUMINT is an essential element

> ***While many new skills and interagency linkages are needed, efforts to build homeland defense will not require a cold start. On the operational and intelligence front, innovative structures, such as the Los Angeles Terrorism Early Warning (TEW) Group, have been bringing together emergency responders from law enforcement, the fire service, DoD entities, and the medical and public health communities to provide indications and warning and operational net assessments for several years.***

of this approach. Combining traditional tools, HUMINT, OSINT, and CyberINT can assist in identifying the precursors and indicators of violence (such as group mobilization, criminal exploitation, and proliferation of materials for weapons of mass destruction) that may trigger a military (or a combined military-civil) response. Adopting the concept of "Deep I&W," that is, extending sensing to capture emerging trends and potentials prior to recognition of an overt threat to minimize the foe's advantage, is essential. To do so, sensing, surveillance, and reconnaissance efforts will require a flexible, integrated analysis and synthesis component.

CIVIL PROTECTION

Meeting fourth-generation warfare threats to stability and security requires a direct and enduring commitment to forward-thinking military and civil readiness.

While many new skills and interagency linkages are needed, efforts to build homeland defense will not require a cold start. On the operational and intelligence front, innovative structures, such as the Los Angeles Terrorism Early Warning (TEW) Group, have been bringing together emergency responders from law enforcement, the fire service, DoD entities, and the medical and public health communities to provide indications and warning and operational net assessments for several years.

The TEW model is a hybrid form, combining the attributes of networked organization to the traditionally hierarchical emergency-response disciplines. By integrating military support to civil authorities into its on-going efforts, the TEW can speed the process of accepting follow-on military assistance and draw upon military planning skills (from local military entities such as the USMC at Camp Pendleton, California National Guard, 9th Civil Support Team) to enhance its process.

The TEW model involves collaboration among local, state, and federal law-enforcement and response agencies. It is designed to provide the operational intelligence needed to quickly develop potential courses of action, move through the decision cycle, forecast potential events, and craft meaningful courses of action for interagency, interdisciplinary response.

Collaboration and partnership, such as interagency, interdisciplinary partnerships with law-enforcement agencies to explore and experiment with novel intelligence applications and approaches for the emerging threat environment, should be explored. We need to focus sharply on what lies ahead, seeking ideas about emerging and future conflict. We need to further develop and integrate our open-source intelligence, HUMINT, and cultural intelligence capabilities. To meet the threat of "now and future" warfare, our intelligence must focus more on cultural and social paradigms, not just military orders of battle.

INTERSECTION OF CRIME AND WAR

Our adversaries span the globe. We face a shifting constellation of bad actors, competitors, sometimes-allies, non-combatants, and criminal opportunists. We will meet them in settings ranging from humanitarian stability and support operations to terrorist attacks, consequence management for complex emergencies, and ethno-religious cultural violence.

To be sure, our world and the nature of conflict are changing. The ways we wage war and protect the public are also rapidly changing. We are witnessing emerging and mutating forms of warfare, embodied by the blurring of crime and war, decline of the nation-state, increasingly lethal terrorism, and the manifestation of highly compartmentalized, cellular, predatory, networked adversaries.

We must learn from our experiences to adapt and develop new intelligence applications and approaches to these emerging and evolving fourth-generation threats at the intersection of crime and war. And we must do so quickly, because fourth-generation warfare is already here. ■