Complex Terrain

Jensen, Benjamin, Breitenbauch, Henrik, Valeriano, Brandon

Published by Marine Corps University Press

Jensen, Benjamin, et al.
Complex Terrain: Megacities and the Changing Character of Urban Operations.

For additional information about this book
https://muse.jhu.edu/book/85798

For content related to this chapter
https://muse.jhu.edu/related_content?type=book&id=3004067
or the dispersal of the population because of military operations will disrupt distribution pathways and networks and stress the capacity of civil services to provide sustenance for personnel. Therefore, symbiotic warfare operations require the military to act as an augmentation force to the local community with the military’s primary objective to ensure resource-allocation networks and distribution pathways remain open.

**The SWOC Is a Synthesis of Urban Warfare, COIN, and Irregular Warfare**

Symbiotic warfare encompasses urban warfare and military tactics associated with military operations on urbanized terrain doctrine and COIN doctrine.\(^{61}\) By definition, *Military Operations on Urbanized Terrain* and *Joint Urban Operations* outline the tactical and capability options available to a commander in an urban environment.\(^{62}\) Explicit in describing the street, subterranean, and air battlespace, urban doctrine takes into consideration that “the basic principles of combat in built-up areas have essentially remained unchanged in this century.”\(^{63}\)

Where the SWOC and urban operations doctrine agree are on the importance of maneuver warfare and combined arms philosophies in the urban environment.\(^{64}\) Where they disagree are on the factors that will have an impact on the manner in which military forces, including the Marine Corps, conduct urban warfare. For example, *Military Operations on Urbanized Terrain* uses historical examples of warfare to suggest the critical factors that contribute to effectiveness are intelligence, surprise, and combined arms. Combined arms, according to this doctrine, require essential categories of weapons in association with: 1) infantry, 2) armor, 3) artillery, 4) mortars, 5) antiaircraft artillery, and 6) aviation.\(^{65}\) While these types of weapons and capabilities were essential in 1998, technological advancements of the U.S. military

---


63 *Military Operations on Urbanized Terrain*, 1-8; and *Joint Urban Operations*.

64 *Military Operations on Urbanized Terrain*, 1-12; and *Joint Urban Operations*.

65 *Military Operations on Urbanized Terrain*, 1-13–15; and *Joint Urban Operations*. 
and our adversaries require the United States to update doctrine to account for operational concepts, tactics, and new types of tactical lethal and nonlethal weapons required to conduct operations.

Additionally, *Joint Urban Operations*'s discussion of the urban operating environment does not account for the interconnectedness between densely populated environments and access to resources. As the previous literature review illustrated, panic ensues when populations become segregated from resources they view as vital (e.g., food, water, power, fuel, cyber, money). If the future of conflict manifests out of a competition for resources, then the military must consider the intelligence preparation of the battlespace (IPB) by defining the populations’ critical resource requirements, mapping out the resource-allocation networks and distribution pathways that provide those critical resources, and assessing those networks and pathways for vulnerability. Securing and ensuring the integrity of resource networks and pathways becomes the military’s primary responsibility.

**Proposed Model for Mapping Predation Intervention Points**

Although the SWOC is geographically agnostic in the sense the military’s objective is to control resources within the terrain and minimize infrastructure damage to avoid disruptions in the daily operations of the community. IPB requires military and civilian planners to identify critical vulnerabilities that exist in resource-allocation and network distribution pathways as a preventive measure against predation. Using biological science and studies to map predator invasion process, a proposed model to identify military intervention points may prove useful. Table 1 illustrates how physical and biological sciences adapt to complement the SWOC to provide military and civilian planners a proactive method of analyzing the symbiotic and delicate balance between a community’s population and resources.

While each predator and community is unique, the qualities of neither the predator nor the population actually serve as the center of gravity in symbiotic warfare. Predators exploit resources and the vulnerabilities that exist in resource allocation and distribution networks and pathways. Neutralizing the threat requires cohesive ef-
forts between the civilian community, metropolitan police forces, and the military. In the SWOC, the military only takes direct action when metropolitan police forces require augmentation or when defending resource-allocation networks and distribution pathways. Thus, the identification of intervention points proves useful for military planners who seek to commit military assets and capabilities to assist in predation neutralization.

**Differences between Symbiotic Warfare and Insurgency**

*Counterinsurgency* defines an insurgency as “the organized use of subversion and violence to seize, nullify, or challenge political control of a region.”\(^{66}\) The SWOC adopts a similar definition for its use of the term *predator*, delineating insurgents from predators primarily by their objective. For example, in an insurgency, the insurgent uses “a mixture of subversion, sabotage, political, economic, psychological actions, and armed conflict to achieve its political aims.”\(^{67}\) Predators, which also use a mixture of subversion, sabotage, political, economic, psychological, and armed conflict, seek to control or exploit resources. The predator’s objective is not political by nature. Furthermore, the hearts and minds of the population is not an objective for predators or for a military, which is charged with assisting a community in neutralizing a predation threat. Predators use the population as maneuver space to gain access to resources. Military planners must determine where populations are most vulnerable to help the community determine where predators may temporary nest.

The SWOC also adopts several concepts from COIN doctrine. For example, similar to COIN, symbiotic warfare is a comprehensive civilian and military effort designed to neutralize predators and address the root causes of resource instability that led to predation.\(^{68}\) Similarly, symbiotic warfare is population centric. The development of proper symbiotic warfare tactics starts with the acceptance of the

---

\(^{66}\) *Counterinsurgency*, I-1.

\(^{67}\) *Counterinsurgency*, I-1.

\(^{68}\) By definition, “COIN is a comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and addresses its root causes.” *Counterinsurgency*, I-1.
Table 1. Mapping predation intervention points

<table>
<thead>
<tr>
<th>Invasion process</th>
<th>Mitigation strategy</th>
<th>Resources</th>
<th>Native population</th>
<th>Predator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Species in vector/pathway</td>
<td>Prevention and interception</td>
<td>Identify allocation networks and distribution pathways</td>
<td>Identify vulnerable population</td>
<td>Identify resource requirement</td>
</tr>
<tr>
<td>Insertion</td>
<td>Early detection</td>
<td>Monitor allocation networks and distribution pathways</td>
<td>Monitor vulnerable population</td>
<td>Identify resource exploitation networks</td>
</tr>
<tr>
<td>Population established*</td>
<td>Rapid response</td>
<td>Secure allocation networks and distribution pathways</td>
<td>Monitor for sign of predation; segregate population from broken networks and pathways</td>
<td>Eradicate predator’s resources</td>
</tr>
<tr>
<td>Spread/ dispersal*</td>
<td>Containment and neutralization</td>
<td>Monitor allocation networks and distribution pathways</td>
<td>Monitor for signs of predation; segregate population from broken networks and pathways</td>
<td>Segregate</td>
</tr>
<tr>
<td>Ecosystem infrastructure and competing population damage*</td>
<td>Restabilization and restoration</td>
<td>Repair damage to infrastructure; strengthen vulnerability</td>
<td>Reintegration</td>
<td>Eliminate</td>
</tr>
</tbody>
</table>

* Dependent on the ecosystem community’s adaptive capacity and the robustness of its resources.


population’s role in identifying and neutralizing the threat. A metropolitan police force may prove fully capable of securing the population; thus, the military will assume only an enabling and complementary role with capabilities such as intelligence, surveillance, and reconnaissance (ISR) and counter electromagnetic warfare.
CHAPTER TEN

Critical Factors in Urban Operations

The factors the SWOC determines critical to urban operations are intelligence, combined arms, and civil military operations. Combined arms break down essential categories of weapons to: 1) offensive and defensive air, sea, and cyber forces; 2) security forces (infantry and SOF); 3) electromagnetic weapons; and 4) nonlethal fires. The SWOC uses the existing infrastructure and resources within the megacity to target and neutralize the threat to the greatest extent possible. Military operations in the support of the SWOC are to fill infrastructure capability and capacity gaps and strengthen the vulnerabilities of networks and pathways that provide resource allocation and distribution.

Offensive and defensive air, sea, and cyber forces require the U.S. military to reassess its current platforms for viability in a megacity environment. For air and cyber assets, the Services could consider using ISR micro air vehicles (MAVs) to swarm and scatter the megacity. Low cost ISR MAVs, using a Lockheed C-130 Hercules as a delivery mechanism, can deploy in an uncontested air space and transfer via flutter, hover, or loiter in a contested air space for up to 10 days.69 Their less than 1.5-inch profile and light weight allows a C-130 to deploy up to 10,000 MAVs during one air delivery. The uses of ISR MAVs prove critical to monitoring resource-allocation networks and distribution pathways.

Furthermore, the military could also use MAVs to set up virtual command and control (C2) nodes. MAVs equipped with dual transmit capability, similar to ISR MAVs, can also carry a unique IP address. Deploying 10,000 components during one launch not only allows for network and transmit capability for military forces but also reestablishes connectivity after a cyber or electromagnetic attack. To assist in neutralizing predation threats, the military and civilian law enforcement can use network mirror imaging to set up a network noose to track predator movements and transmissions. This also opens the virtual C2 environment to facilitate robust information operations campaigns.

to include those launched by intelligence planners who seek to em-
ploy deception tactics.

Fires, while important, play a minor role with IPB planning, MAV
ISR, and virtual C2 nodes. While small diameter bombs may prove pre-
cise, it is important to remember that the concept of symbiotic warfare
is to minimize disruption to infrastructure within a megacity, especial-
ly to resource-allocation networks and distribution pathways that the
predators themselves will seek to exploit.

**Capability Assessment**

Today’s Joint Force cannot meet the challenges of megacity warfare. While *Military Operations on Urbanized Terrain* and *Joint Urban Op-
erations* are starting points for doctrine reassessment, capabilities
require a technology refresh if the Joint Force wants to remain imper-
vious and invulnerable while defending, securing, and protecting a
megacity’s resource-allocation networks and distribution pathways. The purpose of the capability assessment is not to seduce the Joint
Force with technology but to counter twenty-first century technologi-
cal threats that leave megacity resources and communities vulnerable
to predation.

Regarding potential threats that leave resource-allocation net-
works and distribution pathways vulnerable, the SWOC recommends
developing the following capabilities and tactics. Rethinking how the
Joint Force uses its current capabilities and tactics could not come at
a more relevant time. The lag time in acquisition and proper research,
testing, development, and evaluation places 2019 as the right time to
consider 2025’s future needs. The following is a list of current capabil-
ity, platform, and concept shortfalls:

- **Capabilities**
  - Terrain and subterranean loiter, hover, and flutter ISR
  - Terrain and subterranean counterelectromagnetic warfare
- **Platforms**
  - ISR and network-capable MAVs and drones that provide loiter
capabilities and those that can flutter, scatter, and swarm to
counter an electromagnetic threat, reopen networked lines of
  communication, provide network noose capabilities to mon-
itor predator activity, and exploit information exchanges for intelligence gathering

- Concepts
  - Virtual “Cloud” C2 to 1) minimize military footprint on a community’s resources and 2) remain elusive to predators
  - Scatter, swarm, and disperse tactics to counter an electromagnetic attack and track a predator’s capability to use the population as maneuver space.\(^70\)

**Conclusion**

Densely populated and congested environments rely on robust resource-allocation networks and distribution pathways that future agglomerated populations (predators) will attempt to disrupt to exploit resources. The military’s future role in megacity warfare is to provide an undisrupted flow of resources to the population to neutralize predation threats. Symbiotic warfare is nothing more than a hybrid of urban warfare, insurgency, and irregular warfare. Based on scientific research and adaptive modeling of how densely populated species behave when predators attempt to exploit resources, symbiotic warfare provides the intelligence community a map of the predation invasion process, affording the military intelligence community the ability to identify points of intervention useful in neutralizing predation threats.

Furthermore, symbiotic warfare, and the follow-on symbiotic warfare operating concept, focuses on the interdependencies that exist between resources, population, and the predators that seek to disrupt the integrity of resource-allocation networks and distribution pathways. Doctrine analysis reveals obvious oversights in these considerations and still relies on fires as a primary means of threat neutralization. If megacity warfare becomes a reality, then the military needs to prepare for it. Current platforms and capabilities, which they deliver, fall short in meeting heavy ISR demands and networking capabilities. Furthermore, the ability of platforms to maneuver freely within

\(^70\) For detailed explanation of “swarm” and “scatter” as tactics to counterelectromagnetic threats, see Blair and Helms, “The Swarm, the Cloud, and the Importance of Getting There First,” 14–38.
the megacity do not currently exist. If nothing more, this research provides the military with a sobering reality that future warfare may not require direct action and fires as much as it will require the military to deliver and secure essential services for a population.
CHAPTER ELEVEN

Air Domain Dominance in a Megacity

Major Nathan J. Storm, U.S. Marine Corps

The Japanese landings came on 8 December 1941 in northern Malaya and southern Thailand. By the morning of 10 December, they had penetrated well into the Malayan frontier and advanced to Kedah, Malaysia. Japanese aircraft dealt swiftly with any resistance and eased their progress down the peninsula to threaten Singapore. The Japanese had advanced nearly 1,000 kilometers to capture Malaya in only 54 days. On the night of 8 February, two divisions of the Japanese invasion force crossed the straits and landed on Singapore Island. At the end of the day, more than 30,000 Japanese troops occupied Singapore, establishing a stronghold on the northwestern part of the island. The Japanese advance continued until Allied forces had been driven back to the suburbs of Singapore city. Food and water supplies were low, and that evening British lieutenant general Arthur E. Percival surrendered to the Japanese.

MARINE CORPS AVIATION DOCTRINE AND CAPABILITIES IN A MEGACITY

The future of urban warfare is bleak. The possibility, or probability, of conducting any of the range of military operations inside a dense urban environment is incredibly high. A national security professor at the U.S. Naval War College, Richard J. Norton, certainly expects it, stating that “if three quarters of the world will live in cities, and we still fight
wars, then wars are going to be fought in this environment.”¹ With that concept in mind, the Marine Corps must research, develop, and practice new concepts for the conduct of war in a dense urban environment. Current Marine Corps air doctrine and maneuver capabilities are poorly suited for operations within this dense urban environment.

For purposes of this project, we will discuss the dense urban environment as a megacity. To understand how to fight in a megacity, we must have a broad definition from which to work. We also must justify our reason for studying war in a megacity environment and determine if current doctrine and tactics suitably account for the vast human network the military will encounter while operating there.

The generally accepted size of a megacity is an urban area with a population greater than 10 million people. The United Nations 2018 Revision of World Urbanization Prospects (WUP) reports 37 current megacities and predicts 43 by 2030.² The WUP continues:

Today, 55% of the world’s population lives in urban areas, a proportion that is expected to increase to 68% by 2050. Projections show that urbanization, the gradual shift in residence of the human population from rural to urban areas, combined with the overall growth of the world’s population could add another 2.5 billion people to urban areas by 2050, with close to 90% of this increase taking place in Asia and Africa.³

The World Health Organization (WHO) further explains the annual increase in urban population: “The global urban population is expected to grow approximately 1.84% per year between 2015 and 2020, 1.63% per year between 2020 and 2025, and 1.44% per year between 2025 and 2030.”⁴ Expanding urban populations place more humans at closer proximity to each other than ever before. Close physical prox-

¹ Flavia Krause-Jackson and Nicole Gaouette, “Homemade Tank Powered by Game Boy Fights Wars of Future,” Bloomberg, 9 September 2014.
³ 2018 Revision of World Urbanization Prospects.
iminity coupled with increased electronic connectivity yields drastically increased global interconnectedness. During the course of this study, the size of a megacity became irrelevant to our purposes. The key feature became instead population density over absolute size. Gaza is more densely populated than Los Angeles, even with a total population of about 1.8 million people. If our major concern is the interconnectedness of major urban centers, we need not worry about an arbitrarily defined population requirement but that there exists ample opportunity for connections to form within the population.

Mavens and connectors or programmers and switches—no matter what you call them—the people who establish, recruit, train, and run human networks are a major threat. The pool from which recruits are drawn continues to increase as the local, interconnected population size grows. In a networked megacity, the ability to control or regulate those human networks is key. In *The Tipping Point*, Malcolm Gladwell discusses two types of human network facilitators he calls “mavens” and “connectors.” Mavens collect information; they have knowledge and want to distribute that knowledge to as wide an audience as possible. To distribute knowledge, mavens enlist help from connectors. According to Gladwell, connectors are important not only for the number of people with whom they are connected but also for the quality of those connections.⁵ Noted sociologist Manuel Castells discusses a similar concept in his 2011 article, “A Network Theory of Power.” Castells’s concepts of “programmers” and “switches” hold similar meaning to Gladwell’s mavens and connectors. Castells defines *programmers* as a person or group with “the ability to constitute network(s) and to program/reprogram the network(s) in terms of the goals assigned to the network,” and connectors have “the ability to connect and ensure the cooperation of different networks by shaping common goals and combining resources while fending off competition from other networks by setting up strategic cooperation.”⁶ Mavens and programmers control the knowledge base. They trans-

---

fer their knowledge to a close group of followers but need another means to translate that knowledge to a wider audience. Connectors and switches are that means; during a future war in a megacity, the people or groups who facilitate these roles are a key to success in defeating any adversarial group.

Physical and electronic interconnectedness, increasing population density and size, and the power to form, program, and spread networks creates a distinct problem for the Marine Corps with regard to war in a megacity. From an aviation point of view, how does the Marine Corps respond to military operations within a megacity, assuming that control and regulation of physical and electronic network connections are key?

One current military doctrinal publication “recommends isolating and bypassing urban terrain when possible due to the costs involved.”

Obviously when discussing the future of war in a megacity, bypass and isolation is neither possible nor the best means by which to prosecute the war. To effectively fight in a megacity, the U.S. Marine Corps must be capable of controlling individual networks. Current Marine Corps aviation doctrine seems ill-equipped to function against the interconnected complexities of war in a megacity.

The Marine Corps maintains six aviation functions: electronic warfare (EW), air reconnaissance, offensive air support (OAS), assault support, command of aircraft and missiles, and antiair warfare (AAW). Initial problem framing assessment within the megacity describes problems of aviation maneuver. Problem framing also leads to a cursory list of questions the Marine Corps must parse through. How does the Corps adapt these six functions to operate within a dense urban environment? Similar to ground urban operations, aviation urban operations are fraught with myriad challenges. How does Marine Aviation maneuver safely and effectively within this type of environment? Will the megacity’s concentration of electromagnetic radiation affect the capability and effectiveness of EW? How will urban canalization affect the assault support aircraft’s mission of airborne movement of equip-

7 MTTP for Aviation Urban Operations, MCRP 3-35.3A (Quantico, VA: Marine Corps Combat Development Command, 2001), I-1.
ment and personnel? Will the vertical nature of most megacities interfere with OAS and air reconnaissance’s ability to locate, target, and prosecute the enemy without high collateral damage risk? Without adaptation of procedures and capabilities, limited line of sight affects positive command and control of aircraft within a megacity. How will the megacity affect the Marine Corps’ ability to conduct AAW? The asymmetric nature of urban combat affects every aspect of Marine Aviation.

MTTP for Aviation Urban Operations speaks in very broad terms about considerations for military aviation operations in an urban environment, but notably does not discuss the interconnected nature of urban warfare. Joint Urban Operations more appropriately discusses the interconnectedness of a megacity “as a complex and dynamic system, with unique political, military, economic, social, information, and infrastructure (PMESII) and other components. Each element impacts, constrains, and influences military operations.” 9 Joint Urban Operations continues to discuss “complex social and political interactions by compressing large numbers of people into a small geographic area. Critical infrastructures (physical, economic, governmental, social, etc.) are in such close proximity and, in most areas, so intertwined that even minor disruptions by military operations can cause significant repercussions.” 10 It also covers aviation operations, stating that “air operations must adapt to the unique urban environment . . . although [command and control] C2 does not change in the urban environment, tactics, techniques, and procedures (TTP) may be vastly different from those employed on the open battlefield.” 11 The Marine Corps must cooperate with the joint community to research and deploy new techniques and technology suitable to a megacity.

One key to success in megacity warfare is creating and adapting TTPs to the megacity environment. The Marine Corps also must develop new means of conducting urban aviation operations to include airborne, nontraditional intelligence, surveillance, and reconnaiss-

sance (NTISR); and assault support and offensive air support (OAS). With regard to NTISR and OAS, the traditional top-down approach will likely not be as effective in an urban environment because of the vertical characteristics of a modern megacity. Assault support TTPs also may need to be adjusted, especially in light of the probability of aircraft operating below the building horizon and limitations on current aircraft survivability equipment (ASE).

Additional aviation considerations include impacts to aircraft systems, such as forward-looking infrared (FLIR) radar and night vision devices (NVD). For example, thermal reflectivity precludes FLIR systems from being able to see through glass. Glass has high thermal reflectivity and will reflect the thermal energy of the background.\(^\text{12}\) The *Marine Aviation Weapons and Tactics Squadron 1 (MAWTS-1) Night Vision Device (NVD) Manual* continues: “Certain smooth, glossy surfaces, such as . . . windshields and glossy painted fenders can reflect [infrared] IR radiation images incident on them from other sources.”\(^\text{13}\) Glass-fronted buildings dominate the modern cityscape, thereby making them opaque to modern aviation thermal imaging devices.

The nighttime urban environment has similarly negative effects on NVDs. Current advances in the Marine Corps night vision goggle device, the AN/AVS-9 with OMNI-VI image intensifier tubes, have reduced halo effect around non-NVD compatible lights (typical white, yellow, red city lights are non-NVD compatible).\(^\text{14}\) Improved image intensifier tubes cannot account for the increased visual clutter and reflected light that negatively affect the devices. Decreased visual acuity increases the risk associated with flying in the urban environment and creates significant difficulty with locating, tracking, and operating against individuals who control urban networks.

To effectively operate in the megacity environment, the Marine Corps must research, study, and experiment with new and existing


\(^{13}\) *MAWTS-1 NVD Manual*, 28.

\(^{14}\) LCdr Heath Clifford, USN, “NVD Technology Update” (presentation, MAWTS-1, Yuma, AZ, 10 November 2014).
concepts to develop appropriate TTPs and equipment. Current capabilities are more well suited to warfare in the open environments in Iraq and Afghanistan. Current satellites and unmanned aircraft systems are poorly equipped to gather intelligence in the narrow streets of a megacity. To facilitate future success, the Marine Corps must recognize these limitations and develop new methods of locating, tracking, and controlling megacity network programmers and switches.

Before developing a concept for the future of Marine Corps Aviation in a megacity, this chapter will discuss how to develop a more thorough understanding of the problems related to war in megacities. The following case study of the Japanese invasion of the Malay Peninsula and Singapore during WWII develops one perspective of apparent issues of megacity war.

**CASE STUDY: JAPANESE INVASION OF SINGAPORE DURING WWII**

Japan’s first offensive in the Pacific war against the West actually was not the attack on Pearl Harbor. About 20 hours before the Japanese attack on Oahu, Hawaii, five Imperial Japanese Army fighters took off from Thailand to support a convoy in the Gulf of Siam. During their flight, the fighters happened upon a British Royal Air Force (RAF) Consolidated PBY Catalina patrol flying boat. The amphibious aircraft, based out of Singapore, was searching for the convoy those Japanese fighters were meant to support. The Japanese fighters vastly outmatched the sluggish boat-plane and destroyed the Catalina before it could radio back to its headquarters in Singapore.\(^\text{15}\) And so began the war in the Pacific, Japan’s conquest of the Malay Peninsula, and their eventual seizure of Singapore.

Initially, one might look to a 76-year-old battle in the Pacific and think it of little significance to a discussion of twenty-first-century warfare or, more specifically, to war in a megacity. The Marine Corps Doctrinal Publication (MCDP) *Warfighting* extols the “two concepts of universal significance in generating combat power: speed and fo-

---

It is this speed and focus that led the Japanese to dominance during their multimodal and multidomain assault on the Malay Peninsula and Singapore. Japan’s air and sea power dominated in the face of a numerically superior British occupation and established defense. Through the next few pages, we will briefly frame a discussion of the battle and the operational planning for both the Japanese and British. Finally, we will discuss overall findings from the case study and how we can relate this operation to war in a megacity and the concepts to come.

The method of research for this case study was through internet searches, online research databases, written histories, and theoretical works. The intent of this work is to develop a link between the military necessity of gaining and maintaining rapid domain dominance within an urban environment, such as Singapore in 1941, and the capacity to gain the same dominance in a modern megacity environment. To this end, the research for this chapter was primarily concerned with the historical narrative regarding Japan’s domination of the Malay Peninsula, followed by the seizure of the island and city of Singapore. The modern commander may find the best way to gain control of a megacity is through the valuable lesson of the rapid multimodal dominance the Japanese achieved in Singapore.

**HISTORICAL BACKGROUND**

To continue their offensive in China, the Japanese needed access to natural resources they could not otherwise procure in the open markets. The economic sanctions placed on Japan worked to strangle the nascent Japanese empire. Forced to look for war materials elsewhere, Japan looked to the south for relief to “seize for herself the mineral-rich resources of South-east Asia.” At approximately 0215 on 8 December 1941, a little more than an hour before the attack on Pearl

---

16 *Warfighting*, 40.
Harbor, the initial Japanese invasion force in Malaysia landed. During the next few hours, the Japanese brought three divisions ashore in Thailand while holding another division in reserve. Using what one must assume to be deceptive tactics, the Japanese leadership in Thailand “completed [formalities] allowing us to pass through Thailand.”

The British forces in Singapore and throughout the Malay Peninsula had accurate intelligence regarding the impending Japanese assault. However, the general understanding and analysis of that intelligence was that the Japanese Army was attacking Thailand and not the British in Singapore. The British also recognized the difficulty of defending against a Japanese assault into neutral Thailand’s sovereign borders. British forces crossing Thailand’s border to defend Malaysia and Singapore against the Japanese offense would likely paint the British as the aggressor.

In the introduction to Arthur Swinson’s book *Defeat in Malaya: The Fall of Singapore*, Sir Basil Liddell Hart describes the defending British force as having “more than sufficient strength in the island to repel the invasion, particularly as it came in the sector where it was most expected.” Under Lieutenant General Arthur Percival, Malaya Command, the British command in Singapore totaled approximately 88,600 troops. Troop breakdown in Malaya Command included 37,000 Indian troops, 19,600 British, 15,200 Australians, and 16,800 Malayan and Chinese troops. The Indians were broken down into two divisional commands and the Australians had one. The British troops had no division command but were broken into six battalion commands. Percival commanded a weak air force of 158 operational aircraft made up primarily of obsolete models operated by underprepared pilots who

---

22 Swinson, *Defeat in Malaya*, 51.
24 Swinson, *Defeat in Malaya*, 7.
had not seen combat. Finally, the Royal Navy in Singapore included aircraft carrier HMS *Hermes* (95), battlecruiser HMS *Repulse* (1916), battleship HMS *Prince of Wales* (53), and a few smaller ships.  

The approximate total Japanese force brought to bear against the Malay Peninsula and Singapore was roughly matched with the British forces in the area. Japanese forces included approximately 50,000 infantry, 80 medium and 100 light tanks, a strong artillery presence, and various support elements (engineers to support bridging operations) totaling an additional 30,000 troops. The Japanese force came in with more than 450 aircraft and a strong naval presence of cruisers, destroyers, and submarines.

**ANALYSIS**

So how did a numerically inferior force (~80,000 Japanese to ~88,600 Allied) push one of the world’s great powers south along the length of the Malay Peninsula and eventually rout them in Singapore? Herein lies the heart of what this chapter looks to discover. The superior Japanese planning, strategy, and execution kept the British forces continuously off balance and in an almost constant state of withdrawal.

Similar to the numbered war plans the United States maintains, Japan built a specific war plan against the strategically important island of Singapore. To use the parlance of our times, the operational planning team (OPT) leader was Lieutenant Colonel Masanobu Tsuji. Though not specifically trained in amphibious operations or jungle warfare, the Japanese embarked on a crash course. The Japanese planners sought information regarding the tropics from any source they could imagine, including “pestering sea captains, mining engineers, bankers, university professors, diplomats, Buddhist priests—in short, anyone and everyone in Japan and Formosa who knew anything at all about the tropics.” For the Japanese troops to prepare for the assault through Malaysia, they conducted regional exercises through-

---

out the spring of 1941, allowing the army and navy to build interoper-
ability and amphibious experience.\textsuperscript{29} Tsuji and his planners personally 
conducted ground and aerial reconnaissance of the Malay Peninsula 
and potential landing beaches.\textsuperscript{30} With detailed planning, reconna-
sance, and multiple rehearsals, the OPT ensured every opportunity 
for Japanese success in Singapore. Japanese leadership recognized 
the strategic importance of Singapore and the necessity for Japanese 
control over Singapore while conducting the Pacific campaign. With 
this recognition came long-term and deliberate planning that ultimate-
ly led to their success.

Political forces at home in London hampered British defenses in 
Singapore with poor local tactical decisions. In his book \textit{Operation Mat-
ador}, Ong Chit Chung argues that much of the fault for Singapore’s fall 
to the Japanese lay with Winston Churchill. Churchill’s attention was 
with the more immediate war on the European continent than with the 
much farther afield defense of Singapore. The thinking in London was 
that Japan might invade Thailand, but certainly would not risk war with 
the Western powers.\textsuperscript{31} Furthermore, Churchill generally believed that 
Japan was not on the verge of war with the West—given their preoccu-
pation in China—and that the best defense of Singapore was through 
“strong local garrison and the general potentialities of sea-power. The 
idea of trying to defend the Malay Peninsula and of holding the whole 
of Malaya . . . cannot be entertained.”\textsuperscript{32} Churchill’s views delayed ar-
rival of the capital ships \textit{Repulse} and \textit{Prince of Wales} (ill-fated as their 
arrival may have been). Theorists often quote Clausewitz’s definition 
“that war is not merely an act of policy but a true political instrument,

\textsuperscript{29} Henry Frei, \textit{Guns of February: Ordinary Japanese Soldier’s Views of the Malayan Cam-
\textsuperscript{30} Falk, \textit{Seventy Days to Singapore}, 26–27. 
\textsuperscript{31} Operation Matador was the plan by the British Malaya Command to move forces into 
place to counter a Japanese assault. Ong Chit Chung, \textit{Operation Matador: Britain’s War 
Plans against the Japanese, 1918–1941} (Singapore: Times Academic Press, 1997), 
222–23. 
\textsuperscript{32} Winston S. Churchill, \textit{Their Finest Hour}, vol. II, \textit{The Second World War} (Boston: Hough-
ton Mifflin, 1949), 667–68.
a continuation of political intercourse, carried on with other means.”\textsuperscript{33} However, in this case, the converse is true. The politicians in Britain, far from pursuing war in Singapore, found a war in Southeast Asia at least partially because of their political inaction. British unwillingness to initiate Operation Matador, because they feared being seen as the aggressor in Thailand, did not help the defense of Singapore.\textsuperscript{34} Nor did the quick demise of the \textit{Repulse} and \textit{Prince of Wales} or the modest (at best) northern defense in Singapore assist in the ultimate success of the British.

The Japanese fought south quickly. Upon the initial assault, their priority was air supremacy. Japanese air forces destroyed British aviation units and, upon seizure of British-held airfields, extended the range of Japanese aircraft farther south. Once satisfied they had attained air supremacy, the Japanese would speed their southward advance toward Singapore.\textsuperscript{35} Speed was of the utmost importance to the Japanese. Brian P. Farrell, head of the history department at the National University of Singapore, writes that “the British expected the Japanese to consolidate a beachhead, build up their strength, advance only when their main force was concentrated, then advance methodically.”\textsuperscript{36} Farrell points to the success of their strategy:

\begin{quote}
Within 100 hours they shattered all British defensive plans, seized the initiative, and advanced boldly into northern Malaya. Force Z sortied, but was caught at sea by Japanese land-based naval air forces and destroyed on the morning of 10 December. This, plus the Japanese success at Pearl Harbor, gave the [Imperial Japanese Navy] IJN command of the sea. That allowed it to threaten the whole east coast. This forced Malaya Command to keep much of its strength in southern Malaya and on Singapore Island. [Royal Air Force] RAF Far East gave battle, but was outmatched in every respect. Losing nearly half its strength in three days, the
\end{quote}

\textsuperscript{34} Chung, \textit{Operation Matador}, 232–33.  
\textsuperscript{35} Falk, \textit{Seventy Days to Singapore}, 31.  
\textsuperscript{36} Farrell, “High Command, Irregular Forces, and Defending Malaya,” 47.
 CHAPTER ELEVEN

air force drew back to regroup and try to protect reinforce-
ment convoys approaching Singapore; this left the army
vulnerable.37

Contrary to British expectations, the majority of Japanese land
forces flowed like water to the western coast of the Malay Peninsula
then south to arrive at the Johor Strait by the first week of February
1942. Sun Tzu describes the necessity of speed as “the essence of
war. Take advantage of the enemy’s unpreparedness; travel by unex-
pected routes and strike him where he has taken no precautions.”38
Japanese forces succeeded in that paradigm. As mentioned above,
the Japanese land-based naval air forces destroyed the British “Force
Z” (the capital ships Repulse and Prince of Wales), leaving the pen-
insula unguarded at sea. Japanese air forces also destroyed virtual-
ly all of the British aviation capability on the Malay Peninsula and in
Singapore. The rapidity of the attack by the Japanese kept the British
defense off balance and negated the numerical superiority the British
enjoyed.

The battle raged the length of the peninsula and, by the end of
January, the British forces had retreated back across the causeway
onto Singapore Island. On the morning of 31 January 1942 at approxi-
mately 0815, the British forces destroyed the causeway and prepared
for a final defensive stand in Singapore.39 On 8 February 1942, the Jap-
anese arrived at the Johor Strait, began an amphibious assault on Sin-
gapore, and by the morning of 9 February had two divisions of infantry
and portions of their heavy machinery across the strait. The Japanese
continued to push the British forces back toward Singapore and, by
12 February, the Japanese controlled the reservoirs that fed water to
the city. The British forces surrendered in the early afternoon of 15
February 1942.40

38 Sun Tzu, The Art of War, trans. Samuel B. Griffith (New York: Oxford University Press,
1971), 134.
40 Allen, Singapore, 169–74.
INFERENCES

The question now is how to correlate these lessons learned from Japan’s successful assault of the Malay Peninsula and Singapore to the future of warfare in a megacity. We will condense the above pages to a few findings that provide a glance at a theory of victory. First, we want to look at the importance of intelligence gathering, analysis, and planning processes, then discuss the influence of speed, surprise, maneuver, and multidomain dominance as these subjects relate to military operations in a megacity.

Military theorist Sun Tzu describes the need to conduct planning so that one may “know the enemy and know yourself; in a hundred battles you will never be in peril.”\(^4\) The Japanese forces were well prepared for the operation to capture Singapore. They gathered intelligence, built their plan based solidly on intelligence estimates, and rehearsed their concept. To be victorious in a future megacity war, the United States military must be equally prepared. Preparation must entail detailed studies of how conflict in a megacity would present. War in an urban environment is exceedingly complex, even more so because each megacity has a unique character, culture, and environment. A one-size-fits-all approach cannot work (at least not efficiently). To be successful, the U.S. military must fully understand the requirements and the environment to develop tactics, techniques, and procedures (TTPs) by which to gather operable intelligence in the networked environment of a megacity and subsequently attack targets that support those networks.

Clausewitz describes the value of speed and surprise in his treatise *On War* as “the means to gain superiority.”\(^4\) The Japanese did not have numerical superiority so they maximized their use of speed and surprise. Conversely, the British forces on the Malay Peninsula had neither surprise nor initiative. Though Operation Matador could have influenced the outcome of the 70 days between the invasion and the surrounding of Singapore, the authorization to initiate Matador did

\(^4\) Sun Tzu, *The Art of War*, 84.  
\(^4\) Clausewitz, *On War*, 198.
not arrive until 5 December 1941. The Japanese rapid ingress across
the beach and south through the peninsula evidenced no sacrifice of
speed and initiative. As such, the Japanese had little requirement to
build up forces in the traditional sense. Similar to Sir Julian S. Corbett’s
sea power theory, Japanese speed and surprise without loss of initia-
tive created a sort of mass in being. This is not to say that they did
not mass their forces—they certainly did. The speed with which the
Japanese moved gave a semblance of mass that provided maneuver
space while their forces continued to flow ashore.

The Japanese forces quickly captured and controlled critical in-
frastructure on the island of Singapore that contributed to the British
surrender. As mentioned, on 12 February, Japanese forces controlled
the water reservoirs that supplied Singapore. Though the Japanese
did not halt water service to the city, they certainly had the capability.
Controlling this key infrastructure and service must have had some
influence on the British surrender.

The most important finding of this case study is the speed with
which Japan gained multidomain dominance across the length of the
peninsula and the surrounding waters. Though the British ineffective
defense was partially due to political decision making in London, the
reality was that the Japanese quickly marched south along the penin-
sula and dominated nearly the entire way. Only a few hours after the
initial amphibious landing in the north, Japanese bombers completed
their first bombing raid on Singapore. Though there was little signifi-
cant damage, the raid set the tone for the remainder of the Japanese
push south. Still, on 8 December, the Japanese air forces reduced
British air strength in the northern parts of the peninsula from 110
operational aircraft to 50. Japanese air supremacy over the entirety
of the peninsula and Singapore soon followed. Similarly, the Japanese
attained domination of the seas surrounding the Malay Peninsula and

43 Allen, Singapore, 99.
44 Julian S. Corbett, Principles of Maritime Strategy (Mineola, NY: Dover Publications,
2004).
45 Swinson, Defeat in Malaya, 52.
46 Swinson, Defeat in Malaya, 55.
Singapore almost as soon as the British capital ships arrived. By the afternoon of 10 December, both British ships were lost and Japan had control of the sea lines of communication. On 14 February, the Japanese completed repairs to the destroyed causeway across the Johor Strait, adding one more layer to the Japanese area of domination.47 The Japanese now controlled air, sea, and ground access to Singapore. The British subsequently surrendered on 15 February 1942. One can surmise that multidomain supremacy allows the freedom of maneuver to be ultimately successful.

Conclusion
Though this chapter did not discuss the operation in intricate detail, the premise is easy to comprehend. Japan’s thorough planning allowed their army and navy to dominate the Malay Peninsula and Singapore. Nested within their theory of victory was the rapid multidomain control they enjoyed in both the skies above and the seas around Singapore. But if we return to our earlier question, how does this case study affect our comprehension of future war in a megacity?

One way we can look to build and maintain speed and initiative in a megacity is through acquiring domain dominance. The air domain is of particular interest because current doctrine and capabilities do not lend themselves to successful operations within a megacity’s environment. Singapore was initially under total military control by the British, making it easy for the Japanese to gather intelligence and select targets. It is unlikely that a modern megacity will be completely controlled by some group, therefore intelligence gathering, targeting, and fires become infinitely more difficult. Indiscriminate bombing (or even precise targeting that ends in a destroyed building) will likely further the enemy’s cause and enrage the local populace. The military must look to other means to create this domain dominance and one such possibility is the use of unmanned aerial systems, micro air vehicles, and systems and techniques that have yet to be developed.

47 Allen, Singapore, 174.
CHAPTER ELEVEN

FUTURE CONCEPT: HOW UNMANNED AIRCRAFT SYSTEMS SUPPORT MEGACITY WARFARE

General Purpose
The United States military will fight in a megacity. The question is not if but when. Richard Norton, professor of national security at the U.S. Naval War College, states specifically that “if three quarters of the world will live in cities, and we still fight wars, wars are going to be fought in this [urban/city/megacity] environment.” The general purpose of this concept is to describe a paradigm shift for Marine Corps Aviation and implementation of airpower within a megacity environment. Siege warfare is neither feasible nor appropriate for combating an adversary within a megacity. National resolve would likely not be such that the public would willingly ignore the plight of the millions of noncombatants within a besieged megacity. The U.S. Marine Corps must be able to capture the initiative through rapid multimodal, multidomain dominance of specific areas within a megacity. Multimodal and multidomain supremacy describes the ability of the operational force within a megacity to control the air, land, and potentially water within an area via multiple means. The multiple modes of dominance include ground forces, air power, sea power, and cyber capabilities. Major Jonathan T. Frerichs writes of the need to “gain critical maneuver space for the commander.” To support the commander, Marine Corps Aviation should change its theory of victory to provide support within a megacity. In order to support the commander, Marine Corps Aviation should diversify its capabilities through greater use of unmanned aircraft systems. These systems should be able to operate independently as well as in concert with traditional manned aircraft. This concept may offer specific means by which the Marine Corps can add capability within the air combat element (ACE) to better support the ground combat element (GCE) commander.

Based on previous problem framing and case study analysis re-

48 Krause-Jackson and Gaouette, “Homemade Tank Powered by Game Boy Fights Wars of Future.”
garding the question of megacity war, the following concept is offered as one possible solution. The concept represents a narrow view of the defined problems and case study findings. Earlier problem framing describes issues related to aviation doctrine, maneuver, and sensor technology. The concept references these problems in the discussion. The previous case study of the Japanese invasion of Singapore yielded several findings regarding speed, key terrain, and multidomain dominance based on the air domain specifically and ways by which remote and autonomous technologies can assist Marine Corps Aviation to become more flexible and efficient.

**Time Horizon and Risks**

Imagine an increasingly bold and ambitious Boko Haram striking far to the southwest of their current territory in Borno, Nigeria. Imagine this group rapidly moving through Nigeria and establishing a foothold within Lagos, Nigeria. Lagos, the largest city in Africa and 19th largest in the world, has an urban population of about 13 million people. Regardless of the likelihood, the time horizon for the requirement to operate within a megacity environment is, for all intents and purposes, now. By and large, the technology the Marine Corps needs to facilitate nontraditional intelligence, surveillance, and reconnaissance (NT-ISR), targeting, and fires within a megacity already exists. Microair vehicles (MAVs), unmanned aircraft systems (UASs), and remotely piloted vehicles (RPVs) already exist within the military’s inventory. RPVs are what we generally think of as drones and are a subset of UASs. A true UAS does not require human interaction beyond the planning phase because the aircraft autonomously flies its mission, while a pilot or controller “flies” an RPV through all stages of flight. British armed forces currently use similar small air vehicles in an unarmed role. However, the Marine Corps should develop creative doctrine for their use. Swarming, preprogrammed, or autonomous vehicles can add great flexibility with which the ACE can provide ISR and targeting capability

---

50 2018 Revision of World Population Prospects, 26.
51 For purposes of this chapter, the term small air vehicles describes the multiple types of aircraft within the scope of MAVs, UASs, and RPVs.
52 “The UK’s Unmanned Roadmap,” Military Technology 37, no. 12 (December 2013): 76.
that traditional rotary- and fixed-wing aviation cannot provide within a megacity.53

**Military Problem**

To be successful in any operation, a military force must gain and maintain the initiative and domain dominance through speed and surprise. Marine Corps Aviation faces several problems within this concept of victory in a megacity or an extremely dense urban environment. With current TTPs and capabilities, none of these problems are insurmountable, but future adaptations and creative solutions will make victory easier for the Marine Corps. An easier and faster victory with less collateral damage is an obvious benefit. If military operations in a megacity affect fewer noncombatant lives and property, noncombatants are less likely to be aggrieved and thus less likely to take up arms against friendly forces. Some major military problems facing Marine Corps Aviation units fighting in a megacity are:

- Maneuverability in the confines of a megacity
  - Threat envelopes and reaction time. For instance, the RPG-75 has an approximate range of 200 meters against a moving target. The rocket fires at 189 meters per second (m/s) (in excess of 400 mph) and flies approximately 3–6 seconds before self-destruction.54 The SA-7B “Grail” has a 5 kilometer range, flying at nearly 385m/s (in excess of 800 mph).55 The ability to see and react to a system like these is limited within the urban environment due to the canalization if flying below the top of buildings or from reduced identification and reaction time because of the distractions created within the urban environment (e.g., sun reflecting off glass, lights, etc.).

- ISR capability
  - Viewing angle of traditional ISR and NT-ISR platforms.

---

For example, it is difficult to see into a building using traditional ISR tools such as a geosynchronous satellite stationed 23,000 miles above the battlespace.\textsuperscript{56} Other traditional ISR tools like fixed-wing aircraft and drones have similar limitations. Unlike traditional and nontraditional ISR platforms, small air vehicles can fly level with the target upon which they are attempting to gather information.

- Optical sensor capability
  - Night vision devices (NVD), such as infrared cameras.
- Ability to attack specific targets with little or no collateral damage to surrounding spaces

In the next few sections, this chapter matches the above military problems with potential solutions, new technology, and recommended tactical employment changes. These solutions consider the findings gleaned from a recent case study of the Japanese invasion of Singapore in 1941.

**Concept Overview**

The Japanese invasion of Singapore case study provides several pertinent findings. The Japanese were able to overwhelm the massed British forces by creating the semblance of a mass of their own, though the Japanese traded consolidated mass for the ability to maneuver quickly. The Japanese also maintained dominance in multiple domains—land, air, and sea. By dominating these areas and controlling key infrastructure, the Japanese were able to overwhelm the British defenses on Singapore and capture the island. This concept seeks to answer the question of how the Marine Corps can take those lessons of multiple domain supremacy, speed, and mass to impact the future of warfare in the modern, dense urban environment. The concept specifically focuses on the air domain in and above the city.

The Marine Corps set out a vision of distributed operations in the Expeditionary Force 21.\textsuperscript{57} To support the operational intent found there, the Marine Corps should entertain creative solutions for operations within a megacity. This concept entails use of UAS, MAV, and RPV systems to augment traditionally piloted aircraft. This concept’s operating theme requires the coordinated operation of traditional aircraft and small air vehicles. To support this concept, small air vehicles can assist the commander in three distinct ways: 1) flying in concert/close proximity to traditional aircraft in support of the mission; 2) providing real-time NT-ISR capability; and 3) supporting attack and assault support aircraft by providing close air support or NT-ISR support to close air support aircraft.

The Marine Corps creates opportunity for the ground commander by exploring the collection of capabilities created by development of modern technologies such as small air vehicles. As explained below, small air vehicles provide an opportunity for the ground commander to increase his ISR collection, to expand assault support missions, and to reduce collateral damage while destroying point targets.

Application and Integration of Military Functions

Maneuverability

As previously discussed, the dense urban terrain of a megacity restricts maneuverability for traditional UAS and aircraft systems. To maintain sufficient reaction time to enemy threat systems, aircraft must fly above the urban horizon. Ensuring traditional aircraft fly above the cityscape allows additional time for aircraft survivability systems (ASE) and aircrew to react to enemy weapons systems. The ubiquitous RPG supports this argument. With a 200–400m range, traveling at approximately 400mph, aircraft have about 2.1 seconds to react. Reaction time within an urban environment is complicated further by buildings (if flying in or near an urban center) and the ability to identify the threat against the background clutter. Though they likely would not have substantial ASE, smaller air vehicles are less expensive in both

monetary and human capital, thus their loss is more easily accepted. Small air vehicles are not limited by ASE requirements, therefore they can maneuver in an urban environment in unprecedented ways. The flexibility small air vehicles provide to aviation maneuver yields better information to the commander and opportunities for manned aircraft to perform tasks to which they are better suited.

The Marine Corps describes both need and method for distributed operations using the Lockheed Martin F-35 Lightning II program (or Joint Strike Fighter) and other elements of the Marine Air-Ground Task Force (MAGTF). The 2015 “Marine Corps Aviation Plan” defines distributed short take-off, vertical landing (STOVL) operations (DSO) as:

A threat-based limited objective operation which occurs primarily when the entire MAGTF cannot be brought to bear against the enemy. DSO asymmetrically moves inside of the enemy targeting cycle by using multiple mobile forward arming and refueling points (M-FARPs). Using existing infrastructure (multi-lane roads, small airfields, damaged main bases), DSO provides strategic depth and operational resiliency to the joint force.58

Using small air vehicles in addition to current traditional platforms will allow the MAGTF greater flexibility in conducting DSOs. Small air vehicles support DSO from a logistical perspective and a close air support perspective.

Logistical Support of DSO
Platforms such as the Lockheed Martin/Kaman K-MAX power lift helicopter could provide the MAGTF greater flexibility while reducing requirements for traditional aircraft conducting logistics missions. The Marine Corps used two K-MAX aircraft in Afghanistan in 2011 to great acclaim.59 The K-MAX could increase ability to conduct DSO

with fewer logistical requirements on other MAGTF aircraft that may be needed for more sensitive missions. By July 2014, however, the Marine Corps decided they were no longer necessary to operations in Afghanistan and the K-MAX program ended.\textsuperscript{60} K-MAX, or a similar system, can easily conduct logistical support to DSO by ferrying fuel or armament to specified M-FARP locations. Using K-MAX in addition to Sikorsky CH-53E Super Stallions and Bell Boeing MV-22B Osprey assault support aircraft supports greater flexibility by allowing aviation assets to spread the load across the battlespace without increasing manned mission requirements.

Close Air Support of DSO
A traditional Marine Expeditionary Unit (MEU) deploys with four Bell AH-1 Cobras, two Bell UH-1N Hueys, and six McDonnell Douglas AV-8B Harrier IIs. The F-35B Joint Strike Fighter will replace the Harrier IIs within the next several years. Small air vehicles could provide additional close air support (CAS) capability and flexibility in the conduct of DSO. By conducting the DSO mission with both manned and unmanned CAS systems, the MEU can spread its capabilities more widely.

Integration
Instead of these tools being separated by time, space, and altitude, they fly together to conduct their mission. Small air vehicles flying in close proximity to traditional aircraft creates problems. For instance, no helicopter pilot wants a small air vehicle (regardless of size) flying into the helicopter’s rotor systems. A solution to this problem is a proximity signal that prohibits the small air vehicle from coming within a certain distance of the aircraft. If the small air vehicle is “slaved” to the traditional aircraft (“master”) and mirrors its flight, all while maintaining a safe distance, the likelihood of a collision should be significantly reduced. Without modifying existing airframes, small air vehicles can be used in the manner they are used today, where the aircraft

are programmed for the mission at a certain airspeed, altitude, and route. The traditional aircraft simply separate from the unmanned systems by time, space, or altitude. For logistical missions, the traditional means of separation supports the concept but the same method of separation would not realize the same results in conduct of a CAS mission. For the CAS mission, a slave/master relationship between the traditional platform and the small air vehicle would likely provide the best support.

Small air vehicles capable of swarming benefit ground and air commanders. The new requirement will be for additional analysts or information managers for the information swarming air vehicles produce. To translate information produced by swarming drones into actionable intelligence, the intelligence structure within the MAGTF will require modification. Swarming air vehicles also serve to overwhelm enemy defenses. The ultimate goal might be for individual maneuver units as small as squads or fireteams to deploy multiple small air vehicles in support of fire and maneuver.

In August 1997, the Marine Corps Warfighting Laboratory conducted a 12-day experiment at the Marine Corps Air Ground Combat Center in Twentynine Palms, California. The Hunter Warrior Advanced Warfighting Experiment “took a look at enhancing Marine units’ effectiveness by utilizing a combination of experimental equipment and new warfighting tactics and techniques.” The experiment showed that by mixing traditional capabilities with new technologies a small Marine Corps unit could “provide a forward afloat force with the capability to have an operational effect on a larger, capable foe. Hunter Warrior proved that it can be done, but not by using new technology alone.”

ISR and Targeting
Flying above the city restricts a pilot’s viewing angle to a relatively vertical line of sight. Top-down angles create a dilemma within the megacity, especially where high-rise buildings dominate the cityscape.

---

Vertical visibility angles limit ISR, targeting, and fires to top-down approaches. In a megacity, top-down ISR allows the analyst access only to what is not obscured by various structures. Similarly, top-down angles limit targeting and fires to rooftops, entire buildings, or open spaces. Destroying entire buildings is unacceptable in a megacity where limiting collateral damage should be a priority. Smaller air vehicles level the visibility angle, allowing greater visual access to previously obscure places. Additionally, small air vehicles can augment current platforms in the megacity environment. Imagine the following scenario: attack helicopters conducting an escort mission deploy a number of swarming MAVs that provide the aircrew with ISR of specific terrain, a route, or objective area. Those MAVs could increase the situational awareness of the escort helicopters by expanding the visual range of the aircrew.63

Optical Sensor Capability
As mentioned previously, operations in a dense urban environment have detrimental effects on optical sensors.64 One possible solution is removing the limitations to these sensors by mounting them on small air vehicles. By mounting a low-light video camera on a small air vehicle, limitations such as thermal reflectivity and the detrimental effects of environmental lighting can be eliminated. Imagine a small air vehicle affixing itself to the outside of a building, allowing a camera to be placed immediately against the outside surface of a window. This theory requires continued advancement of optical sensors and technology. The research does not address battery capacity, but technology exists to allow small drones and MAVs to recharge via prestaged inductive charging stations.65

---

63 Norway’s Prox Dynamics developed and manufactured a production-quality helicopter “nano air vehicle” called the PD-100 Black Hornet Personal Reconnaissance System. The entire system, including two air vehicles, weighs 1.3 kilograms (km) for a 1.5km video datalink and 25 minutes of flight. “The $40,000 Nano Drone Used by British, German, and Norwegian Army,” Droning On, 1 June 2017.
nologies, the Marine Corps should be willing to use them creatively and develop operating concepts with these tools in mind.

Minimizing Collateral Damage

Minimizing collateral damage in a megacity is not only a moral obligation, but it may also be a military imperative. Innocent civilian and non-combatant deaths may encourage noncombatants to take up arms with enemy combatant forces. Reducing collateral damage may reduce the future strength of enemy combatants. One method by which to provide precise fires is through the use of small air vehicles instead of traditional weaponry. One such concept under development by the U.S. Air Force Research Laboratory (USAFRL) and General Dynamics are weaponized small air vehicles capable of attacking a specific person with little or no additional collateral damage.\footnote{“US Air Force Flapping Wing Micro Air Vehicle,” YouTube, video, 4:32, 16 July 2009.} Another technology pursued by the USAFRL is biologically inspired small air vehicles capable of adaptive flight.\footnote{Team AFRL, “WOW Technologies, BIO Inspired Flight for Micro Air Vehicles,” YouTube, video, 1:38, 28 February 2013.} Using similar technology, local commanders can target or reconnoiter key infrastructure, named areas of interest (NAIs), or numbered targets. These small air vehicles have the ability to enter specific buildings and find the requisite rooms once inside. These small air vehicles can discretely prosecute targets without unnecessary destruction.

These advanced capabilities will not be without a certain level of risk and cost. Any small air vehicle that does not autonomously fly its mission would certainly be at risk of being hacked by an adversary. The informed public likely would not accept a completely autonomous version of a micro air vehicle capable of targeting specific people. Therefore, these vehicles would require authorization from some responsible actor leaving open a window of opportunity in which those vehicles could be hijacked. The financial cost of developing such a product is likely to be relatively high given the current fiscally constrained reality. Militarized micro air vehicles also impart moral, ethical, and public relations costs on the country that uses such technology. It
is difficult to distinguish between the controversial drone strikes seen in the Middle East during the last few years and the potential use of militarized MAVs.  

**Necessary Capabilities**

The capabilities required for these small air systems are as varied as the six functions of Marine Corps Aviation. The full realization of this concept requires continued technological development and creative application of current technologies. Small air vehicles promise flexibility in their use; developers (civilian and military alike) must also be flexible in imagining a future of unmanned air vehicle use. Likewise, future leaders should see use of small, unmanned air vehicles as augmenting traditional manned aircraft. These systems should operate in concert, not independently of each other. The paradigm by which manned and unmanned vehicles do not mix should change; to that end, the future of Marine Corps Aviation is best maximized by teamwork between both systems.

**CONCLUSION**

This concept is a creative solution to an exceedingly difficult problem. One can only accept an attempt to distill warfare in a dense urban environment such as a megacity to a short document for what it is: a possible option to solve one perspective of war fighting within a megacity. Using small air vehicles to augment, support, and extend current aviation capabilities will take time, experimentation, and patience. The majority of technologies mentioned in this concept already exist, and their potential uses are limited only by our own ambitions. The British Army bought 160 Black Hornet MAVs for $20 million. Likewise, for a relatively small sum, the Marine Corps might invest in similar technology that could greatly expand Marine Corps Aviation capabilities.

This concept is not merely a collection of current and future ca-

---


CHAPTER ELEVEN

pabilities but shows a possible future in which the Marine Corps can be better prepared for warfare in a dense urban environment like a megacity. Current Marine Corps capabilities prove the force as capable of dominating the ground and rooftops. The concept offers a means by which the Marine Corps can also dominate the space in between—in a megacity—this space is within the individual buildings. The capabilities offered herein create an opportunity for the ground combat element to better perform its mission.
Virtual Resistance Networks

Enabling and Protecting Electronic Information Flows in the Megacity

By Colin R. Relihan

Under current Chinese law, Hong Kong residents can only vote for preapproved political candidates, making it impossible for opponents of Beijing to get on the ballot. By September 2014, the situation had frustrated attempts by grassroots groups, such as Occupy Central, to achieve greater democracy in Hong Kong, leading to a weeklong boycott of classes led by Scholarism, a student group. Approximately 13,000 students campaigned against China’s encroachment on Hong Kong’s governance. The protests expanded when the Occupy Central movement and Scholarism-led campaign combined. Riot police advanced on the protesters in Hong Kong’s Admiralty district in the territory’s worst incident of civil unrest in decades, leaving 38 people injured and hospitalized and 78 arrested.

The development of megacities and the rapidly evolving information and communications technology environment likely will overwhelm traditional approaches to intelligence and information operations (IO). Megacities are the focal point for a vast array of electronic and physical networks with highly globalized social and economic connections. Rapid demographic change can stymie any military force’s attempt
to gain an understanding of the battlespace. Information and communications innovations such as big data analytical techniques and social media offer new opportunities to understand human terrain. These same technologies create new ways for IO planners to push narratives to target audiences on a massive scale. More people are now able to register their reactions to political change in an accessible, open-source environment such as the internet than ever before. Crowd-sourced intelligence has proven useful for military operations without a human adversary, such as foreign humanitarian assistance and disaster response (HADR). The explosion of social media and other communications platforms can simplify the task of building a “social radar” for monitoring sociopolitical developments in electronically connected megacities.¹ But for military intelligence and IO officers, optimism about the ability of Web 2.0 user-generated content to deliver endless streams of useful social media information may be premature. In the rapidly expanding megacities of the developing world, nonstate armed groups—drug cartels, terrorist groups, and ethnic militias—are likely to attack and subvert electronic social networks that challenge their influence over the operational environment. To prevent the shutdown of these virtual resistance networks (VRNs) by violence and subversion, U.S. military and interagency actors will need to encourage higher volume online information flows from local civilians.² And if the American military seeks to use this open-source data to weaken militant groups, it must devise engagement, counterintelligence, and force protection strategies that safeguard local civilians providing this intelligence.

This chapter recommends that the U.S. military develop ways to work with VRNs. While civil society has taken the lead in providing technical support to online actors suffering from government censorship or repression, only the military or other security forces can

provide the physical protection necessary to protect VRN participants from real-world reprisal. Criminals and militants have long been able to deter civilians from sharing information with governments and civil society through traditional media, and these groups will likely improve their capability to track unwanted information flows in cyberspace as well. Because of the decentralized nature of online social networks, the military-VRN link will necessarily be an indirect quid pro quo partnership. The network provides open-source intelligence and the military provides protection. Such a relationship will blur the line between intelligence collection, information operations, and civilian security. A joint interagency task force can take advantage of the megacity’s connectivity, global links, and density to support layered defenses for VRNs in the face of armed group coercion. If secured, the VRN can provide the basis for an electronic counterinsurgency, particularly in environments where local host-nation governance is too weak or corrupt to be the focus for resistance. A VRN with thousands of participants willing to provide information online can produce massive amounts of sociocultural data, security atmospherics, and other intelligence for the military commander. These participants can come from the local urban area or involve global allies, such as diaspora members, activists, and connected commercial actors.

The development of an open VRN also can serve as an IO objective in and of itself, as militants will be less able to deter local civilian involvement in online information sharing if they see that resistance is possible. Effective collective action by the megacity public is only possible if there is sufficient security. But the solution to physical threats to virtual networks may not be found by exerting more direct control—increased classification of intelligence sources and centralization of IO messaging—but by accepting the information decentralization of the evolving urban environment. Indirect influence over massive, private social networks creates security and IO risks, but open-source electronic media provides speed and volume advantages to the military planner not available through military and government resources alone.
NEW INFORMATION NETWORKS IN THE MEGACITY: OPPORTUNITIES AND CHALLENGES

Traditional U.S. military doctrine recommends isolating urban areas to retain initiative and ability to maneuver, as the high density of people and infrastructure can complicate operations. Even if physical isolation were achievable, growing electronic connectivity and globalized socioeconomic networks makes cutting off the megacity’s information links to the outside world next to impossible and generally undesirable. Vital sections of the population rely on internet connectivity more and more, particularly youth who form the bulk of mass protest movements and criminal/militant groups alike. A Pew Research Center 2014 study shows that the 18- to 29-year-old generation across the developing world is rapidly adopting internet, social networking, and smartphone technology far ahead of their older counterparts.

This rapid change can be destabilizing. David Kilcullen claims that the largely uncontrolled expansion of megacities clustered along the world’s coasts, and deeply connected with the rest of the globe, will drive future conflict. Modern information technologies, connected youth social movements, and global online activism have already helped feed disruptive change throughout the Middle East during the 2009 Iranian “Green” movement protests and the 2011 Arab Spring, as well as the 2014 pro-democracy demonstrations in Hong Kong. Turning off virtual access, whether done by local militant groups, censoring governments, or a U.S. military seeking to exercise control, may precipitate a broader regional crisis. Megacities serve as the nodes

---

for crucial regional and even global social, economic, and electronic networks. It is more likely that the U.S. military will find itself trying to preserve these linkages to safeguard regional stability than seeking to shut them down.

But if megacity growth, economic globalization, and communications innovations have made old military solutions to the urban battlespace obsolete, they also offer opportunities. Growing penetration of cellular phones, internet, and social media use in developing world cities provides new opportunities to gather information on dense, rapidly changing urban environments. Populations that previously existed in the city’s shadows, living in slums, and participating primarily in gray or black markets can now connect to the rest of the world through new modes of informational, social, and economic exchange. Manuel Castells expresses an optimistic viewpoint, claiming that “the emergence of mass self-communication offers an extraordinary medium for social movements and rebellious individuals to build their autonomy and confront the institutions of society in their own terms and around their own projects.” According to Castells, these tools later allowed Middle Eastern nonstate groups to coordinate activity and disseminate large amounts of information through massive many-to-many online networks. This information “counter-power” allowed well-organized but largely unarmed groups to challenge state repression and censorship during the Arab Spring.

So new technologies have created new ways for disadvantaged populations to coordinate and to participate in urban governance, and

---

8 The concepts behind terms such as developed and developing worlds are beyond the scope of this chapter. However, additional information on how their complexities may impact urban warfare can be found at Tariq Khokhar and Umar Serajuddin, “Should We Continue to Use the Term ‘Developing World’?,” Data Blog (blog), World Bank, 16 November 2015.


10 The term many-to-many networks refers to information generated and received by multiple sources, such as social media and other internet-based forms of communication. See “1 to Many, Many to Many, and Many to 1—for PR and Inbound,” IMRE (blog), 11 January 2018.

they have done so by increasing the ability of online networks to share information publicly. In Nairobi, Kenya, the Map Kibera project allows local populations to provide “volunteered geographic information” to map previously uncharted sections of the city.\textsuperscript{12} In New York, the Occupy Sandy movement used social media–driven crowdsourcing to improve distribution of humanitarian aid in the immediate wake of a natural disaster.\textsuperscript{13} Both systems rely on decentralized methods to collect and disseminate information, gaining in speed and volume what they lose in direct control. Civil society has taken advantage of these techniques, but the military also is capable of leveraging crowdsourced information to improve situational awareness. Michael T. Flynn, James Sisco, and David C. Ellis rightly caution that geospatial visualization of social media “big data” is insufficient on its own for good sociocultural analysis of the potential battlespace.\textsuperscript{14} But social media’s utility as an intelligence source will likely improve, as future urban environments will be more saturated with open-source electronic data than in the past. Past network analytical products may have focused on nondigital links, such as tribal affiliation or black-market economic ties, but urban populations of the future—particularly youth—are more likely to organize and communicate online. This shift makes mass collection and analysis of publicly available online social network information more vital than before. If the battlespace’s population lives online, then that is where the U.S. military must go to find intelligence.

OPEN SOURCE UNDER ATTACK
Crowd-sourced intelligence has proven useful for missions without a clear adversary, such as foreign humanitarian assistance/disaster


\textsuperscript{13} Eric Ambinder et al., \textit{The Resilient Social Network: @OccupySandy #SuperstormSandy} (Falls Church, VA: Homeland Security Studies and Analysis Institute, 2013).

\textsuperscript{14} Flynn et al., “‘Left of Bang,’” 17.
relief, but harnessing social media analysis in a conflict environment raises new problems. Criminals, terrorists, and insurgents have always targeted local nationals who report on their activities to state or foreign authorities. They will likely continue to do so against perceived internet or social media informants, attacking and subverting electronic networks that challenge their influence over the operational environment. States such as Iran, Egypt, China, and others have clamped down on online dissent with varying levels of success, but nonstate armed groups will increasingly target civilian electronic networks as well.

Many militant groups and criminal organizations will likely emerge as a hybrid electronic-physical threat, integrating electronic warfare strategies with their traditional ability to use violence to deter civilians from participating in open-source resistance networks. They will often better understand local environments, complicating security force response by nesting themselves among the most dispossessed groups in the city and developing difficult-to-target transnational links. Some of their strategies are simple information denial, such as with the Islamic State’s 2014 shutdown of Mosul’s cell towers ahead of an expected Iraqi counteroffensive. Others are more sophisticated, such as Mexican drug cartel Los Zetas’ communications arm, La Direccion. It reportedly collects electronic intelligence to prevent law enforcement, rival cartels, and the public from interfering in its drug and other illicit businesses. In some cases, state/nonstate armed group online collusion will emerge, possibly as seen during the 2007 and 2008 Estonia and Georgia cyberattacks. There is widespread suspicion that Russian organized crime used its hacking capabilities to support a state’s political aims. Groups that mix criminal entrepreneurs and political motivations are especially likely to have the resources and willingness to pursue this hybrid strategy against VRNs.

In a 2010 speech on internet freedom, then U.S. secretary of state Hillary Clinton claimed that “information has never been so free,” recognizing that state censorship posed one major threat to internet freedom.\(^\text{18}\) But nonstate armed groups pose a different threat, using coercion to prevent VRNs from developing, imposing what John P. Sullivan called “zones of silence” when he described the cartel-dominated information environment in northern Mexico.\(^\text{19}\) If the U.S. military operates in a future megacity conflict and does not protect these VRNs from militant intimidation, it will have little social radar to monitor.

Events in the Middle East—primarily the 2011 Arab Spring but also the 2009 Iranian Green Revolution—are among the most commonly cited examples of the future role played by social media networks in fostering resistance networks.\(^\text{20}\) Twitter, Facebook, and cellular phones all allowed antigovernment activists to organize protests and share information with the outside world. During the Arab Spring, government countermeasures to limit protesters access to the internet largely failed. Local activists and their international supporters developed innovative workarounds for continued access, such as a program that evaded an Egyptian internet ban by converting voicemail messages into online text “tweets.”\(^\text{21}\) Cyberspace-only repressive strategies failed, but elsewhere hybrid physical-digital strategies met with greater success. Also in 2011, but across the Atlantic, the hacker network Anonymous launched Op Cartel, threatening to reveal information on Los Zetas members and Mexican government associates to the public. Los Zetas did reportedly release an Anonymous-associated Mexican hacker, but countered the larger threat to reveal information by claiming it would kill 10 random citizens for every name

\(^{18}\) Hillary Clinton, “Internet Freedom” (speech, Washington, DC, 21 January 2010).

\(^{19}\) John P. Sullivan, “Attacks on Journalists and ‘New Media’ in Mexico’s Drug War: A Power and Counter Power Assessment,” Small Wars Journal, 9 April 2011.

\(^{20}\) Castells, Networks of Outrage and Hope, 53–66, 94–105; and James Jay Carafano, Wiki at War: Conflict in a Socially Networked World (College Station: Texas A&M University Press, 2012), 57–62.

\(^{21}\) Castells, Networks of Outrage and Hope, 61–66.
States may feel constrained from using extreme violence against online informants and activists, but many gangs, terrorist organizations, and other nonstate threats that proliferate in developing world megacities will feel no such restraint.

In this contested environment, enabling and protecting online information networks is difficult because their source of strength also makes them fragile. According to James Jay Carafano’s study of electronic social networks and conflict, only a few actors in any online information network—broadcasters—are responsible for the vast majority of activity linking different network segments. Nonstate armed groups can quiet whole networks just by intimidating or killing the most active broadcasters. Potential social network participants face a collective action problem as broadcasters create value for all network members who want to resist militant influence. However, in the face of widespread intimidation, few or none are willing to take on these crucial, but vulnerable, nodal positions in an online information network. Violence deters anyone from exercising the crucial “network-making” power that creates links between subnetworks and ensures sufficient information flow among the members. Without these key actors, local civilians are likely to act rationally and rely on “self-help” strategies that increase their personal security without providing broader resistance. But without coordinated action, thousands of individual rational decisions to avoid attracting any reaction from a violent cartel or militant group—gated neighborhoods, shuttered newspapers, and mass migration to safer areas outside the urban area—destroy the city’s resilience.

Stephen Graham called this tendency urbicide when describing wartime Baghdad, where walls, security guards, and other security measures broke down the vital economic and social activity that gave

---

23 Carafano, Wiki at War, 8–9.
the city life. Preventing urbicide and zones of silence is particularly relevant for megacities of the future, which will serve as the center of regional and even global economies. Graham admonishes that turning off informational, economic, and other flows in an attempt to manage the security situation is a form of “suicide.” Conventional military operations commonly disrupt and destroy, but information-centric megacity warfare seeks to protect civilian open-source networks and create resilience. To prevent urbicide and restart the city’s circulation, intervening military forces will need to address two broad categories of action: countering zones of silence and protecting VRNs. These efforts will require intervention strategies based in both cyberspace and the physical world.

COUNTERING ZONES OF SILENCE

A healthy, active online information environment will provide analysts sufficient data to exploit methods, such as sentiment analysis and social network mapping, to build up an intelligence picture of the urban battlespace. But this may not initially be possible for many neighborhoods where zones of silence have developed. Combining geotagged tweets, other social media posts, and telecommunications infrastructure in a common visualization will allow the joint task force commander to identify the areas of the city that produce little security or sociocultural atmospheric information. There may be multiple reasons for a lack of information emerging from a neighborhood. Militant groups may be intimidating the local population, who are deterred from providing online resistance or information. The next section will look at U.S. military options when nonstate armed groups are creating these data black holes by targeting online information networks. These techniques also may prove useful if the reasons for silence are rooted in a neighborhood’s lack of economic development or political apathy resulting from being ignored by the host-nation government.

There are several measures U.S. military elements can take to raise the “volume” of online networks. Communications and engineer-

---

ing detachments can increase the local population’s ability to access online networks, especially if militant groups respond to civilian reporting by attacking or subverting existing internet or cellular infrastructure. Instead, the task force can crowd seed internet connections by sowing Wi-Fi hubs or cheap internet-accessible mobile phones throughout the megacity. This can help ensure free online connections available to civilians interested in reporting on security issues. Partnerships with local businesses and civil society can build further sources of resilience and a positive local-centric IO message. Engineering elements can partner with local information technology (IT) firms to provide a broadband backbone for the megacity. Increased bandwidth will allow local civilians to not only post text on social media, but better enable use of camera phone and video capabilities to improve the quality and impact of their messages. The Arab Spring and Iranian Green Revolution experiences showed that the more options for online resistance, the better. Multimodal systems reliant on no single transmission conduit and using multiple available technologies offers flexibility to local populations if militants threaten one communication platform or another.28

Besides direct involvement in building information infrastructure, engagement with local business and IT communities can help reduce zones of silence. Even in developing countries, megacities may be centers for a nation’s telecommunications investment and IT elite. Developing world urban centers as diverse as Bangalore, India; Monterrey, Mexico; and Cairo, Egypt, are regional IT and media centers. The city’s IT business sector and universities are likely sources of computer-savvy individuals for the host nation, civil society, or adversary, so the U.S. military should treat them as key human terrain.

Engagement with these groups provides three potential advantages. First, they provide local knowledge of the operational environment, which can be vital in developing strategies to encourage local participation in online networks. Second, they provide credibility. U.S. military efforts to build Wi-Fi networks or develop social media platforms may raise suspicion from many urban populations worldwide, 28 Castells, Networks of Outrage and Hope, 61–66.
but locally developed initiatives will likely be more acceptable. For example, in cartel-plagued Monterrey, Mexico, local businesses helped develop Tehuan, a social network focused on public safety reporting. Because of its potential role as a force multiplier and IO conduit, U.S. military outreach to a megacity’s business/IT sector is crucial in creating information advantage in a social media-saturated environment. Finally, the adversary also can attempt to take advantage of this element of the human terrain to boost their information operations. For example, some IT workers in Bangalore, India, have created greater instability by providing logistic support to Islamist terror groups. Engagement that not only fosters communication but economic development keeps these key cyberspace actors employed and less likely to provide services to nonstate armed groups.

Information dispersal is another option to combat zones of silence. The military can leverage transnational partners, such as diaspora organizations or multinational corporations with interests in the target megacity. Civil affairs or Department of State personnel can engage local civil society through these transnational actors. Local actors are more apt to provide intelligence if it is passed through a trusted intermediary via more secure, but still private, means such as virtual private networks (VPNs), financial remittance systems, and corporate reporting mechanisms. Having multiple information conduits inside and outside the megacity for local actors to push security reporting provides the layered, resilient defense necessary to protect online information networks participants from discovery, while still maintaining the volume and IO advantages of an open-source network. Other mission sets will address the civilian network’s security concerns more directly.

PROTECTING VIRTUAL RESISTANCE NETWORKS
If the U.S. military and interagency can help local actors connect to online networks to ensure mass security reporting, it is vital that the

29 “Acerca del CIC” [About the CIC], Centro de Integración Ciudadana.
United States develop methods to protect networks threatened by nonstate armed groups. The VRN protection mission is critical for two closely related reasons. First, civilian open-source networks are fragile, large, and potentially influential, but they often rely on a limited number of vulnerable nodes. Broadcasters and network managers allow social media systems to produce massive quantities of data by linking large numbers to the network. The same quality makes these networks fragile if key nodes are targeted. However, this vulnerability can simplify the military’s job. If the military can identify and protect those key nodes—a popular blogger, a public-minded software developer, or a locally trusted nongovernmental organization (NGO)—it can safeguard the whole information-producing system.

In a related concept, physical protection—not just cybersecurity and network expansion measures—is crucial because it is a mission that civil society actors often cannot replicate. During the Arab Spring and the 2009 Iranian Green Revolution, outside IT-savvy actors used many of the techniques described in the previous section to counter zones of silence without outside government assistance. In the face of government attempts to restrict protesters’ network access, outsiders—diaspora populations and online activists—enabled local groups to maintain access to social media and other communications tools. But hackers and diasporas could not provide the physical protection local protesters needed. In the case of Cairo and Tahrir Square, local soccer fan networks provided necessary muscle to keep government security forces away, while in Mexico, bloggers died as host-nation security forces were often outgunned and subverted by cartel enforcers.31 Both the U.S. government and private actors have multiple options to expand opportunities for high-volume social media reporting and big data open-source analysis. The U.S. military will often have advantages over private actors in terms of resources and access to transnational partners, but protecting VRN participants from physical reprisal is a task that only government security forces can truly do. And

if host-nation security forces are overwhelmed, corrupt, or not locally trusted, the U.S. military and its interagency partners may own that network protection mission, both in the physical and cyberspace realms.

The VRN protection mission consists of two parts: identify and protect. The joint task force needs to identify what nodes are most critical to the network’s survival and success and which ones are most threatened by violent actors. Open-source analysts could identify key actors within the megacity already at the center of information-centric resistance. Traditional counterintelligence capabilities could also help identify the reprisal and extortion networks of nonstate armed groups. Analysis should move beyond reactive measures to assess preemptively which network nodes are most likely to be targeted in the future. Open-source intelligence officers can perform social network analysis to assess which online actors are central to information flows. Integrating open-source social media and counterintelligence analysis should help assess current threats. The intelligence cell’s ultimate goal should be to develop protection measures for civilian network participants even before the militants’ reprisal architecture has identified the target. The ability for preemptive protection measures is necessary because, once a nonstate armed group has decided to intimidate an online informant, it is often too late to reassure network members that their activity is safe.

How we reassure key civilian network participants that they can continue their organizing activity is crucial. Online activists, journalists, NGOs, and other groups may not trust the U.S. military. Building trusted relationships is more important than traditional command and control mechanisms. The joint force commander cannot give orders to a civilian information network. Attempts to overtly influence the online network would likely backfire by undermining the IO message that the local population is creating its own forms of resistance. Interagency partners may have more credibility in this area, with military intelligence, communications, maneuver, and civil affairs elements prepared to support the Department of State, the U.S. Agency for International Development (USAID), and other civilian agencies. Network influence and protection boards (NIPBs), consisting of military, intelligence, and
other interagency elements active in the megacity would allow for a coordinated U.S. government civilian protection effort. Intelligence and military members would be responsible for identifying which online activists and groups need protection. NIPB members would de-conflict which agency will be responsible for each target and decide who receives what kind of protection. Intelligence analysts also can identify potential sources of support outside the megacity, such as diaspora organizations, multinational corporations, or NGO networks. NIPB members can then arrange for other U.S. government elements to engage those out-of-theater organizations.

The military component is well-suited to address physical protection concerns. Civil affairs and security assistance teams can engage with civil society and business organizations to improve physical security measures. Training can be offered through secure online means so as to avoid associating the network node too closely with the U.S. government. Military patrols in commercial areas can increase civilian confidence and reduce opportunities for militant extortion teams to operate. Finally, countersurveillance and close protection teams can respond to immediate threats or cover particularly critical information nodes. Special operations forces can focus direct action operations against a nonstate armed group’s reprisal and cyberspace teams. As nonstate armed groups increase their options for identifying online informants, U.S. military and interagency elements will need to prepare for multiple avenues of subversion from the militants’ reprisal architecture. Los Zetas operations in northern Mexico during the past several years suggest that future nonstate armed groups may exploit three broad capabilities to identify online VRN participants.32 They can use traditional informant networks to identify online activists with insufficient offline operations security measures. Nonstate armed groups (NSAG) can develop organic computer network exploitation capabilities to identify VRN participants, possibly by recruiting local IT professionals. Finally, they can bribe law enforcement and security

32 Krepinevich, Cyber Warfare, 22–23; Grayson, Mexico, 188; and Stewart, “Anonymous vs. Zetas Amid Mexico’s Cartel Violence.”
personnel into providing them access into a country’s telecommunication infrastructure.

Improving nonstate cyberspace capabilities highlights the need of the joint task force or interagency to support virtual protection measures through programs to improve network participants’ cybersecurity. It may be impossible to prevent a determined militant reprisal team from identifying some online activists, but cybersecurity experts inside and outside the U.S. government can provide training and tools to increase the likelihood of remaining anonymous. Cyber protection teams provided by U.S. Cyber Command, USAID contractors, or partnered NGOs may be most effective in improving civilian online security practices, with local threat and trust levels driving the NIPB’s decision. Outside diaspora and civil society are another avenue of cybersecurity support, as local actors are more likely to provide intelligence if it is passed through a trusted intermediary. Having multiple security programs inside and outside the megacity helps provide the layered, resilient defense necessary to protect the VRN while still maintaining its open-source advantages. Encouraging and protecting sources of crowd-sourced intelligence online can address all elements of this layered defense—focused on anonymity, dispersal, and mass. This may increase overall civilian security if it even partially replaces nondigital institutions, such as analog media like newspapers and radio stations with targetable physical addresses.

The military’s final contribution to protect online information networks is to prevent catastrophic subversion of the network. Besides the node-specific NIPB effort, the intelligence cell also needs to monitor the “commanding heights” of the electronic domain in the urban battlespace, including the city’s telecommunications infrastructure, host-nation law enforcement, and the IT sector (both businesses and universities). Extorted telecom executives, unemployed computer science graduates, and corrupt police wiretap officers may provide militants with access to subvert online information networks on a massive scale. Joint task force counterintelligence activity, commercial and academic liaisons, and patrols of key IT-related terrain all reduce the chances of a catastrophic subversion of the whole information network. Focusing interagency anticorruption efforts on government ac-
tors with greatest access to telecommunications networks may also mitigate risk. In the end, protecting online information networks is similar to other aspects of military operations in the megacity. It favors resilient systems and open information flows over disruption, destruction, and urbicide.

THE ELECTRONIC COUNTERINSURGENCY: TRANSFERRING VRN PROTECTION TO THE HOST NATION

Effective collective action by the megacity public is only possible if they can organize and share information, but only with sufficient security. The U.S. military helps create security and local resilience by expanding information access, creating electronic safe havens, and creating positive feedback loops between the U.S. government and the local population. U.S. forces may develop an indirect information-for-security quid pro quo relationship with these networks, but this is an indirect connection. Indirect influence over massive, private social networks creates security and IO risks. The military cannot control the VRN’s message, and the intelligence cell will need to verify the most critical elements of VRN-provided intelligence to provide a safeguard of militant subversion of the network. But open-source electronic media provides speed and volume advantages to the military planner not available through military and government resources alone. The fact that the military commander cannot control these online information networks reinforces their power as information source and change agent.

If protected and access is assured, online information networks are likely to grow. A large enough network could provide sufficient quantities of intelligence that would allow government forces to counteract nonstate armed threats. The large network itself could also serve an IO purpose by its continued public existence in the face of militant disapproval, rallying others to see resistance as possible. This is another advantage of an open-source network over a clandestine one. If adversaries attempt to break it but fail, the network becomes stronger.

As time passed, continued reporting from the online information
network could allow the U.S. government to shift responsibility back to host-nation security forces. As seen in locations as diverse as Mexico, Egypt, and Hong Kong, online civilian networks will commonly push anticorruption messages and other campaigns designed to compel improvements in host-nation government and security force performance. As the online information network matures, the immediate militant threat recedes, and the activists’ ability to monitor corruption improves. This may enable the military to work with DOD or Justice Department-vetted host-nation security or law enforcement units. The joint task force could transfer its network protection duties, including the NIPB, to these trusted host-nation elements, creating intermediate structures that would survive the U.S. military’s departure. This could support the long-term U.S. end state of enabling host-nation security structures to manage the militant threat after the U.S. military’s withdrawal. In Castells’s words, the information networks shift from a “network of outrage” focused on militant coercion to a “network of hope,” a change agent that provides grassroots pressure for longer-term improvements in civilian security.33

CONCLUSION

Current military doctrine focuses on avoiding a fight in urban areas, isolating them whenever possible. But megacities are too vital to cede to insurgents, drug cartels, and terrorists, as they serve as economic, social, and political hubs on a regional and global scale. While megacities create many problems, growing so quickly multiplies security and governance issues for U.S. partner countries, and these countries require the economic vitality these urban areas produce. As a result, warfighting doctrines that disrupt or isolate those crucial flows threaten a country’s overall health. Physical barriers, such as those built in Baghdad or Belfast, are isolating, as are barriers in the informational environment. NSAG can threaten the megacity’s electronic flows, threatening the local population, corrupting host-nation institutions, and preventing local reporting of security threats. Information flows

33 Castells, Networks of Outrage and Hope.
such as these are the urban area’s central nervous system, sending messages that drive change within private and public-sector institutions to counter threats to the megacity’s well-being.

Enabling online information flows and the VRN protection mission allows U.S. military forces to help restart those flows where violent and subversive actors have been able to impose zones of silence, leaving the host-nation government incapable or too compromised to respond. Civil society may exist but remains incapable of coordinated resistance in the face of NSAG threats. But a U.S. military/interagency task force can take advantage of emerging trends in the megacity to boost the local population’s own ability to report and resist. Increasing electronic connectivity globally provides new options to develop forms of online “counterpower” to militant and criminal influence, in the form of the VRN. Globalization creates new communities of interest outside the megacity that can support the VRN’s development. The megacity’s own vitality, in the form of dense commercial and social networks, can become a mechanism to jump-start reporting. The VRN can support a public intelligence cycle whereby increased reporting by network participants on security threats improves the military’s ability to protect the VRN. Traditional military capabilities, such as counterintelligence and special operations direct action, buttress the VRN in areas where the public does not have the will or capacity to act.

But the end-state goal of enabling and protecting VRNs is to make U.S. military intervention unnecessary. The U.S. military and interagency enable the VRN to grow in its early stages, helping it over the threshold of the collective action problem. Over time, it should acquire its own momentum, building its own links to the global community and developing its own tools for online security. In the long run, the VRN supports real-world civil society mechanisms, such as NGOs and media organizations, previously weakened by militant coercion. Ultimately, the VRN may challenge the host nation’s own poor security and governance performance, whether a result of corruption or limited capacity. VRNs based in the megacity, a likely stronghold of political and economic strength, are well-placed to pressure the host-nation government to improve its performance and provide secu-
rity. VRNs thus protected and shepherded are able to reestablish the feedback loop between the government and the governed. This will enable U.S. military forces to hand responsibility back to host-nation forces, with politically active VRN members providing the incentive to counter future threats in the target megacity.
The City Prism
A Triangle of Urban Military Operations

Henrik Breitenbauch, Mark Winther, and Mikkel Broen Jakobsen

Haiti saw a resurgence of political and economic actions along with a newly elected leader in 2006, which would prompt the United Nations to extend the mandate of the UN Stabilization Mission in Haiti (MINUSTAH). In Port-au-Prince, Haiti, however, the heavily armed gangs controlled the streets and the city’s slums. Gang leaders garnered support from the local population through fear and intimidation, but also by providing services they could not get from the government. The MINUSTAH actions to counter the gangs was implemented in a gradually escalating series of military operations attacking the gangs from multiple perspectives.

INTRODUCTION
Cities are centers of power and resources, and power and resources drive political conflicts. Where there are people, there are conflicts. Increasing urbanization also means a rising number of political conflicts in urban areas. Some of these conflicts will be violent, ranging from

---

1 All authors are affiliated with the Centre for Military Studies, University of Copenhagen.
organized crime and forceful political factions to armed resistance and civil war, often with international dimensions. Some of these violent conflicts and its actors will merely be criminal, a bane to the local population, while others will be a threat to national or international stability, including transnational terrorism. Because of population growth, urbanization, and poor government, the problem will therefore remain—and likely become further—politically, strategically, and militarily relevant in the decades to come.²

As has already been visible in the campaign to defeat ISIS, Western political leaders will increasingly be faced with choices of whether to authorize the implementation of various kinds of military operations in urban terrain (MOUT) to influence or force an end to such conflicts. Western military and civilian organizations must therefore analyze and make plans to deal with such operations. The combination of the increased share of cities in future operational environments and changes in the Western approach to military operations—including broader political intentions regarding stability and the imperative to protect civilians—poses conceptual and practical challenges for the state and its military and civilian organizations.

When faced with a city as a military problem, the preferred options have traditionally been: avoid them (or lay a siege), or raze them to the ground. Because of the urban topography, the city represents a fundamental challenge for armed forces, as it complicates military activities, such as reconnaissance, the exchange of fire, communications, and even simple transport. This all combines to reduce considerably the ability to acquire an understanding of a situation. Streets

---
² Urban military operations force us to think more holistically about what it is that the military instrument is meant to achieve, but this thinking does not appear automatically. The authors would like to thank Benjamin Jensen for inspirational conversations on, among many other things, the 2015 megacities study with his colleagues at the U.S. Army Chief of Staff’s Strategic Studies Group. See Col Marc Harris, USA, et al., Megacities and the United States Army: Preparing for a Complex and Uncertain Future (Arlington, VA: Office of the Chief of Staff of the Army, Strategic Studies Group, 2014). Parts of this chapter stem from a report on MOUT published by the Centre for Military Studies at the University of Copenhagen in Danish. See Henrik Ø. Breitenbauch et al., Byens prisme: Tendenser og udfordringer for militære operationer i urbant terræn (Copenhagen: Centre for Military Studies, University of Copenhagen, 2016).
and alleyways are transformed into gorges and gullies that limit communications and provide defending forces with perfect conditions for carrying out ambushes. Intervening military forces have therefore traditionally sought either to avoid this theater of operations entirely or, if they possessed adequate firepower, to neutralize the significance of the theater by totally destroying the city without considering the civilian population.

But two factors combine to challenge the Western military organization to think differently and conceive of how to engage operationally with the city. Political demand for broad counterterrorist efforts also include urban operations through warfighting, peace operations, and special forces operations, including combinations of these to provide stabilization. At the same time, Western expectations shaping the use of armed force dictate an increasing political requirement for following international humanitarian law (IHL) and other kinds of normative regulations that work against extensive use of firepower.³

Because urban operations are notoriously difficult, they are at the same time prisms of a larger set of conceptual problems for Western military operations. Since the end of the nineteenth century, Western militaries have, to a large extent, turned into pure warfighting organizations or institutions that exist functionally, as well as at the level of professional self-understanding, to use lethal force to fight and win wars. This division of labor between warfighting and other security tasks has not been fully implemented for the reason that the state that controls the military institution occasionally (and sometimes often) also requires the military to continue carrying out security tasks other than annihilating the enemy, as was the case in earlier days. The task of policing in various meanings of the word (not all of them civilian) thus continues to haunt Western militaries as a kind of professional phantom pain. Western militaries live with a tension between their intentional design (as lethal organizations) and their

³ IHL refers to "a set of rules that seek to limit the effects of armed conflict. It protects people who are not or are no longer participating in hostilities and restricts the means and methods of warfare." See “War & Law,” International Committee of the Red Cross.
political taskers (to not only deter and, if need be, win wars but also to bring conflicts to a peaceful end). Add to this situation the complexities of a quickly growing population in the Global South (a.k.a. the Third World), much of it in megacities outside of formal government control and governance.

Western military leaders are therefore faced with a triple challenge: to increase organizational self-awareness of the warfighting paradigm and its limits (not to destroy it, but to help supplement it and shift gears when necessary); to engage continuously with the political requirements of policing (or peace operations); and to face the new reality of a fast-growing world with battlefields of a size where Western militaries may be able to dominate locally but not seize or hold terrain at a broader scale, including the human terrain. Urban operations challenge us to rethink our approach to conventional operations, particularly regarding the ability to operate in the absence of territorial control and to solve or support civilian police work—both of which fall outside of a twentieth century self-understanding of the military organization.

This chapter introduces a model depicting a triangular space of military operations that enables us to derive and discuss some important overall dynamics of MOUT—dynamics that are typical of this broader set of dilemmas and tensions facing Western military operations, in particular in the Global South.

While the model is a transparent and systematic conceptual construct, it is also merely a heuristic device enabling the structured use of ideal types to derive a broader analysis. It is not predictive, and it is not meant to be an exhaustive illustration of all military operational activities. But what it lacks in detail it makes up for in reach: the model fundamentally challenges the implicit argument of the spectrum of conflict that has undergirded much of U.S. and NATO doctrine development since the 1990s. This full spectrum approach tacitly proposes that the ability to conduct operations at the lower and middle level of the conflict spectrum is included in the ability to conduct high-intensity operations. The operations triangle shows how there is an inherent tension between the two problems sets and corresponding
capabilities—and that these cannot be seen, according to Thomas P. M. Barnett, as “lesser includeds” in overall defense planning.\(^4\)

Two main sections follow. In the first, the operations triangle is introduced, and in the second section, it is applied to the urban environment to identify implications relating to each operations’ ideal type as well as the dynamic mix required for stabilization operations. Finally, we sum up and discuss takeaways.

**THE OPERATIONS TRIANGLE**

Military operations vary with respect to their ends and means. The nature of the city renders the ends more complicated to realize and the operative means more difficult to use. Based on experiences from operations in Mogadishu, Somalia; Port-au-Prince, Haiti; Sarajevo, Bosnia and Herzegovina; and other conflicts in the 1990s, General Charles C. Krulak, in his concept of “Three Block Warfare,” points out that in order to be effective, military forces must sometimes simultaneously carry out classic combat operations, peacekeeping operations, and humanitarian aid all within a three-block area.\(^5\) Krulak’s remarkable analysis briefly summarizes a fundamental—possibly the most fundamental—strategic challenge to military operations; operations do not become successful via combat alone, but they often consist of complex and not necessarily mutually helpful tasks and capabilities.

This section introduces a new way to think holistically about military operational activities. First, we introduce three fundamental distinctions between the different attributes a military operation may have. Second, these systematic distinctions are then used to define three ideal-type military operations, logically combined in a triangle.

The idea of the model is that while each corner of the triangle represents the pure ideal type, every coordinate inside the triangle represents a specific operation, characterized by a mix of the three types, in a given moment. A conflict or an operation may, over time, escape these categories, but the triangle represents a useful tool for understanding the complexity of modern military operations.
