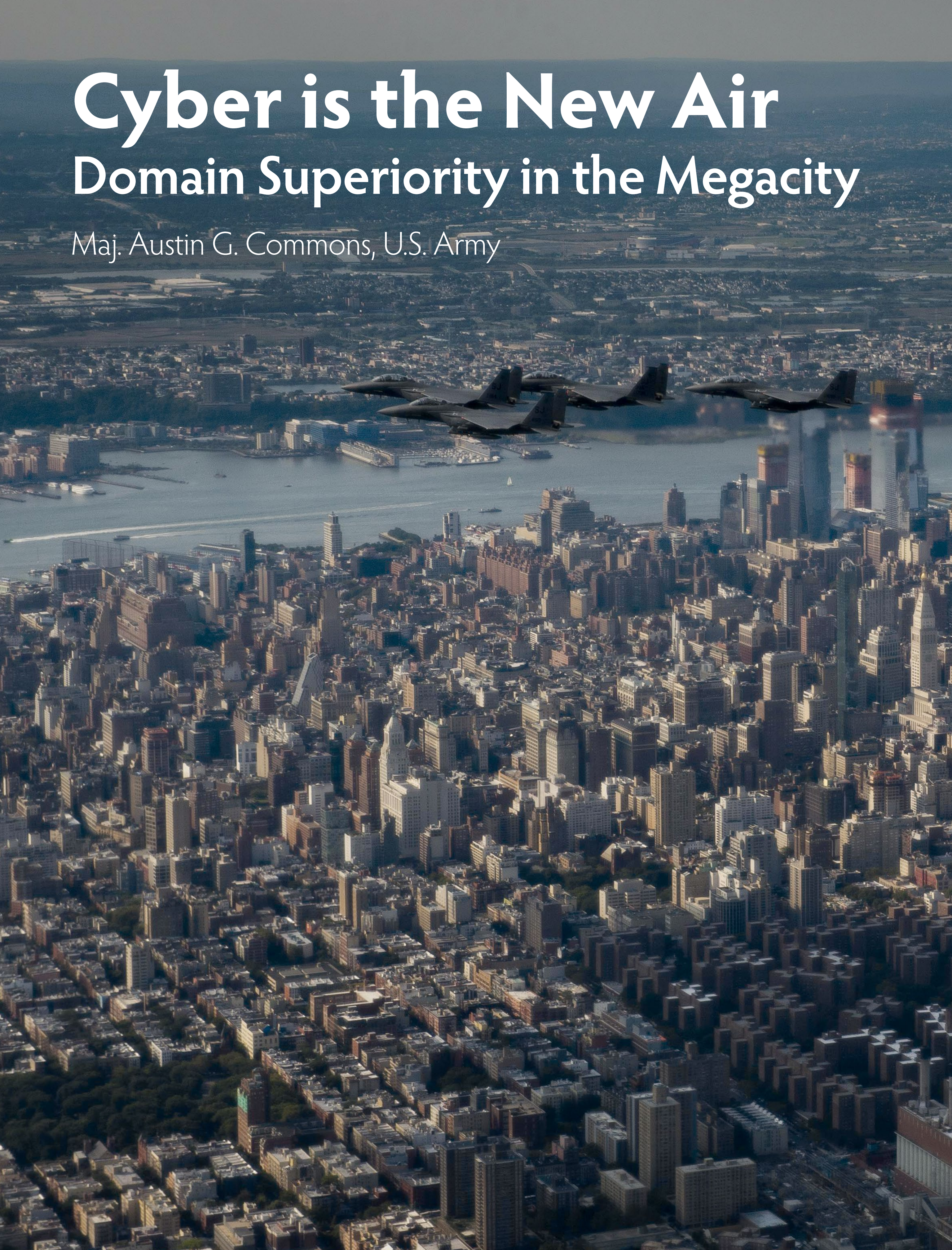
Cyber is the New Air

Domain Superiority in the Megacity

Maj. Austin G. Commons, U.S. Army



War is, at its most elemental level, a human endeavor. Violent conflict on all scales will nearly always take place in the spaces where people live and work. Two current global trends are significantly shaping the human dimension of conflict: the movement of people to megacities having populations of over ten million and the increased interconnectedness of populations and infrastructure. As of 2014, there were twenty-eight megacities in the world, and that number is projected to reach forty-one by the year 2030.[1] Furthermore, a global explosion in internet and cellular access has resulted in cities and populations that are densely networked.

Modern megacities are the most complex environments in the world today, with the city functioning as a complicated and intricate ecosystem. The megacity is unique as an operational environment because it layers three elements: large spaces, complex and restrictive physical terrain, and dense human populations. This environment creates significant friction across all domains

Four U.S. Air Force F-15E Strike Eagles assigned to the 334th Fighter Squadron at Seymour Johnson Air Force Base, North Carolina, fly over the U.S. megacity of New York, September 2017. The massive size and complexity of such megacities that are emerging globally present a range of new challenges to military planners, especially those charged with establishing control through air superiority in the event of an urban conflict. (Photo by Staff Sgt. Andrew Lee, U.S. Air Force) (land, sea, air, space, and cyberspace), providing ample opportunity for adversaries to deny U.S. forces' freedom of action. Gen. Mark Milley, chief of staff of the Army, has highlighted the importance of this problem by calling for the development of concepts for megacity combat.[2] The U.S. military's current joint doctrine is insufficient to address this type of conflict.

Since World War II, joint doctrine has prioritized achieving air superiority as a prerequisite to enjoying freedom of action in the other domains.[3] Megacities, however, with their tall buildings, narrow and crowded streets, and subterranean spaces offer extensive protection from aerial surveillance and close air fire support. Fortunately, a new domain—cyberspace and the electromagnetic spectrum—has emerged as the preeminent medium for understanding and shaping actions in the other four domains. For the joint force to seize, retain, and exploit the initiative in a megacity environment, joint task force commanders must prioritize cyberspace superiority rather than air superiority as an operational prerequisite.

One might argue that the U.S. military's recent decade of experience fighting in Iraqi cities such as Baghdad, Fallujah, and Mosul provides a solid conceptual and doctrinal foundation for urban combat that is applicable on a larger scale to the megacity problem. Joint Publication (JP) 3-06, *Joint Urban Operations*, underwent significant revision in 2009, with updates across all joint functions.[4] These updates comprehensively address the challenges inherent in modern urban environments, citing lessons learned from recent conflicts such as Operation Iraqi Freedom. JP 3-06 provides an accurate description of the challenges faced in urban environments and lays out nine fundamental principles for conducting urban operations:

- Conduct a systemic assessment.
- Integrate all actions within the context of an overarching major operation or campaign.
- Learn and adapt.
- Selectively isolate key portions of the urban environment.
- Apply highly discriminate, destructive, or disabling force to disrupt an adversary's ability to pursue its objectives.
- Establish and extend control and protection of urban sectors and subsystems.
- Persuade municipal governments, groups, and population segments to cooperate with joint force operations.
- Provide essential support into the urban environment to sustain it during the ordeal of combat operations to improve its ability to survive.
- Support improvements to urban institutions and infrastructure.[5]

These principles are objectively sound and reflect years of experience in Iraq and other urban conflicts. However, while this framework may be adequate for smaller cities, the uniquely layered characteristics of the megacity make the current doctrinal framework insufficient to win a fight in this environment. This article outlines the shortfalls in current joint doctrine when applied to the megacity environment and demonstrate how cyberspace superiority can enable the joint force to overcome these disadvantages.

The Megacity Problem: Inadequate Doctrine

Current joint urban operations doctrine is insufficient to guide military operations in a megacity due to the unique challenges presented by their layered combination of size, density, and complexity. As noted above, joint urban operations doctrine prescribes nine fundamentals for commanders and staffs. All of these are essential to winning an urban fight, and all require significant freedom of action to execute effectively—making these fundamentals especially difficult to apply in megacity combat. Two of the most difficult principles to apply in this environment are selectively isolating key portions of the urban environment and applying highly discriminate force to disrupt an adversary. The extreme degree of complexity presented by this environment provides an adversary with a myriad of opportunities to deny and disrupt a joint force commander's freedom of action.

Physical isolation of key terrain is often unfeasible in a megacity due to the long physical distances that a maneuver force needs to travel through a heavily congested environment. Task Force Ranger experienced this in 1993 in Mogadishu, Somalia, physically overwhelmed by the crowds and congestion in a relatively small city that today has a population of "only" 2.1 million.[6] At the operational level, isolation means "cutting the adversary off from the functions necessary to be effective," which current urban operations doctrine describes as being critical for success.[7]

However, even if the key terrain targeted for isolation is relatively small, maneuver forces will often need to move a considerable distance to reach it. Crowded

> “… in any city where the legitimate government is ineffective and unable to provide basic services, criminal and other unofficial networks are inevitably quick to fill the void and thus exert considerable influence and control over the population.”

city blocks connected by narrow, congested streets may make it nearly impossible for ground units simply to maneuver to an area that must be physically isolated. Translating the example of Mogadishu to a much larger megacity illustrates how easily a small-combat formation such as Task Force Ranger can be swallowed up by a large urban population.[8] The numbers of ground troops required to maneuver to isolate key terrain may be unavailable or politically unpalatable. Furthermore, moving to objectives and key terrain is only part of the challenge that fighting in a megacity presents.

Physically isolating key terrain in a megacity environment is also unfeasible due to the requirement to control the lines of communication (LOCs) that provide an adversary force with people, materiel, and information. During the 2008 terrorist attack on Mumbai, India, by the Pakistani extremist group Lashkar-e-Tayyiba, ten attackers infiltrated the city from the water and moved to their targets by taxi, rail, and foot.[9] In addition to these physical LOCs, the attackers and their commanders in Karachi relied heavily on the digital infrastructure of the city to control and coordinate their actions, without which they would not have been able to inflict nearly as much damage.[10] This example represents a network of LOCs that are far too complex for a joint force to control physically. The megacity environment, with its extreme population density, highly interconnected transportation infrastructure, and illicit criminal networks, tips the scales considerably against any security force attempting to isolate and control key terrain. Even with troops numbering in the tens of thousands, physically controlling an urban area consisting of tens of millions of people inverts the force ratios recommended in doctrine.[11] Moreover, physically controlling a conflict area often requires the application of lethal force—another urban doctrine precept.

Applying destructive or disabling force to disrupt an adversary is immensely difficult in a megacity not only due to collateral concerns but also because of the unique complexity of the megacity ecosystem in which adversary networks operate. In a megacity such as Karachi, with a population of 27.5 million, potential adversary groups meld seamlessly into a complex web of illicit networks, with cooperation stemming more often from convenience and financial gain than from shared ideology. Members of extremist groups such as the Pakistani Taliban, the Afghan Taliban, and Lashkar-e-Tayyiba enjoy a symbiotic relationship with the armed criminal organizations that provide their own form of security and governance to the poorly governed slums of Karachi. Furthermore, Karachi is a bustling port city through which large amounts of international commerce flow; it is “Pakistan’s equivalent to New York City, Chicago, or Los Angeles.”[12] The shipping and trucking industries in Karachi employ significant numbers of extremists and other young men susceptible to criminal or extremist recruitment.[13] This industrial base is also a key source of fundraising for the Pakistani Taliban and other extremist groups through extortion and other criminal activities.[14]

Urban operations doctrine specifies that destructive force must be highly discriminate, minimizing the impact on the broader urban environment.[15] However, in any city where the legitimate government is ineffective and unable to provide basic services, criminal and other unofficial networks are inevitably quick to fill the void and thus exert considerable influence and control over the population.[16] Unfortunately, assuming that the joint force could accurately find and fix these networks in place,

Maj. Austin G. Commons, U.S. Army, is a student at the United States Naval War College in Newport, Rhode Island. He holds a BS from the United States Military Academy, West Point, New York. During his career, Commons has served in operational assignments with the 101st Airborne Division (Air Assault), the 1st Cavalry Division, and the 75th Ranger Regiment. He has deployed in support of Operations Iraqi Freedom and New Dawn in Iraq, and Operations Enduring Freedom and Freedom’s Sentinel in Afghanistan.

applying lethal force to these interconnected adversary groups will inevitably have a significant negative impact on the broader environment and population because the lethal force applied against any adversary group or their base of support in a megacity such as Karachi has the potential to cause major disruptions in basic services. Likewise, similar disruptions to regional and international commerce stemming from lethal force could be expected to have the same kinds of effects that would reach far beyond the immediate area of operations for a joint task force.

A Concept for Cyberspace Superiority

While applying joint urban operations doctrine to the megacity fight is extremely challenging, joint task force commanders can mitigate these challenges by prioritizing the attainment of cyberspace and electromagnetic spectrum superiority to have freedom of action across the physical domains. To explore these options, it is necessary to establish a concept of what cyberspace superiority might look like in practice. This concept will closely mirror the concept of air superiority, long considered an operational prerequisite for freedom of action in the other domains. JP 3-0, *Joint Operations*, states that "control of the air is a prerequisite to success for modern operations or campaigns" because it prevents enemy air assets from interfering with operations in other domains "thus facilitating freedom of action."[17] However, as previously discussed, the complexity of the physical and human terrain in a megacity can significantly diminish the advantages gained from air superiority. To mitigate this, superiority in the cyberspace domain can set the conditions for friendly freedom of action in the other domains. Conceptually, for a joint task force to achieve cyberspace superiority in a megacity, it must be able monitor and collect the preponderance of digital communications traffic in the area of operations, access adversary and host-nation digital networks at will, and defend friendly networks against interference by adversaries or third parties.

Current joint doctrine defines cyberspace superiority as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary," which repeats nearly verbatim the doctrinal definition of air superiority.[18] Notwithstanding, this concept goes a step further by establishing a set of concrete conditions that can assist a joint force in evaluating their degree of cyberspace superiority.

The ability to monitor and collect digital communications in a megacity area of operations is key to achieving cyberspace superiority. The inability to see what is passing through the digital terrain is analogous to the inability to conduct aerial surveillance of a physical area of operations. Achieving this will require access to the digital communications infrastructure of that city, to include cellular networks and wired internet. Examples of systems that are able to do this already exist.

Since 2007, the National Security Agency (NSA) has run a collection system, known as Prism, which collects communications traffic from a long list of prominent U.S.-based internet companies such as Google, Yahoo, and Facebook. These companies account for a large portion of global internet traffic, and programs such as Prism provide valuable access points to the cyber terrain of megacities around the world.[19] Similarly, the NSA has access to cellular networks around the world, many of which are owned by U.S.-based companies, through previous agreements.[20] These agreements with both wired and wireless internet providers cover the vast majority of digital communications in any megacity. The remaining cyber "terrain" that is inaccessible through standing agreements will need to be accessed clandestinely and covertly through the myriad of hacking tools at the NSA and the U.S. Cyber Command. Gaining access to these denied communications networks is a crucial component of achieving cyberspace superiority during a conflict.

Digital communication networks that the joint force cannot access provide freedom of action to an adversary in a megacity, while also providing opportunities for an adversary to disrupt U.S. freedom of action. These may be networks belonging to insurgents or criminal organizations, or to a government-controlled communications network run by a hostile nation-state. The air superiority analog would be a portion of the area of operations that are covered by enemy air-defense systems and thus inaccessible to friendly forces under current doctrine.

The Libyan revolution of 2011 provides an example of the impact of denied cyberspace as insurgent groups utilized commercial off-the-shelf tools to create their own digital communications networks to circumvent the Mu'ammar Gaddhafi regime's internet crackdown. By establishing these networks separately from Libya's existing digital communications infrastructure, revolutionary groups were able to procure funding, influence international opinion, pass targeting data to NATO intelligence centers, and avoid the regime's digital spying capabilities.[21]

While the Gaddhafi regime may not provide an example of moral conduct, its military situation throughout the revolution highlighted that being able to access adversary networks is a key component for achieving cyberspace superiority in modern conflict. Though the regime recognized the vital need and had some limited success hacking the Skype calls and other digital communications passing over the insurgent networks, its efforts came too late and too little in the face of NATO support for revolutionary groups.[22] Irrespective, the Libyan example illustrates that without access to adversary networks, the joint force cannot achieve superiority and freedom of action in cyberspace as denied cyber terrain will provide a given adversary a means to disrupt U.S. joint functions while enabling its own.

Understanding the Megacity through Big Data

A second key factor in cyberspace dominance will be the relative advantage achieved by the effectiveness of data collection techniques. One emerging technique that will play an increasingly important role is *big data* collection, since it is nearly impossible for a joint task force to effectively assess and understand the complex megacity ecosystem without relying on massive amounts of digital data collection and analysis. According to current doctrine, conducting a systemic assessment of the urban environment is the first fundamental of urban operations. Doctrine states that an understanding of the urban environment is the basis for planning and executing operations in it.[23] Assessing and understanding a megacity comprehensively and effectively using established methods and tools is an extremely daunting task.

Task Force Ranger personnel take cover alongside buildings near the site of a helicopter crash 3 October 1993 in Mogadishu, Somalia. This is the only photo released of the battlefield during the battle. (Photo courtesy of the U.S. Army)

Task Force Ranger and the Battle of Mogadishu

From 3 to 4 October 1993, a joint U.S. special operations task force fought a prolonged battle through the densely populated streets of Mogadishu, Somalia, after its mission to capture key members of a Somali militia group led by Mohamed Farrah Aidid was met with unexpectedly stiff resistance and a portion of the task force was pinned down in the center of the city. The lessons learned from Task Force Ranger portended even greater challenges in the future for U.S. forces facing the prospect of combat in urban settings and megacities.

Task Force Ranger included units from the 3rd Ranger Battalion, 1st Special Forces Operational Detachment–Delta, the 160th Special Operations Aviation Regiment, and other special operations elements from the Air Force and the Navy. It was given the mission to capture Aidid and dismantle his organization, the Somali National Alliance. On 3 October, it sent a force of 19 aircraft, 12 vehicles, and 160 men to arrest two high-level leaders of the Aidid organization.

The mission began well, with the quick capture of two militia leaders, although one ranger was injured during a fall from a helicopter while fast-roping. However, a large crowd of armed militia and civilians, including women and children, rapidly converged on the scene, congesting the roads and blocking the extraction of the injured soldier and the two militiamen by ground convoy. The situation degenerated further after two helicopters were shot down by rocket-propelled grenades. The task force was forced to defend itself and the surviving helicopter crewmembers in place overnight.

After a night of beating back attacks by the Somalis, the group was able to extract itself with the help of a rescue convoy comprising U.S. 10th Mountain Division, Malaysian, and Pakistani forces. In the end, eighteen members of the task force were killed and eighty-four others were wounded; one Malaysian soldier was killed and ten were wounded; and two Pakistani soldiers were wounded. Estimates of Somali casualties range from three to five hundred dead and seven hundred wounded.[1]

U.S. forces have since fought significant battles in urban areas in Iraq and Afghanistan, reinforcing and adding to the lessons learned in Somalia regarding urban combat. These lessons should be adapted and applied to prepare for future multi-domain battles in megacities.

Note

[1] Casualty estimates vary; the data here is from *U.S. Forces, Somalia After Action Report and Historical Overview: The U.S. Army in Somalia, 1992–1994* (Washington, DC: U.S. Army Center for Military History, 200].

However, big data—the ability to collect, analyze, and correlate massive amounts of information in novel ways to produce useful insights—can provide a vital set of tools for joint task forces to understand the megacity environment.[24] For example, New York City's government established a data analytics task force in 2009 to determine how to use the city's massive stores of information to improve the effectiveness of city management. This task force collected and analyzed information ranging from tax records to rodent complaints in order to more efficiently address illegal housing practices and improve public safety.[25] The data this task force used already existed in a wide variety of city databases—it simply needed to be aggregated, correlated, and otherwise analyzed to produce useful insights. Similarly, in today's urban environment, a vast majority of individuals and institutions are connected via digital communications networks, providing a trove of data that allows a better understanding of the environment.

Just as New York City's analytic task force did, a U.S. military force operating in a megacity environment using big data can collect and analyze massive amounts of digital data generated daily. This still-nascent capability is referred to in the military intelligence community as computer network exploitation (CNE), and it can provide an essential tool to understand more fully the megacity sociopolitical and economic ecosystem. Currently, mobile broadband networks ("third generation" [3G] and above) reach 84 percent of the global population, and mobile broadband subscriptions are growing at double-digit rates in developing countries.[26] Because individuals utilize mobile broadband networks for a wide variety of activities—including texting, emailing, banking, reading the news, and interacting via social media—this data, when properly aggregated and scrutinized, can provide insights on everything from movement patterns to public opinion and to the functioning of illicit criminal networks.

With a significant portion of a megacity's population accessing the internet daily from a geolocatable mobile device, a joint task force with cyberspace superiority can collect and analyze a glut of data points to gain insights about the megacity environment and the system of systems operating within it.

In addition to the digital activity of individuals and human networks, the digital activity of city and national governments can help shape a detailed understanding of the megacity environment. Increasingly, governments around the world are providing services and information to their citizens via the internet. While the connectivity of individual governments varies around the world, all 193 United Nations member states have a degree of online presence.[27] In heavily networked megacities, where a greater portion of the population has access to the internet, it is reasonable to assume that government entities utilize digital networks to collect and process a significant amount of data. Government communications and databases will increasingly contain large amounts of information regarding law enforcement, public services, government finances, and public infrastructure. A joint force with cyberspace superiority can access and analyze this data, providing additional layers of understanding about the megacity and its inhabitants.

While CNE has the potential to provide an unprecedented level of understanding of the megacity environment, a joint task force must have cyberspace superiority to collect, analyze, and glean insights from this valuable resource. Collecting the required data from individual and institutional digital activity requires access to the majority of internet and cellular networks in the area of operations, as outlined in the previously proposed concept of cyberspace superiority. Additionally, much of the process of harvesting and analyzing big data is automated with already existing software tools capable of creating an automatic and persistent push of data to intelligence analysts.[28] This reliance on automation, along with the large data storage requirement, is unquestionably necessary due to the sheer volume of data to be collected and analyzed. However, the expansion of a joint task force's digital footprint and increased reliance on analytical software also increases its vulnerability to cyberattack from adversaries. Therefore, cyberspace superiority requires not only the ability to access digital communications networks but also to defend friendly networks against attacks and disruption.

While CNE is a valuable and necessary tool for understanding the complex megacity environment, a joint task force cannot harness this capability unless it has achieved cyberspace superiority first.

Shaping the Megacity Battlefield

Along with using cyber capabilities to better assess and to understand the complex megacity ecosystem, joint task forces will need to shape the megacity battlespace by utilizing cyberspace and electromagnetic

Second Lt. Stephanie Stanford, 90th Information Operations Squadron (IOS) cyber development lead, Staff Sgt. Aaron Wendel, 90th IOS cyber network technician, and Senior Airman Brett Tucker, 90th IOS cyber systems operator, perform cyber operations 1 August 2012 at Lackland Air Force Base, Texas. (Photo by Boyd Belcher, U.S. Air Force)

spectrum tools to create effects in the physical domains. These cyber and electromagnetic capabilities, when utilized to create effects on the battlefield, are termed nonlethal fires. The U.S. Army's emerging multi-domain battle concept embraces this idea, promoting the employment of "cross-domain capabilities" to create and exploit chronological "windows" of advantage.[29]

The multi-domain battle concept, however insightful, broad, overarching, and, applicable to a wide range of different operating environments, must nevertheless be adapted to the unique characteristics manifest in each. Consequently, as urban contingencies emerge, the multi-domain battle concept must be tailored to the megacity environment, which is unique in that it combines large spaces, complex and restrictive physical terrain, and dense human populations. One common feature that a megacity's characteristics give is the strong potential to deny and disrupt U.S. freedom of action in the physical domains of land, sea, and air. A megacity's physical and population characteristics stack the deck against U.S. ground forces from the outset. In such an anticipated environment, only in the cyberspace domain can the joint force enjoy freedom of action without the disruptions endemic to the physical obstacles characteristic of the megacity environment that impede movement. Therefore, cyberspace superiority provides the joint force with a potential means to shape the physical battlefield to their advantage using cyber tools as key enablers for actions in the physical domains, making attaining cyberspace superiority a prerequisite for conducting physical domain operations. For example, large areas filled with a complex maze of streets and buildings, densely crowded with civilians, will make land combat extremely difficult without cyber assistance. As illustrated in the Battle of Mogadishu, a crowded urban environment can significantly enable adversary forces to deny U.S. forces freedom of action.[30]

Because a megacity's physical and population characteristics puts U.S. ground forces at a great disadvantage from the outset, cyberspace superiority provides the joint force with a means to shape the physical battlefield to their advantage. To mitigate the physical environment in future megacity engagements, ground units will need to employ nonlethal fires along with cyberspace and electromagnetic spectrum intelligence collection to identify and create avenues of approach, identify targets, isolate objectives and key terrain, and disrupt enemy functions. Additionally, a joint force with cyberspace superiority operating in a megacity can shape the physical battlefield through nonlethal effects such as transmitting misleading messages to enemy leaders and fighters, locating concentrations of enemy troops, transmitting messages to the broader population, shutting down communications networks in an objective area, disrupting financial transactions and resupply operations among enemy networks, geolocating or shutting down enemy devices, shutting off electricity to an objective area, and directing host-nation security forces (either overtly or covertly), to name just a few.

> … ground units will need to employ nonlethal fires along with cyberspace and electromagnetic spectrum intelligence collection to identify and create avenues of approach, identify targets, isolate objectives and key terrain, and disrupt enemy functions.

Additional Challenges Related to Maritime Megacities

On considering the common problems related to dealing with urban warfare in megacities, it is important to note that a significant number of the world's megacities are located in crowded coastal areas, which creates additional operational challenges for a maritime force that it must overcome with cyber capabilities. For example, sea spaces surrounding megacities such as Mumbai and Lagos, Nigeria, are extremely congested with fishing vessels, container ships, and passenger ships, and are often home to illicit smuggling and piracy networks. Adversary forces can leverage this congested littoral environment to disrupt joint maritime operations in a variety of ways including clandestine surveillance and reconnaissance, electronic disruption of communications systems, obstruction of sea lines of operation, and armed resistance to amphibious operations. Consequently, just as land forces in a megacity can be quickly overwhelmed by swarming crowds and narrow streets, maritime forces can easily lose their freedom of action in a crowded littoral space where adversary forces are nearly impossible to identify and isolate.

The littoral area of a megacity presents nearly as many physical disruptions as the city's land area, and joint maritime forces must leverage freedom of action in the cyberspace domain to overcome obstacles and frictions in the physical maritime domain. In order to enjoy freedom of maneuver in this challenging coastal zone, maritime forces must employ nonlethal fires to achieve effects such as identifying adversary networks concealed in civilian marine traffic, manipulating or disrupting enemy communications, manipulating or disrupting enemy navigation systems, transmitting instructions or misleading messages to civilian vessels, and shutting down communications and electrical networks on shore in advance of an amphibious assault.

Air Operations Over Megacities

The nature of the megacity environment also enables adversary forces to bypass and disrupt U.S. airpower, making it necessary to apply nonlethal fires to employ effective aerial assets. No matter what degree of air superiority a joint task force enjoys over a megacity, the nature of the physical environment on the ground makes many air operations prohibitively difficult to execute. Tall, closely spaced buildings and narrow streets inhibit aerial reconnaissance and surveillance, and crowds and other collateral concerns constrain the employment of aerial fires, rendering air assets largely ineffective. Furthermore, the densely packed urban terrain provides ample cover and concealment for enemy air defense systems.

To overcome these challenges, joint forces with cyberspace superiority can employ nonlethal fires and cyberspace intelligence collection to disrupt enemy air defense targeting systems, geolocate and maintain custody of targets prior to engaging them, conduct electronic surveillance and reconnaissance from the air, conduct airborne manipulation or disruption of enemy communications, and many other actions that shape the physical battlespace in the megacity.

Conclusions and Recommendations

Demographics and global security trends make it likely that the U.S. military will find itself operating at some point in megacities, a distinct operating environment in which the United States has very limited experience. The unique physical characteristics of the megacity—vast spaces layered with complex urban terrain and massively dense populations—make it possible for adversaries to disrupt and deny U.S. forces' freedom of action on land, sea, and air.

In the megacity environment, cyber and electromagnetic spectrum capabilities will enable the joint force to understand and shape the physical battlespace across all three of these physical domains in the megacity. However, a joint task force cannot do this without cyberspace superiority. The joint force must have freedom of action in cyberspace in the megacity area of operations to effectively collect, analyze, and weaponize data and electronic signals. This makes cyberspace superiority a crucial operational prerequisite for military operations in a megacity, supplanting air superiority. To effectively employ this operating concept, however, the joint force must adjust its doctrine and organization.

Computer network exploitation has the potential to ensure that joint force commanders thoroughly understand the uniquely complex megacity environment. Technology companies are already harnessing big data similarly to understand the world and make businesses and governments more effective. However, for this capability to be successful, the U.S. military and broader intelligence community must be better postured to adopt the technological tools that the private sector continues to develop rapidly. The Department of Defense must significantly revise its innovation and information technology-acquisition policies, instituting a "technology push" acquisition model as well as the existing "demand pull" model.[31]

The U.S. Army Training and Doctrine Command appears to have fully grasped the ability of cyber and electromagnetic activities to understand and shape the physical battlespace, as evidenced by the development of the multi-domain battle concept. The broad concept of conducting actions in one domain to gain advantages in another is a natural modernization of traditional combined arms operations. Going forward, the entire joint force must understand and adopt this operating concept, with the air and maritime services revising and influencing the concept to ensure it is truly joint. More importantly, as multi-domain battle is written into future doctrine, joint force leadership must emphasize that this is a broad, overarching concept that must be appropriately tailored to fit specific operating environments.

In incorporating the multi-domain battle concept, joint doctrine must account for the challenges posed by fighting in a megacity. Future editions of JP 3-06 should contain a portion dedicated to the unique characteristics of megacities, the challenges they present in the physical domains, and options to defeat these challenges via the cyberspace domain. Future editions of joint operations publications must encourage cyberspace superiority as an operational prerequisite for megacity operations, rather than promoting air superiority as a universal precondition for operations in all environments.

Finally, given the growing ability of cyberspace and the electromagnetic spectrum to influence the physical domains, operational-level joint task forces should establish a joint force cyberspace component similar to the existing air, land, and maritime components. Currently, operations taking place in the cyberspace domain and across the electromagnetic spectrum fall under a variety of compartmented functions, organized differently across the military services. Service members from communications, signals intelligence, electronic warfare, information operations, and cyberwarfare specialties all operate and function in cyberspace and the electromagnetic spectrum. A joint cyberspace component with the requisite commander and staff will ensure that cyberspace and electromagnetic activities are synchronized and deconflicted across the task force's area of operations, as well as providing a crucial link between the task force and U.S. Cyber Command.

The U.S. Naval War College tested this concept in a 2014 war game and concluded that there is a valid requirement for a cyber component commander.[32] As this is still a nascent and undeveloped concept, the joint force must continue testing and refining the model of a joint cyberspace component.

Just as air superiority emerged as an operational prerequisite throughout the twentieth century, so too must cyberspace superiority emerge as such during the twenty-first century. Current joint doctrine and operational concepts acknowledge and account for the importance of the cyberspace domain. However, when the U.S. military is called upon to fight and win in a densely populated, heavily networked megacity, acknowledging the importance of cyberwarfare will not be enough—operational commanders striving to win the fight on the ground will need to win the digital fight first. ■

Notes

[1] United Nations (UN), "World Urbanization Prospects: The 2014 Revision, Highlights" (New York: UN Department of Economic and Social Affairs, 2014), 2, accessed 3 November 2017, https://esa.un.org/unpd/wup/publications/files/wup2014-highlights.pdf.

[2] Michelle Tan, "Army Chief: Soldiers Must Be Ready to Fight in 'Megacities,'" DefenseNews (website), 5 October 2016, accessed 3 November 2017, http://www.defensenews.com/articles/army-chief-soldiers-must-be-ready-to-fight-in-megacities.

[3] Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 10 February 2014), I-1.

[4] JP 3-06, *Joint Urban Operations* (Washington, DC: U.S. GPO, 20 November 2013), iii.

[5] Ibid., I-10–I-12.

[6] Central Intelligence Agency (CIA), "The World Fact Book: Somalia," CIA (website), last updated 19 October 2017, accessed 3 November 2017, https://www.cia.gov/library/publications/the-world-factbook/geos/so.html.

[7] JP 3-06, *Joint Urban Operations*, III-18, IV-27.

[8] Task Force Ranger was a joint special operations task force that deployed to Mogadishu, Somalia, in 1993. Their mission was to kill or capture tribal warlords who were interfering with the distribution of food aid to the starving population. On 3 October 1993, a mission to capture two top lieutenants of warlord Mohammed Farah Aidid went awry. Two helicopters were shot down and the ground force was swarmed by thousands of armed Somalis, as what was supposed to be an hour-long mission turned into an all-night battle for survival between ninety-nine elite U.S. soldiers and Aidid's militia. A partial account of this battle is available in Mark Bowden's book *Black Hawk Down: A Story of Modern War* (New York: Atlantic Monthly Press, 1999).

[9] David Kilcullen, *Out of the Mountains: The Coming of Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 62.

[10] Ibid.

[11] Marc Harris et al., "Megacities and the United States Army: Preparing for a Complex and Uncertain Future" (report, Washington, DC: Chief of Staff of the Army, Strategic Studies Group, 2014), 8, accessed 3 November 2017, https://www.army.mil/e2/c/downloads/351235.pdf.

[12] P. H. Liotta and James F. Miskel, *The Real Population Bomb: Megacities, Global Security, and the Map of the Future* (Dulles, VA: Potomac Books, 2012), 83.

[13] Ibid., 83–87.

[14] Ibid.

[15] JP 3-06, *Joint Urban Operations,* I-11.

[16] Kilcullen, *Out of the Mountains,* 116–25.

[17] JP 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 17 January 2017), III-28.

[18] JP 3-12(R), *Cyberspace Operations* (Washington, DC: U.S. GPO, 5 February 2013), GL-4.

[19] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York: Houghton Mifflin Harcourt, 2014), 44.

[20] Ibid.

[21] John Pollock, "People Power 2.0," *MIT Technology Review*, 20 April 2012, accessed 3 November 2017, https://www.technologyreview.com/s/427640/people-power-20/.

[22] John Scott-Railton, *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution,* Center on Irregular Warfare & Armed Groups (CIWAG) Case Study Series 2013 (Newport, RI: CIWAG, U.S. Naval War College, 2013), 50.

[23] JP 3-06, *Joint Urban Operations,* I-11.

[24] Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Force Quarterly* 79 (October 2015, 4th Quarter): 5, accessed 3 November 2017, http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/Article/621113/defense-intelligence-analysis-in-the-age-of-big-data/.

[25] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New York: Houghton Mifflin Harcourt, 2013), 186–88.

[26] International Telecommunications Union (ITU), *ICT [Information and Communication Technologies] Facts and Figures: 2016* (Geneva: ITU, 2016), 1, 4, accessed 3 November 2017, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf.

[27] UN, *United Nations E-Government Survey 2016: E-Government in Support of Sustainable Development* (New York: UN Department of Economic and Social Affairs, 2016), 5, accessed 3 November 2017, http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf.

[28] Symon and Tarapore, "Defense Intelligence Analysis in the Age of Big Data," 6.

[29] U.S. Army Capabilities Integration Center (ARCIC), "Multi-Domain Battle: Combined Arms for the 21st Century," ARCIC (website), accessed 3 November 2017, http://www.arcic.army.mil/App_Documents/Multi_Domain_Battle.pdf.

[30] Bowden, *Black Hawk Down*, 135.

[31] Symon and Tarapore, "Defense Intelligence Analysis in the Age of Big Data," 5.

[32] Don Marrin and Walter Berbrick, *U.S. Naval War College Global 2014: Game Report*, Navy Global War Game Series (Newport, RI: U.S. Naval War College War Gaming Department, 2015), 53, accessed 3 November 2017, http://www.dtic.mil/get-tr-doc/pdf?AD=AD1014472.