SMALL WARS JOURNAL

smallwarsjournal.com

Police Operational Art for a Five-Dimensional Operational Space

John P. Sullivan and Adam Elkus

The last fifteen years have yielded a rich literature on structural dimensions of modern-day tactics and operational art, particularly on the challenge posed by information age command and control (C2) technology, decentralized swarming, and irregular opponents. [1] The linguistic shift of "battleground" to "battlespace" recognizes the current reality of forces operating in a multidimensional battleground against complex opponents. [2] Similarly, many have recognized that in a rapidly urbanizing world, cities will be the main battlefields in fights between military/police units and "hybrid" opponents. "Global cities" such as New York, Tokyo, London, and Mumbai have become prime targets for terrorists, networked insurgents, and criminal organizations. Operations in global cities carry a special weight because of the strategic compression created by globalization, and pervasive communication networks—raising the significance of what would ordinarily be considered purely tactical counterterrorism operations.[3]

In our previous pieces "Postcard from Mumbai: Modern Urban Siege" and "Preventing Another Mumbai: Building a Police Operational Art" we've explored the operational level of police and counterterrorism response.[4] While military doctrine for operations is sophisticated and battle-tested, police operational doctrine has lagged behind. Counterterrorism response—situated in a complex operational space (opspace)—can now be considered as part of the operational level of maneuver, the midlevel point where strategic objectives are implemented on the theater level. [5] Genuinely *operational* doctrine for this unique form of engagement is underdeveloped, consisting of an ungainly mishmash of police, military, and emergency response tactical doctrine.

---

[1] See Frederick Kagan, *Finding the Target: The Transformation of American Military Policy*, San Francisco: Encounter Books, 2006, Antoine Bosquet, *The Scientific Way of Warfare*, New York: Columbia University Press, 2009, and Thomas K. Adams, *The Army after Next: The First Postindustrial Army*, Palo Alto: Stanford Security Studies, 2006 for intellectual histories of recent military thinking.

[2] See *Joint Publication 5-0: Joint Operation Planning*, Washington D.C.: US Department of Defense, 26 December 2006, p. 17.

[3] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three-Block War," *Marines Magazine*, January 1999. http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm

[4] See John P. Sullivan and Adam Elkus, "Postcard From Mumbai: Modern Urban Siege," *Small Wars Journal*, 16 February 2009, and John P. Sullivan and Adam Elkus, "Preventing Another Mumbai: Building a Police Operational Art," *USMA Countering Terrorism Center Sentinel*, June 2009, pp. 4-7.

[5] Lt Gen Sir John Kisely, "Thinking About the Operational level," *Royal United Services Journal*, December 2005, p. 38.

We propose a model for urban police operational art that has a five-dimensional view of the operational space, focusing in particular on the doctrinally neglected elements of cyberspace and temporality.[6] Our intention is to summarize and clarify a wide array of military thought, incorporating it into an operational framework for police operational response. In particular we will examine the military theories of Robert Bunker, Robert Leonhard, and William McRaven.

Understanding Cyberspace in Operations

Cyberspace is a contested—and critically misunderstood--element of the modern battlespace. The Department of Defense Dictionary of Military Terms holds that cyberspace is "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] However, many see it solely as a purely informational realm that we enter through the Internet. When we talk about cyberspace in the context of police and counterterrorism operations, we are not referring to the rather overused concept of "cyber warfare." Instead, we're talking about a wider definition of cyberspace that has bearing on command and control of operations.

The power of the Internet-oriented interpretation is not surprising, as science fiction writer William Gibson popularized the term "cyberspace" with his series of cyberpunk novels. [8] The Internet and "cyberspace" are now interchangeable in popular language, making the "humanspace" (or "meatspace" as Gibson called it) "real" world where guns fire and bombs go off. While cyberspace is certainly not the same thing as the physical world, it is contiguous with our day-to-day reality. Cyberspace permeates both the "real" and "virtual" worlds, and is thus both "everywhere and nowhere." [9] The Greek term *kyber*, (to "steer") from which the term "cyber" derives means steersman. The term "cyberspace" in this conception encompasses the "the idea of navigation through a space of electronic data, and of control which is achieved by manipulating those data."[10] As the Principia Cybernetica project argues, Gibson himself conceived cyberspace as a global computer network encompassing all people, machines, and sources of information. [11] In the introduction to his book *The Hacker Crackdown*, Bruce Sterling elaborates further on the nature of cyberspace:

> "Cyberspace is the `place` where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. The indefinite

[6] Five-dimensional battlespace or operational space (opspace) is introduced by Robert J. Bunker in his many works, op sit.

[7] http://www.dtic.mil/doctrine/jel/doddict/data/c/10160.html

[8] Martin Libicki discuses "Gibson warfare" his McNair paper "What Is Information Warfare?," Washington, D.C.: National Defense University, August 1995. http://www.ndu.edu/inss/books/Books%20-%201990%20to%201995/What_is_IW_Aug_95/a003cont.html

[9] John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, 8 February 1996. http://homes.eff.org/~barlow/Declaration-Final.html.

[10] "Cyberspace," Prinicipia Cyberntica Web, 17 October, 1994. http://pespmc1.vub.ac.be/CYBSPACE.html

[11] Principia Cybernetica.

> place out there, where the two of you, human beings, actually meet and communicate." [12]

The Cold War was dominated by the science of *cybernetics*, which conceived physical organisms, organizations, and even whole societies as self-regulating systems optimized according to the flow of information. [13] Cybernetics is fundamentally a science of control, as it seeks to uncover how information, broadly understood as feedback, regulates systems. In *Command Concepts*, Carl H. Builder, Steven C. Bankes, and Richard Nordin argue that the concept of "control" in command and control refers to a cybernetic loop of nodes whose interactions and exchange produce operational plans. [14] Many command and control systems are predicated on the idea of the organization as an information-processing system. Of course, this doesn't mean that the correct posture for the commander is to act as a simple information-processing node. As Builder notes that a successful "command concept" originates in the cognitive processes of the commander and regulates and prioritizes the minimum amount of information that must travel through the system. [15]

Within the military or police organization, cyberspace is the totality of the communication and interaction between fielded forces. Thus, a cyber attack means an attack that manipulates the "data" that is exchanged in the process of communication. This understanding of cyberspace is in accordance with the holistic systems perspective recommended by the Army's *Commander's Appreciation and Campaign Design* pamphlet. [16] Cyber attacks are directed towards disrupting instruments of control—whether those are specific communication systems or the human mind. A cyber attack does not have to originate from a computer—it could be a bomb placed in a commander's barracks or an accumulated process of a series of swarming attacks destroying an opponent's C2 ability to function in the battlespace. Overarching opposing force C2 nodes are coordinated through cyberspace, as demonstrated during the Mumbai attacks.

This is not an endorsement of controversial "effects-based" operational theory. The commander rarely has enough information to determine the nature of the "effects" applied to a system, as human complex systems are not purely mechanical. They are complex adaptive systems that are very sensitive to initial conditions—and their course of future evolution cannot be scientifically predicted. [17] This is why Effects-Based Operations (EBO), a method of operational art derived from systems thinking, is widely acknowledged to have failed against Hezbollah in Lebanon. [18] Nevertheless, organizations do comprise systems between which information is spread in the form of interaction between nodes and messages sent up and down the chain.

---

[12] Bruce Sterling, *The Hacker Crackdown*: *Law and Disorder on the Electronic Frontier*, New York: Bantam, 1993. p. xii.
[13] See Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, Chicago: University of Chicago Press, 2006.
[14] Carl H. Builder, Steven C. Bankes, and Richard Nordin, *Command Concepts: A Theory Derived from the Practice of Command and Control*, Santa Monica: RAND Corporation. p. 10.
[15] Builder *et all*, p. xiv.
[16] The United States Army Commander's Appreciation and Campaign Design, TRADOC Pamphlet 525-5-500, 28 January 2008, p. 5.
[17] Major Ketti Davison, "From Tactical Planning to Operational Design," *Military Review*, September-October 2008, p. 33.
[18] See James N. Mattis, "USJFCOM Commander's Guidance for Effects-based Operations," *Parameters*, Autumn 2008, pp. 18-25.

We must also point out that the understanding of cyberspace we outlined also acknowledges the importance of the infosphere, the layer of communications that the global media comprises. [19] When many people write about cyberspace, they are thinking about the infosphere. Information effects have substantial effects on battlespace shaping, information operations, and can give tactical events strategic significance. Cyberspace comprises a part of the infosphere, but cyberspace is more of a limited and technical area whereas the infosphere by definition comprises the totality of media. [20]

As military theorist Robert J. Bunker points out, terrorist hide in a "virtual" domain that adversaries cannot reach, utilizing organic camouflage, sympathetic social spaces, or aspects of cyberspace to mask their activities until the last moment. [21] While this sounds exotic, insurgent camouflage could be something as simple as a sniper's cover in an abandoned building, an underground tunnel, or a crowd of civilians protesting in an urban center. Cyberspace is a form of camouflage, as the distributed online jihadist network in the infosphere demonstrates. While they ordinarily cannot be targeted from these areas, insurgents can fire from them. As stealth technology and advanced camouflage in First World states continues to develop, it is inevitable that it will also trickle down to insurgents.

In turn, Bunker notes, conventional forces use "data fusion" to rapidly reach hidden targets and neutralize them. [22] The adaptive information processing Bunker describes isn't necessarily technological in scope—it ranges from a technical countersniper system that pinpoints the exact location of the shot to sociological information gained through intelligence work that allows an Army patrol to locate and ambush a crew of insurgents laying Improvised Explosive Devices (IEDs) on a street corner. In the context of irregular warfare, the technological race is not necessarily as important as the social dimension of operations. IED planters and counter-IED systems will engage in a rat race to out-innovate each other. But by targeting the social networks that support IED-planting operations, the Army made the technical contest largely irrelevant.

When coordinating large-scale counterterrorism operations in urban environments, command and control often fractalizes because of the complexity of the physical terrain, the presence of the media, and the chaotic and individualized nature of the battlespace. The commander uses cyberspace to visualize his forces in a single point of space and organize and coordinate their efforts through visualization technologies, tactical radio, and other command and control systems. As previously mentioned, the commander's concept of future operations—the command concept—informs the resources allocated and the actions of subordinates, giving them the autonomy to carry out their duties and avoiding the trap of becoming a prisoner of his own cybernetic array of C2 nodes. [23]

---

[19] John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica: RAND, 1999, p. 18.
[20] Arquilla and Ronfeldt, p. 11.
[21] Robert J. Bunker, "Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI," *Parameters*, Autumn 1996. http://www.carlisle.army.mil/USAWC/PARAMETERS/96autumn/bunker.htm
[22] Ibid.
[23] Builder et al, p. 13.

To summarize, the cyber dimension of the battle space consists of the infosphere, organic and cyber forms of camouflage, the cyber element of deployed forces, critical electromagnetic infrastructure in the battlespace, and C2 networks. The cyber element of deployed forces consists of command and control (C2), communications, the flow of information within the organization, and the distributed computational intelligence of the force itself.

What does this mean in a typical tactical setup? Sid Heal, a retired commander in the Los Angeles Sheriff's Department and a tactical theorist sketched out the implications in his essay "Fighting in the Fifth Dimension." [24] First, any commander who expects only to fight in "humanspace" will be targeted from cyberspace. Second, sensing rather than firepower will be the key to victory. Detecting combatants in order to strike them becomes paramount, utilizing both technological and social sensors. Developing networks of human sensors is often the best means of preventing attack. Third, rules of engagement become more interlinked with issues of privacy and civil rights. Collecting both technological and social data will inevitably raise questions about rights-security tradeoffs. Fourth, sorting relevant data from noise will comprise the chief barrier to targeting hidden opposing force units. Lastly, complex situations are going to require that the commander reach across cyberspace (and geography) to utilize cross-organizational and civilian expertise needed to accomplish the goal.

Understanding Temporality and Surprise

Sustained study of operational theory shows that time is in fact a contested zone of the operational space. Opponents contest time in the same way they fight over a crucial piece of terrain. Most understand time as the general timeline, the event horizon on which opposing forces place their assets in time and space. While the linear timeline is undoubtedly one element of the temporal dimension, it ignores the fact that different sides of the engagement perceive time in vastly different ways. The divergence between Blue Force and Red Force's perception of the engagement guides operational planning, shaping their respective approaches to the central clash of forces. There are two dominant perspectives on time as an element of tactical warfare: Robert Leonhard's writings on surprise and William McRaven's theory of special operations direct action.

Robert Leonhard argues that the issue of readiness makes time is the controlling element of war. Forces are perpetually unready because they cannot always remain in a state of alert and full combat readiness. Because unready forces cannot respond at their full combat strength, opposing forces seek to strike them before they can position themselves to defend. In turn, the defender will attempt to quickly detect attacking adversaries in order to destroy them. The opposing force planning the attack will attempt to create surprise (which is simply a delayed detection of attack) by *slowing down* the adversary's detection through stealth, surprise, operational security, or deception. In turn, the defending commander will try to *hasten contact* to deny the attacking force the advantage of surprise at the point of unreadiness. [25]

[24] Sid Heal, "Fighting in the Fifth Dimension," *US Cavalry on Point*. (Date Unavailable) http://www.uscav.com/uscavonpoint/Feature.aspx?id=45

[25] See Robert Leonhard, "Surprise," at http://www.jhuapl.edu/areas/warfare/papers/surprise.pdf

Leonhard's theory of surprise was written during the era of maneuver warfare, which principally concerned itself with conventional force-on-force contests. However, it has great applicability to today's "hybrid" contests. What is most crucial to Leonhard's concept of temporal battle is his emphasis on readiness. Garrison societies can place their forces on 24-hour alert, but this still does not obviate the human need for rest, dispersion, and recovery. Only the *Terminator* robots stand perpetually alert and ready to battle. [26] The most important element of time for Leonhard is the amount of time it takes for a force to *detect* an approaching attacker, which in turn determines its ability to fight off the attacker.

William McRaven advances a complementary theory that explains how some foes attack without the benefit of general surprise. In special operations warfare operations have succeeded in spite of a lack of general surprise through the concept of relative superiority. This does not mean that surprise isn't important—rather it means catching the enemy off guard as opposed to unprepared. [27] What this semantic difference means is that targeting weaknesses and points of slackness should be valued above all else. As in Leonhard, the point is not to completely escape detection (which is impossible) but slow down detection in order to prolong your advantage. Relative superiority is the pivotal point in an engagement when the attackers have the advantage over defenders. [28]

Ideally, relative superiority is achieved early on. To do so, the operators must quickly pass through the point of vulnerability (defined as the point in the mission when the force reaches the opposing force's first line of defense). At this point the frictions of war (chance, uncertainty, the will of the opponent) have the opportunity to scuttle the mission). The longer it takes to achieve relative superiority, the greater havoc these frictions wreak on the attacker. [29] For McRaven, who undoubtedly writes from the point of view of the attacker, the most important factor is the time it takes for the special operations operator to reach the point of advantage. Time is constructed as a linear chart that shows the crossover from vulnerability to operational superiority. The operator has to get to the objective as fast as possible, as any delay widens the vulnerability window. [30]

What both Leonhard and McRaven suggest is that the attacker and defender both perceive time differently. This is especially true in contests between terrorists and other irregulars and counterterrorist/counterinsurgent groups. In counterterrorism and modern irregular warfare the adversary starts out in a state of dispersal and unreadiness to attack. He is "cloaked" beyond what Bunker calls "humansensing" by various forms of camouflage, be it organic camouflage, technology, the vastness of the modern city, or the support of a segment of the population. In order to strike, the defender takes a series of steps that makes him vulnerable to detection. The act of "uncloaking" and building up the assemblage of the "kill chain" to strike is slow and is the terrorist's chief window of vulnerability.[31]

---

[26] One might argue that even Terminators need a break, hence Arnold Schwarzenegger's famous saying "I'll be back."
[27] William McRaven, *Case Studies in Special Operations Warfare: Theory and Practice*, New York: Ballantine Books, pp. 16-17.
[28] McRaven, p. 4.
[29] McRaven, pp. 6-7.
[30] McRaven, p. 19.
[31] Sullivan has termed this window of vulnerability the "I&W Envelope" in his many works on Intelligence Preparation for Operations (IPO); see especially John P. Sullivan and Alain Bauer (Eds.), *Terrorism Early Warning:*

While formless, he has the advantage of being unseen. But he must trade his safety away for mass in order to create combat power. Time factors into his calculation of relative superiority—he has to find the right moment to strike and must minimize the period of vulnerability while he conducts pre-operational surveillance and puts the elements of the attack together. Once he has achieved relative superiority, he can kill as many as he chooses with little blowback. Time is *slow* for him because he can choose the point of attack. During the attack itself, however, he *speeds up* in order to create relative superiority and operational shock.

The defender is usually unaware of the specific nature of the plot. If he is doing dignitary protection or protecting a mass event, he has deployed assets on the field but suffers from an information asymmetry. He is also completely visible to the attacker. However, his command of resources ensures that he can act quickly to crush an attack provided he has the correct information and his command and control (C2) and capabilities enable him to rapidly swarm forces. He must defeat the adversary before he attains relative superiority. It is preferable to prevent the attack before it happens, but once an attack is in progress it can be stopped through rapid response. Time is *fast* for the defender because he has to quickly move to neutralize the attacker before the attacker can attain relative advantage. Otherwise, the attacker accomplishes the mission and the defender's C2 and ability to counterattack withers.

For the Blue Force commander, an intuitive notion of timing is an essential component of negotiating and influencing a complex operational setting. Timing is critical to achieving mass, selecting an opportune time to maneuver, and leveraging surprise to engage an adversary. Time is thus a significant dimension for operations. It can be exploited by both sides and is critical at all levels of engagements: tactical, operational, and strategic. Indeed, time is an integral element of all political and consequently terrorist and warfighting endeavors.

Synchronizing operations in largely dependent open the selection of optimal timing for engagement, maneuver, or counterforce operations. Intelligence is frequently geared toward understanding time. When will a group or element attack, what is the optimal timing for an operation to influence the strategic and political calculus? Indications and warning are frequently pegged to time. Understanding a terrorist "kill chain" or an event horizon is largely dependent upon discerning a phase of operations by observing key transactions and signatures. Selecting alternative courses of action to counter an attack or craft a response is also time dependent. An operational commander (and his or her staff) seeks to identify tripwires or decision points for selecting options. In this sense, time interacts with speed in forming a basis for successfully negotiating a decision cycle. [32]

The addition of the cyber-dimension interacts with time in a special way. The choice to act, the choice to temporally modulate (speed or slow) pulses in a swarming operation, the timing of convergence of physical and cyber attacks all demonstrate that time is the key to unlocking cyber potentials. The infosphere element can be used to leverage the impact of time, by allowing a

---

10 Years of Achievement in Fighting Terrorism and Crime, Los Angeles: Los Angeles County Sheriff's Department, October 2008, pp. 147-150.

[32] John Boyd's Observe-Orient-Decide-Act (OODA) loop is a crucial element of timing and response.

message, meme, or information operation to resonate. Likewise, a maneuver operation that rapidly targets a point of weakness to target C2 or use speed to overextend an opponent's C2 is leveraging cyberspace.

Cyber attacks create a temporal advantage for the attacker. A cyber attack targeting a command and control (C2) system creates a singular weakness in time and space that is quickly exploited in the operation itself. For example, in the Mumbai attack, the accumulated collapse of C2 functions through swarming created a critical weakness in the Indian command network. Propaganda and forms of societal warfare or dislocation otherwise known as battlespace shaping put up social, political, or physical obstacles to the defender's ability to counter attacks. If no one in the population is willing to help the defender or actively assists the terrorist or insurgent, then the response to the attack is critically weakened. Likewise, if the attackers lack popular support and cannot utilize camouflage it causes them to speed up their planning and target acquisition process and take unnecessary risks.

To summarize, the temporal dimension of the operations/battlespace consists of the general timeline (the event horizon), the moment of relative superiority, and the respective perceptions of time by the defender and attacker. The general timeline is the event horizon on which opposing forces place their assets in time and space. The moment of relative superiority is the moment in which the attacker gains a pivotal advantage over the opponent that allows him or her to complete the operation. The defender perceives time as a fast process because he must quickly response and/or detect the adversary. The attacker perceives time as slow because he can choose a target at his leisure. However, one the choice has been made the attacker must gradually speed up as he or she assembles his forces in time and space for attack.

Conclusion: A Framework for Operational Art

The implications of both cyber and temporal dimensions for operational framework may appear intuitive or commonsensical, but are not well stated in doctrine. The irregular battle is essentially a struggle situated around targeting. The attacker, situated within organic or inorganic cover, must attack before he is pinpointed by the defender and neutralized. The defender hastens contact to target and neutralize the attacker before he can assemble his weapon and employ it in the operational space. If the battle is essentially a targeting duel, then police and counterterrorism operational forces must devote the most doctrinal space and research and development time to coming up with means of speeding up data fusion and making it more comprehensive.

Improving data fusion and detecting is not merely a matter of inventing more technological tools, which only have an impact on the technical level of engagement. Rather, improving data fusion results from the harmonization of tactical level information-dispensing through both technological and command tools and higher-level strategic foresight and intelligence. The Intelligence Preparation for Operations (IPO) process and the Terrorism Early Warning (TEW) concept acts as a kind of bridge between tactical and operational levels of engagement, creating a networked intelligence system.[33] IPO, a civilian analog to the military planning system

[33] See John P. Sullivan and Alain Bauer (Eds,), *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime*, Los Angeles: Los Angeles County Sheriff's Department, 2008, available at http://www.lasd.org/tew/TEW2009.pdf for a comprehensive history and doctrinal template of the LA TEW.

Intelligence Preparation of the Battlespace (IPB), generates operational plans and defines the parameters of engagement. The TEW is an engine for networked intelligence and meta-analysis among regions at the operational level.

However, the increasing complexity of engagement points to the necessity of strategic forecasting and futurism. Although the military employs countless analysts engaged in strategic forecasting and futurism, operational level counterterrorism limits thought about future operations to wargaming and strategic forecasting of near-term threats. Futurist workshops and long-range studies devoted to long-term trends in the evolution of the operations/battlespace, technological and geosocial change, and the capabilities of opponents are necessary in order to guide future operations planning. Without being cognizant of the future evolution of the operations/battlespace, counterterrorism professionals will continue to be caught flat-footed by opponents who must adapt in order to survive—and thus will extensively study new military theory and developments. [34]

Likewise, C2 capabilities have to measure up to the challenge of modern operations. Recent operations like Mumbai have shown that current counterterrorism response doctrine is overwhelmingly tactically focused and is not up to the task of facing down a complex attack that can attack from multiple directions, with multiple elements. Dealing with this has both cognitive and doctrinal implications. Carl H. Builder's idea of the "command concept" holds that effective command and control is rooted not in information tools but in the cognitive processes of the leader. A well formed "command concept" of future operations intuitively guides choices about the minimum of information that should flow through command and control systems. [35] Although it is mediated through machines, this concept *necessarily originates* in human cognitive processes. Command concepts for operations can help organizations deal with cyber attacks--technical strikes from command and control warfare, psychological warfare and deception, disruption strikes, and simultaneous attacks designed to overload C2 networks and software. On the doctrinal end, forces must be trained to operate in a fluid environment with multiple levels of engagement. This requires written doctrinal concepts for operations that can be standardized and institutionalized into free-play wargaming exercises.

The elements of the temporal dimension sketched out in preceding sections also have implications for warning and response. By understanding surprise as merely the delayed detection of attack—and something that can occur in even the most fortified of environments, we can move away from a static and rote concept of force protection that sees layers of fortifications and personnel as the best means of preventing attack. As Leonhard argues, no force can remain at full battle rattle in perpetuity, and openings for attack occur as a result of this entirely human weakness. Rather, speeding up detection of approaching attack is more a matter of creating layered sensing networks—both human and technological—integrated closely with operational response.

[34] See "Bin Laden Lieutenant Admits to September 11 and Explains Al-Qa'ida's Combat Doctrine," Middle East Media Research Institute, Special Dispatch No. 344, February 10, 2002. http://www.memri.org/bin/articles.cgi?Area=sd&ID=SP34402
[35] Builder *et all*, p. xiv.

As previously noted, societal warfare and operations/battlespace shaping also has a long-range impact on the temporal dimension of operations. An opponent supported by the populace or able to shape the parameters of the operations space to his will can choose an attack with leisure. It takes longer for the defender to detect him, and response is also greatly complicated by lack of information. If police and military forces, through adaptive intelligence networks, human and technological sensors, and the support of the populace, have shaped the operations/battlespace in a manner that gives them the advantage, the opponent operates in fear of being apprehended and makes quick and hasty decisions.

A focus on understanding cyberspace in its original meaning and incorporating time as a dimension of operations may seem pedantic or perhaps overly academic. But understanding cyber and temporal dimensions of operations means synthesizing a mixture of old and new ideas to gain a better understanding of the modern operational space—and is crucial to dealing with opposing force and environmental challenges.

John P. Sullivan is a career police officer. He currently serves as a lieutenant with the Los Angeles Sheriff's Department where he is assigned to the Emergency Operations Bureau. He is also a Senior Research Fellow at the Center for Advanced Studies on Terrorism (CAST). His research focuses on counterinsurgency, intelligence, terrorism, transnational gangs, and urban operations. He is co-editor Countering Terrorism and WMD: Creating a Global Counterterrorism Network (Routledge, 2006).

Adam Elkus is an analyst specializing in foreign policy and security. He is currently Associate Editor at Red Team Journal. His articles have been published in Red Team Journal, Small Wars Journal and other publications. Mr. Elkus blogs at Rethinking Security, Dreaming 5GW, and the Huffington Post. He is currently a contributor to the Center for Threat Awareness' ThreatsWatch project.