Any Time, Every Place

The Networked Societies of War Fighters in a Battlespace of Flows

Maj Dave Blair, USAF

> *In a world of networks, the ability to exercise control over others depends on . . . the ability to constitute network(s), and . . . the ability to connect and ensure the cooperation of different networks . . . while fending off competition from other networks.*
>
> —Prof. Manuel Castells, *Communications Power*

> *It takes a network to defeat a network.*
>
> —Prof. John Arquilla and Gen Stanley McChrystal

In a hypothetical retelling of any of 100 recent battlefield encounters, two networks coalesce around a compound of buildings at the western border of a nation at war with itself. On one side, a disparate assemblage of fighters drawn from the Middle East, North Africa, Europe, and Asia attempts to enter a country at war using an amalgam of ancient trade routes and modern commercial navigational and communications technology. Their stories are as diverse as their backgrounds—for one, an Internet web magazine

linked them to a religious leader they once knew personally; for another, they come to avenge a brother or an uncle; a third comes for the prospect of adventure, as advertised by other fighters on streaming video. In a previous war, fighters might have brought with them their preferred printed propaganda piece, perhaps even a signed copy. In this war, those authors are very much present and part of the conversation, linked to their progeny by way of e-mail and voice over Internet protocol. The financiers are just as present, relationally linked to the real-time consequences of their donations.

This force exists in many spaces at once; it is anchored in relational space but flexible in physical space. The flexibility allows it to coalesce at a time and place of its choosing, achieve fleeting objectives, and disperse before an enemy can respond. This strategy works remarkably well against a conventional adversary, bound by physical areas of operation and beholden to fixed-response timelines.[1]

This force's opposite number is strikingly similar in this regard: a diverse network of special operators, aircrews, and intelligence professionals, bound together by a mix of trust networks and modern communications technology, has been hunting this cell for some time now. One such team—a special operator working from a tactical headquarters, an MQ-1 aircrew in Nevada, a Liberty MC-12 crew, and a team of analysts in at least two places in the continental United States—locates and tracks this cell along a transit route. Upon finding their quarry, helicopters full of operators, fixed-wing gunships, high-speed fighters, and sundry support aircraft press toward the cell before it can flee. Once they are established on scene, the target location provides a focal point for the operation, but the trust networks between operators continue to give the teams the nimbleness necessary to pursue the objective. These trust networks have been built over years through a combination of shared combat experience, in-person exercises, and weekly teleconferences. All of these places and times are invoked at once "on the op."

This is a battle of small margins in brief windows. Victory goes to the side that can fix its opponent in a physical place while retaining the flexibility to bring its own forces to bear across physical space. In this case, it belongs to the special operations team members who can call upon forces from across 10,000 miles and bring them into this place. The terror cell, fixed in place and decoupled from its larger networks, cannot. The special operations team remains in a "space of flows" while the terror cell is trapped in a "space of places."

Castells and the Space of Flows

In his seminal trilogy *The Information Age: Economy, Society, and Culture*, sociologist Manuel Castells describes changes wrought by increasing global connectivity in the way societies perceive the intersection of social space, physical location, and relational networks. He defines space as "the material support of time-sharing social practices."[2] People must be somewhere to be together. In their seminal work on information theory, Claude Shannon and Warren Weaver similarly identify a technologically facilitated layer of communications.[3] Whether through the formal technology of electronic transmission or the social technology of language, societies construct (and are constructed by) shared spaces between people. This article argues that a battlespace is very much a "space" by Castells's definition.

Castells describes two formulations of social space: societies can be organized around physical location, in a space of places, or around relational networks, in a space of flows.[4] The space of places, the traditional mode of social organization, remains the dominant mode. According to Castells, "A place is a locale whose form, function and meaning are self-contained within the boundaries of physical continuity."[5] For instance, decades ago, a physical building might supply a social focal point for organizing the relationships of a company.[6] In this space, flows are contained and summarized by physical geography. Incremental and territorial approaches to combat are captured well by this space of places, a fact demonstrated by both the classic command to "take that hill" and the ubiquitous idea of the combat zone.

In contrast, a space of flows is an abstract space built around social networks; accordingly, it is less bound to physical space and linear time. In Castells's words, "*The space of flows is the material organization of time-sharing social practices that work through* . . . purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in the economic, political, and symbolic structures of society" (emphasis in original).[7] As a practical example, the discussion concerning a Facebook post relaxes the constraints of space and time that a normal conference would demand. A user can interact with a group of people not only without regard to distance but also without regard to time. A post takes virtually no time to update but persists long enough for one to interact with it hours or even days later. In a space of places, distance translates into time via physical transportation media; in a space of flows, distance and time are essentially unlinked due to the near-instant speed of global communications.

This is not to say that physical presence is unimportant in a place of flows. Quoting Gen James Jones and a host of others, "Virtual presence is actual absence."[8] In contemporary "coder" culture, relational network flows organize physical space. Relationships are embedded in semipermanent sociotechnical patterns such as e-mail lists and websites, and these relational networks coalesce into physical spaces.[9] These networks do not diminish the need for interaction in physical places, but the need for a *specific* physical space becomes less important in this world. For instance, coder meet-up groups are structured in virtual space but gather in a variety of physical spaces to reinforce social relationships and accomplish tasks.[10] In a space of flows, physical meetings primarily grow out of relational networks rather than relational networks primarily emerging from physical structure.

We might envision this difference by imagining different modes of interaction between the alumni of a given school. A class reunion that calls members back to the physical college for a homecoming weekend embodies place-based logic. Conversely, monthly happy-hour meet-ups among alumni in a given city grow from flow-based logic, especially if the meetings are arranged through a static online forum.

Flow-based logics increasingly complement, and in some cases supplant, the place-based logics in the business world. Telework has become an option for inclement weather days or as a means of minimizing time wasted during commuting. Increased use of inexpensive and convenient video teleconferencing mitigates some of the concomitant loss of face-to-face interaction. Improved remote desktop capabilities and increasingly accessible security technology allow businesses to maintain enterprise integrity from across diverse locations. Outsourcing and crowdsourcing transfers

repetitive tasks to cheaper milieus via communications technology. Some technology startups so fully embrace these concepts that they forgo owning physical space entirely, creating a market for rentable "incubator" space.[11] These same changes map onto emerging trends in warfare.

The Battlespace of Flows

The thesis of this article is straightforward: by means of networking technologies, warfare is increasingly becoming a space of flows. It holds that the flow-based logics that sparked these changes in the business world have initiated similar alterations in the world of armed conflict. Just as telework enhances the modern business space, so do the special operators physically present in the modern battlespace work alongside remote operators. Traditionally, we've seen "reachback" support based in the continental United States for deployed war fighters in the form of intelligence products or technical support, but this is something different. As opposed to traditional off-site support, which assists the decisions and actions of others, these remote operators take action and make determinations themselves that decide outcomes—their choices directly shape the battlespace. In an even more extreme form of flow-based warfare, cyberspace operators do not commit to a physical battlespace at all, except perhaps in their endgame. Even if software could generate physical effects, it would do so ad hoc, without any means or intent to hold that physical space.

Flow-based warfare is a form of fighting that can transcend physicality. The potential for physical effects without being physically proximate enables flow-based warfare to bypass boundaries. For instance, cyber warfare can access locations that would be prohibitively costly or politically difficult to reach through traditional physical force. Just as call centers allow companies to outsource algorithmic tasks, so do data links and satellites allow American commanders to generate persistent surveillance via remote aircraft from the location with the lowest manpower-deployment cost—the United States.

In a place-based world, only a state with fixed-location factories could churn out the tools of modern war. This fact provided the accountability necessary for making the Westphalian system work—a tank came from a factory somewhere, and that factory had a flag attached to it. As spaces of flows democratize information production in the business world (and, potentially, physical production with the advent of additive manufacturing or 3-D printing), they democratize the production of violence in war fighting.[12] For both al-Qaeda and the United States government, flow-based warfare enabled coordinated violent action from network members in sundry locations. Since these flows are more complex than physical place, an organization must be able to think, coordinate, and act on a more abstract level to make use of them. Small organizations tend to be nimbler in dealing with complex problems since they make better use of tacit knowledge and need not reduce a problem to coordinate a solution.[13] Therefore, flow-based warfare likely will be adopted more rapidly and eagerly by small organizations with strong trust networks and less so by industrial, bureaucratic forms.[14]

This article proceeds with a plausibility probe of this thesis, using three cases from the past decade. First, it traces the reciprocal adoption of flow-based logics by al-Qaeda and the US special operations community. Second, it explores the extreme case of the MQ-1 Predator's remote split operations (RSO) concept. Finally, it evaluates the effects of a mature form of flow-based warfare against a place-based adversary through the battlefield use of social media by the Free Libyan Army in 2011.

The article claims that flow-based warfare became a structural feature of the conflicts of the last decade. However, it does not claim that flow-based warfare has become more important than place-based warfare. Scoping the claim in this way diminishes the potential threat of selection bias. By establishing its presence and significance in the defining conflicts of that decade, the article demonstrates this claim. Additionally, since the special operations forces (SOF) case and the related Predator case both involve organizational learning and change toward flow-based warfare, they inherently include both negative and positive valences of our dependent variable. The article seeks to establish the heuristic utility of Castells's concept of flows for describing certain recent changes in warfare. A follow-on research design that pays more attention to these negative cases might trace the contours of flow-based versus place-based conceptions of the battlespace over time.

Special Operations Forces versus al-Qaeda: The Adoption of Flow-Based Warfare

Flow-based warfare offers an excellent tool for an asymmetric adversary to attack a vastly superior place-based opponent. In a space of flows, the production of violence can be democratized in the same way that the production of information shifted from centralized news sources to social aggregation. Command and control can similarly be democratized. In a place-based system, one commander might have a radio channel for a given area—this structure lends itself toward centralized control and vertical command links. A modern war fighter has myriad means of communications that can potentially support communications with vast numbers of peer units—such technologies allow for lateral flat and ad hoc command structures. These flow-based structures can take form in a space, execute their mission so long as they retain relative advantage, and then disperse before a place-based adversary can marshal forces to respond.[15]

Moreover, a flat-networked insurgent group should find these sorts of logics easier to implement than a hierarchical, compartmentalized military.[16] For this reason, illicit actors and terror groups were early adopters of flow-based war fighting.[17] Al-Qaeda's financial and recruiting networks cut across a number of different places. An amalgam of Chechens, Arabs, and Afghans constituted their forces in Afghanistan.[18] Their money was infused through global financial systems from a variety of "donors" and was often conveyed through the technologically facilitated trust networks of *hawala*.[19] Al-Qaeda itself might have been described as a space of flows rather than a space of places.

The Iraqi improvised explosive device (IED) network provided a clear expression of this space of flows. Financiers outside the country would pump resources into

that system from sundry locations; engineers inside and outside the "combat zone" would counter coalition countermeasures with new designs; in-country bomb makers would assemble these designs; finally, the network would contract with local nationals to emplace these weapons.[20] This network took ground only in the very last step, when it emplaced the weapon itself; the network held that ground only as long as it took to strike and then fell back to the space of flows. Place-based conventional forces had tremendous difficulty matching this flexibility. Although the flows-based network could not directly control ground, it could make the use of that ground extremely costly to its adversary.[21]

Early moves against this network remained locked in place-based logics. By adding armor and jammers to ground logistics vehicles, coalition forces became better prepared for their physical intersection of the IED network. Similarly, by increasing aerial patrols for IED emplacers, they sought to deny the physical lines of communications to their adversary. Unfortunately, these were both losing bets with terrible exchange ratios—the IED network could export most of its risk upstream to the space of flows, where it could not be targeted through these means. Moreover, the fact that the flow-based network could attack anywhere and at any time forced the place-based conventional forces to commit everywhere at all times. One IED design change could force an order-of-magnitude costlier response in armor, jammers, and patrols.[22] For this reason, an Army brigadier general concluded that "you can't armor your way out of this problem."[23]

The alternative was a move toward flow-based warfare. According to a 2007 *Washington Post* article,

> Ultimately, eliminating IEDs as a weapon of strategic influence—the U.S. government's explicit ambition—is likely to depend on neutralizing the networks that buy, build and disseminate bombs. Military strategists have acknowledged that reality almost since the beginning of the long war, but only in the past year has it become an overarching counter-IED policy. Left of boom—the concept of disrupting the bomb chain long before detonation—is finally more than a slogan. If you don't go after the network, you're never going to stop these guys. Never. They'll just keep killing people, the senior Pentagon official said. And the network is not a single monolithic organization, but rather a loosely knotted web of networks.[24]

Small teams with flat cultures and strong trust networks, empowered with rapid logistics and robust communications, could become the "network to defeat a network."[25] This network emerged gradually from the seedbed of elite SOF teams during the early 2000s. These teams already had strong reputations as well as habitual relationships with members of the interagency process and the intelligence community. Thus, they provided an excellent substrate for the growth of a flow-based network.

The latter took shape, in part, through an expanding group of liaison officers, sent both from and to these teams. These liaisons offered transgeographic and transinstitutional access for these teams. They also created alternative coordination pathways for the interagency process, using the trust networks of the SOF teams as a routing hub, thereby increasing the social power of the teams within that process.[26] Over time, the alumni of the liaison group advanced within their own organizations, further enhancing the access of this network.

The network used this structure to implement a flow-based targeting cycle, which grew both more expansive and quicker throughout the campaign. This find,

fix, finish, exploit, analyze, and disseminate cycle allowed coalition SOF teams to pin their adversary network while retaining their own flexibility.[27] The "fix" stage of this cycle invokes the idea of flow most clearly since it attempted to deny flow to the IED network by anchoring and holding its nodes in physical space.[28] Over the course of the campaign, the growth of this cycle shifted the balance of networks in favor of the coalition and helped dislodge al-Qaeda-backed IED networks from Baghdad.

Although the "finish" stage of this cycle was both the most valiant and celebrated, the "fix" stage was often the limiting factor. To carry out an operation, surveillance assets would have to locate and track individuals from an adversary network until a strike force could take action against them. To keep an "unblinking eye" on these targets from identification to action, this network needed heretofore-impossible amounts of low-grade but long-dwell intelligence, surveillance, and reconnaissance time.[29]

Enter the Predator's RSO concept, which uses sociotechnical flow to enable crews in the United States to pilot aircraft "down range." This capability removed the deployment constraint for aircrews. Rather than maintain several crews to keep one deployed at all times, all crews could fly as many aircraft as were available at any given time. However, in doing so, crews from a place-based cockpit culture found themselves struggling to master a new, flow-based conception of what it meant to be a pilot.

Remote Split Operations: "You Are Now Entering the CENTCOM AOR"

Flow-based and place-based logics often fractiously collided in the marketplace. Telework is incongruous with place-based conceptions of work. An employee might be more productive by splitting a would-be two-hour commute between additional work time and additional family time, but this hour of increased productivity would not register with an organization whose incentive structures were oriented toward place. Market forces have adjudicated clashes between flow and place. In the case of place-based information technologies such as video rental stores, these proved fatal. Conversely, a number of ambitious flow-based online stores unpleasantly discovered the continuing relevance of place during the dot-com bubble. Our present business environment presents an incomplete synthesis of these two logics.

These same cultural collisions are happening presently between flow- and place-based logics in the military. From a place-based perspective, a Predator crew's lack of physical presence in the battlespace inherently cheapens its work. This argument takes two major forms. First is the "no skin in the game" trope. A Predator crew does not directly experience risk comparable to that of ground troops in the course of its duties, thus diminishing the crew members' professionalism or seriousness about their duties. Second, the "video game" trope holds that the reality of the experience of remote aviation stops at the ground station, and because of the distance of the connection, crews are held to feel disconnected from the effects of their choices.[30]

In fact, the Predator community members' flow-based perspective concentrates on the equivalence of direct battlefield effects and the ramifications of those effects for their comrades.[31] These institutional struggles over meanings are covered exten-

sively in other works on the history of that technology.[32] Rather than attempt to adjudicate these claims, this article holds that they are incommensurable but demonstrate real tensions between flow and place in the contemporary military context.[33] The Predator community's experience offers a window into cultural clashes that accompany transitions from place-based to flow-based conceptions of warfare.

To situate this case, the move toward flow-based warfare in the Predator platform was not inherent to the airframe's "fly-by-wireless" control system.[34] Pop analysis of the platform typically addresses the onboard automation and computers, presumably as a replacement for human judgment; such an approach is a fundamental misapprehension of the platform's design and capabilities. In the words of Abraham Karem, primary designer of the aircraft, "Almost all of our subsystems from 1985–89 are still flying in some Predators today [in 2012], including its 27-year-old computer and, with minor changes, the ground station."[35] Processors that are outperformed by five-year-old smartphones should prove disappointing to both technofetishists and technophobes who see this aircraft as some sort of advanced war-fighting robot. As with any other aircraft, the heart of the system remains the aircrew, but the sea change is in the relationship of the aircrew to the aircraft.[36]

The craft and crews evolved toward a flow-based understanding of their relationship with each other. Much like previous remotely piloted aircraft (RPA), the GNAT 750, an early model in the Predator's lineage, was essentially a long-dwell radio-controlled plane.[37] This crew controlled the aircraft from a ground station within the combat theater. The production-model Predator incorporated a satellite data link that greatly expanded the range from which the craft could be flown—from line-of-sight range to anywhere in the satellite's footprint. In this intermediate state, crews would still deploy to a forward operating location, and the craft could be flown within the same general theater but outside the immediate combat zone. This general model saw use during operations in the former Yugoslavia.[38]

During the campaigns in Iraq and Afghanistan, the RSO model connected these satellite downlinks to terrestrial communications circuits, allowing the craft to be flown from virtually any location on the global information grid. As previously noted, the act of piloting moved to a place where it was least logistically costly: the continental United States.[39] Moreover, it enables data flows to non-colocated intelligence analysts, resulting in a transgeographic social network built around the focal point of a Predator mission. Managing this network is a primary issue for an RSO crew.

Coming to terms with the demands of a flow-based relationship between aircrew and aircraft proved challenging for previously place-based aircrews:

> During our first year in the Predator, we found learning the domain a much greater obstacle than learning the aircraft. In manned aircraft, space was important—satellite communications and the Global Positioning System (GPS) served as critical mission enablers. In the Predator, though, space became part of our domain. Orbits and footprints turned into practical rather than academic concerns as we realized that losing a satellite link could cut our control cables. Further, cyberspace folded into our world; servers acted as the eyes with which we scanned for other aircraft. Simultaneously, our ability to interpret engine sounds and vibrations through a throttle quadrant atrophied. Our experience of aviation became more abstract as we adapted to our new domain—neither better nor worse but different as we gained a new common sense. For instance, in RPA common sense, it is commonsensical to "demand" effects (rather than "command" actions) from a number of aircraft

at once through a multiplexer when doing so increases intelligence collection without degrading kinetic capabilities.[40]

Over time, the Predator and Reaper RPA communities reached some synthesis between the old and the new. As a symbol of this synthesis, RPA units began posting large signs over the entryway of their command centers declaring, "You are now entering the CENTCOM AOR [Central Command area of responsibility]." In an explicit formulation of a flow-based conception of a combat theater, the crews inside declared that they were in Afghanistan—in a substantive but nongeographic sense. Their duties, actions, and significant social relationships were more strongly manifest there than in their local physical environs.

In this synthetic identity, what one did in a place constituted his or her presence in that place. For this reason, a number of squadrons began to seek identity in "lineages of action" rather than in similarity of airframe.[41] Narratives of persistent sensor-shooter gunships over the Ho Chi Minh Trail and stories of similarly low-performance but high-impact Cessna observation pilots from Vietnam became reservoirs for identity.[42] This functional, human-centric lineage contrasts the normal hardware-centric interpretation, which traces the Predator to the Firebee "drone" and other remote predecessors.

This synthesis was hardly settled. In his autobiographical account *Predator*, Lt Col Matthew Martin recalled that the aforementioned sign "could just as easily have read *You Are Now Entering C. S. Lewis's Narnia* for all that my two worlds intersected."[43] This idea of living in a space without places proved disorienting to crews over time, especially when life for both their comrades "down range" and their significant home relationships remained oriented around place.[44] We have yet to understand the long-term effects of this conflict between cognitive distance and physical distance, especially when these effects are experienced in isolation.[45]

This situation was further complicated by the firm role of place in the American public discourse about war—to have someone use deadly force from within a place of peace was deeply incongruous with American expectations of a homeland essentially immune to organized armed violence. Perhaps this perspective explains the hyperbolic response to an op-ed by the Brookings Institution's Peter W. Singer during the recent drone performance recognition controversy.[46] Unfortunately, this yields a strange civil-military scenario in which a group of service members who are among those who kill the most in our wars are not included in the constructs that normally legitimate killing in war. Without straying too far into normative territory, the "video gamer" answer to this paradox—the idea that remote killing is less real—induces principal-agent problems into the act of legally legitimated killing. First, it lessens the gravity of lethal policy choices in the popular imagination, and second, it decouples those who carry out those choices from the constructs by which the larger society reconciles itself to those who kill in its name. Suffice it to say, the conflict between the Predator's extreme case of flow-based warfare and traditional place-based conceptions of combat is far from being resolved.

Libyan Rebels: Crowdsourcing Intelligence

Our third case explores how flow can effectively repurpose extant networks against a territorial or bureaucratic adversary. Steve and Sonia Stottlemyre explored the Free Libyan Army's use of online social infrastructure as a means for command, control, communications, and intelligence during the 2011 Libyan civil war.[47] During the period of armed conflict, the same networks that had been built through social media during the uprising hosted ad hoc flow-based forms of command and control. These constructs proved resilient in their battle against Mu'ammar Gadhafi's traditional structures. Three vignettes illustrate this point.

Crowdsourced Human Intelligence

According to John Pollock of MIT's *Technology Review*, one tech-savvy French intelligence officer leveraged social media to build an online human intelligence network with willing Free Libyan Army partners:

> After about a hundred hours of work, Martin [a pseudonym] had 250 or so direct contacts in Libya and elsewhere. He created, in effect, a private intelligence network. Initially, he expected only "ambient" or background information, but the intelligence he gathered soon proved useful for both strategy and tactics. Martin tried alerting his hierarchy to its potential for following the flow of action on the ground. It took a while for them to accept this. "They were very afraid in the beginning, because they had no control," he says, "[so] I ran a kind of laboratory." He set up a desk and was given no military intelligence. His captain asked specific questions and matched Martin's performance against more formal intelligence channels. Precise comparison is difficult, but Martin estimates that eventually 80 percent of the intelligence used by his [unit] came from his sources.[48]

This vignette demonstrates the use of flow that transcends place. The officer was able to build a network rapidly with no physical contact, organized around the simple principle of cooperation between NATO and the Libyan rebels. The network allowed mutual sense-making across geographic boundaries.

Crowdsourced Subject-Matter Expertise

These expertise-seeking flows went both ways. Libyan rebels could ask sundry tactical and engineering questions to networks of supporters and sympathizers around the world. In one particularly memorable episode, according to Pollock,

> After weeks of skirmishes in the Nafusa Mountains southwest of Tripoli, Sifaw Twawa and his brigade of freedom fighters are at a standstill. It's a mid-April night in 2011, and Twawa's men are frightened. Lightly armed and hidden only by trees, they are a stone's throw from one of four Grad 122-millimeter multiple-rocket launchers laying down a barrage on Yefren, their besieged hometown. These weapons can fire up to 40 unguided rockets in 20 seconds. Each round carries a high-explosive fragmentation warhead weighing 40 pounds. They urgently need to know how to deal with this, or they will have to pull back. Twawa's cell phone rings.
>
> Two friends are on the line, via a Skype conference call. Nureddin Ashammakhi is in Finland, where he heads a research team developing biomaterials technology, and Khalid Hatashe, a medical doctor, is in the United Kingdom. The Qaddafi regime trained Hatashe on Grads during his compulsory military service. He explains that Twawa's *katiba*—brigade—is well short of the Grad's minimum range: at this distance, any rockets fired would shoot past them. Hatashe adds that the launcher can be triggered from several hundred feet away using an electric cable, so the enemy

may not be in or near the launch vehicle. Twawa's men successfully attack the Grad—all because two civilians briefed their leader, over Skype, in a battlefield a continent away.[49]

These approaches, these global collaborations for local effect, became commonplace over the course of the conflict. Again, Pollock writes,

> As with Wikipedia, [weapons] . . . expertise might come from anyone—like Steen Kirby, a high-school student in the state of Georgia. As well as identifying weaponry, Kirby pulled together a group through Twitter to quickly produce English and Arabic guides to using an AK47, building makeshift Grad artillery shelters, and handling mines and unexploded ordnance, as well as detailed medical handbooks for use in the field. These were shared with freedom fighters in Tripoli, Misrata, and the Nafusa Mountains.
>
> The Misratans showed impressive ingenuity. Engineers hacked new weapons—including a remote-controlled machine gun mounted on a children's toy—and adapted technology on the fly. Laptops, Google Earth on CD-ROMs, and iPhone compasses gave the freedom fighters range. After a rocket was fired, a spotter confirmed the hit, reporting that it had landed, for example, "30 yards from the restaurant." They then calculated the precise distance on Google Earth and used the compass, along with angle and distance tables, to make adjustments.[50]

By applying flow-based approaches, the Libyan rebels redefined the boundaries of the battlespace. Rather than solely relying on physically present intelligence forces, a balance that would have overwhelmingly favored their adversary, they leveraged their cultural support through communications technology to pit advanced volunteers who were technically knowledgeable and cyber-savvy groups against their enemies.[51]

Repurposed Civilian Spaces of Flow

Finally, the Libyan rebels made extensive use of extant civilian communications architecture. Pollock notes that "as military budgets shrink, the world urbanizes, and . . . cheap handheld technology is making citizen networks an inevitable feature of the information battle space."[52] This was most apparent with the rebels' use of Twitter, which Stottlemyre and Stottlemyre demonstrate through exchanges among rebels, crisis mappers, and various sympathizers:

> Twitter acted as a platform for collaboration on and compilation of intelligence products. Many separate Twitter users began compiling data and information on their own pages. They Tweeted data they collected, information they processed, links to information provided in crisis maps, and Retweeted information provided via private and professional (i.e., media) Twitter users, thus creating a central repository of links to tactical information they deemed valuable.[53]

The increasingly common use of civilian communications by all parties in conflict supports their finding. Interestingly, since civilian telecommunications is intended to create lateral peer-to-peer communication, the collision of civilian communication with military command and control will likely be fractious. Historical ad hoc uses of such communications—most notably the utilization of a commercial telephone to call down gunship fire support during the invasion of Grenada—have been innovative and unconventional.

Altogether, the case of the Libyan civil war demonstrates how a local rebel group transformed its struggle by globalizing the conflict by employing flow-based tactics. In this campaign, we see a profound blurring of the lines between combatants and civilians because of extensive real-time collaboration. Flow-based conflict patterns

may make framing and narrative far more important because people can opt in and opt out more easily through web-based collaboratives than they could with recruiting lines. Therefore, the decision to join a conflict may be increasingly about political will and social popularity since technological ability is ubiquitous. We also see how flow can bring virtual expertise and off-board skills into the battlespace without regard for where those skills are housed. The implications of these cyber-guerilla wars for civil-military interaction and noncombatant immunities bear much thought.

Conclusion: Coming to Terms with Flow-Based Warfare

This article set out to explore the thesis that recent changes in communications technology have increased the prevalence of flow-based warfare in modern conflict. We found either new or geatly expanded flow-based warfare in at least three major contemporary wars, thus demonstrating the utility of Castells's theories as a heuristic for emerging forms of warfare, especially in understanding the adoption of these forms and the cultural clashes that surround them. As a plausibility probe, this effort should be considered theory building rather than theory testing. Follow-on research designs might establish the conditions under which flow-based warfare might be more likely adopted or effective. We also might evaluate the relative balance between flow-based and place-based logic in battlespaces over time.

Moving from academic to policy questions, we see that the rise of flow-based warfare brings with it new questions and new challenges. Such warfare has two imperatives: to protect fluidity and to fix the enemy in place. To the first point, one must protect connectivity and use it both to export risk into sanctuaries and import knowledge and resources from a wide range of sources. Connectivity and its resulting flexibility keep situational awareness strong and allow the network to synchronize actions. This, in turn, enables the network to attack at a time and space of its choosing, attain its goals, and remove itself from the geographical place before the adversary can respond. The second imperative is to deny the enemy the ability to do the same. Fixing his network in place has the effect of isolating flows, interrupting connectivity, and dismembering the network, node by node. Dynamic strategies such as the classic Boydian observe-orient-decide-act loop work well toward these reciprocal offensive and defensive ends.[54]

Following Castells, flow-based warfare has two key types of players.[55] First are the programmers, who build the narratives that bind and grow networks. These narrative-crafting skills are often associated with transformational leaders but are generally difficult to identify directly through status quo bureaucratic personnel systems. Second are the linkers, who identify mutually beneficial partnerships, storehouses of knowledge, and previously untapped resources for the network.[56] The skills that make an excellent linker are often threatening to a centralized bureaucracy since effective linkers maintain wide networks of "off-org-chart" lateral ties.

Finally, flow-based warfare involves two issues. First, as alluded to in the previous paragraph, present industrial-age military personnel systems are poorly suited to managing a flow-capable force. A system that uses the attainment of static, formulaic goals as its primary metric for advancement has little chance of attracting, retain-

ing, and developing these players. If a flow-based force were so easily identified by an algorithm, an enemy would easily pin it down as well.

The second issue is even more difficult. For Americans, the deep constructs that surround the fundamental civil-military problem—how we as a society deal with those who have killed in our name—are based almost entirely around place. The idea of combat as a place of legitimate killing is built explicitly in geographic zones. Someone who kills as part of a flow, as do Predator and Reaper crews, does not fall cleanly into these constructs. This creates a liminal space, which hampers our understanding of the reciprocal civil-military duties and responsibilities in flow-based warfare.

More so, Westphalian understandings of sovereignty and the concomitant accountability for the use of force are built explicitly (at least in their original form) around space. *Cuius regio, eius religio* assumes that *regio* (physical realm) is the core framing logic of the system.[57] Given the increased global impact of transgeographic violence from flow-based networks, ungoverned and poorly governed places take on a new significance. These places can provide sanctuary for a "space of [violent] flows," for which Westphalian accountability cannot provide effective recourse. The adoption of low-based warfare, at least in part, comes as a response to these threats. If sovereignty is a space, then one can envision a difficult debate about whether it is a space of places or a space of flows.

This discussion lies beyond our present scope, but it does highlight one final benefit of Castells's heuristic—it is a critique of the state of the current "drones" debate. Armed RPAs are likely the most controversial expression of flow-based warfare, but the contemporary debate overly concentrates on the hardware and tends to neglect the humans. If a space is a material support to social practices, then it is fundamentally about people.[58] Similarly, warfare is a human enterprise, undertaken by humans against other humans for human objectives. It involves technology, much like any other social practice, but it is never entirely constituted by hardware.[59] Castells's idea of flows refocuses us on the classic military principle that "war is an extension of politics with an admixture of other means" and dissuades us from the temptation to see war increasingly as a technical problem.[60]

Technology matters insofar as it changes relationships between people—in Melvin Kranzberg's classic formulation, "technology is neither good nor bad; nor is it neutral."[61] Here, the communications technologies that enable flow-based operation of the Predator aircraft have no independent agency, but they do deeply shape the agency of all the players in that process. This influence matters in any of a number of ways, not the least of which is how we train and equip future forces and how we hold current forces accountable for their choices. In a closing recommendation, this article proposes that the academic discourse about emerging military technology might shelve the reductionist drones trope for a bit because those arguments tend to fixate on the technical aspects of a largely misunderstood and surprisingly banal technology. The debates that we should have are about the increasingly blurred distinction between combatants and civilians, the meaning of politics and narratives in a world of democratized violence, and the importance of evolving civil-military relations, given the changing meanings of place and flow in the battlespace.

Notes

1. William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: Presidio Press, 1996), 1–28.
2. Manuel Castells, *The Information Age: Economy, Society, and Culture*, vol. 1, *The Rise of the Network Society*, 2nd ed. (Oxford, UK: Wiley-Blackwell, 2010), 441.
3. Claude E. Shannon and Warren Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949), 1.
4. Castells, *Rise of the Network Society*, 442.
5. Ibid., 453.
6. Robert Sugden, "A Theory of Focal Points," *Economic Journal* 105, no. 430 (1 May 1995): 533–50, doi:10.2307/2235016.
7. Castells, *Rise of the Network Society*, 442.
8. "Keeping America Safe: The New Defense Strategy," Deloitte FedCenter Interview, 7 March 2012, http://federalnewsradio.com/sponsored-content/2012/03/march-7th-2012/.
9. Pekka Himanen, *The Hacker Ethic and the Spirit of the Information Age* (New York: Random House, 2001), xiv–1.
10. See, for instance, "Computer Coding Meetups," accessed 20 July 2015, http://coding.meetup.com/.
11. Idea incubators such as 1776 in Washington, DC, are an outgrowth of this trend. See "1776," accessed 20 July 2015, http://1776dc.com/.
12. A similar trend occurred with the introduction of dynamite, which empowered anarchists around the turn of the twentieth century.
13. To this point, the US Coast Guard adapted more quickly than its larger Bureau of Prohibition counterpart to the challenge of rum-running networks in the 1920s. A major reason concerns the small size and deep connectivity of the Coast Guard's officer corps. There were approximately 300 officers total, the vast majority of whom knew each other from time at the Coast Guard Academy and shared time in service. Effectively, the most junior officer could reach the commandant with an innovation or a novel idea through two or, at most, three steps. National Archives, Records Group 26, Box 178; and Dr. William Thiesen and others, various interviews by the author, US Coast Guard Historian's Office, Spring 2013.
14. James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press, 1998), 262–306; and Michael Polanyi, *The Tacit Dimension* (Garden City, NY: Doubleday, 1966), 1–26.
15. McRaven, *Spec Ops*, 1–28.
16. John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND Corporation, 2001). This idea that certain groups can take on certain structures invokes a simplified version of Horowitz's adoption capacity theory, especially the idea of organizational capacity. Michael Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010).
17. Arquilla and Ronfeldt, *Networks and Netwars*, 1–28.
18. Lawrence Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (New York: Vintage Books, 2007), 283–90.
19. Patrick M. Jost and Harjit Singh Sandhu, *The Hawala Alternative Remittance System and Its Role in Money Laundering* (Washington, DC: US Department of the Treasury Financial Crimes Enforcement Network and INTERPOL, 2000).
20. Rick Atkinson, "Left of Boom: The Struggle to Defeat Roadside Bombs," pt. 1, "The IED Appears," *Washington Post*, 30 September 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/28/AR2007092801888.html.
21. This cost-imposition strategy roughly parallels the ubiquitous sea-control versus sea-denial naval debates. Roger John Brownlow Keyes, 1st Baron Keyes, *The Naval Memoirs of Admiral of the Fleet Sir Roger Keyes: The Narrow Seas to the Dardanelles, 1910–1915* (New York: Dutton, 1934–35); and Paul M. Kennedy, *The Rise and Fall of British Naval Mastery*, 2nd ed. (Amherst, NY: Humanity Books, 1983).
22. Atkinson, "Left of Boom," pt. 3, "You Can't Armor Your Way Out of This Problem," 2 October 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100101760.html.

23. Ibid., pt. 4, "If You Don't Go After the Network, You're Never Going to Stop These Guys. Never," 3 October 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100202366_pf.html.
24. Ibid.
25. Stanley A. McChrystal, "It Takes a Network: The New Front Line of Modern Warfare," *Foreign Policy*, 21 February 2011, http://foreignpolicy.com/2011/02/21/it-takes-a-network/.
26. For a text on the principles of social network analysis and an introduction to core concepts of information flow and institutional architecture, see Phillip Bonacich and Philip Lu, *Introduction to Mathematical Sociology* (Princeton, NJ: Princeton University Press, 2012).
27. Charles Faint and Michael Harris, "F3EAD [find, fix, finish, exploit, analyze, disseminate]: Ops /Intel Fusion 'Feeds' the SOF Targeting Process," *Small Wars Journal*, 31 January 2012, http://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process.
28. Ibid.
29. Rebecca Grant, "Toward an Unblinking Eye," *Air Force Magazine* 96, no. 10 (October 2012): 44–48.
30. Sundry responses to Col Hernando Ortega, "Psychological Health of RPA Aircrews" (presentation, Brookings Institution, 2013).
31. Maj David J. Blair and Capt Nick Helms, "The Swarm, the Cloud and the Importance of Getting There First: What's at Stake in the Remote Aviation Culture Debate," *Air and Space Power Journal* 27, no. 4 (July–August 2013): 29–33, http://www.airpower.maxwell.af.mil/article.asp?id=161.
32. Notably, Maj Michael Kreutzer's forthcoming Woodrow Wilson School dissertation on the adoption of remote aviation technology and Caitlin Lee's forthcoming King's College dissertation.
33. For a discussion of the concept of incommensurability, see Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962), 109–11.
34. Dave Blair, "Remote Aviation Technology—What Are We Actually Talking About?," Center for International Maritime Security, 5 March 2014, http://cimsec.org/remote-aviation-technology-actually-talking/.
35. "The Dronefather," *Economist*, 1 December 2012, http://www.economist.com/news/technology-quarterly/21567205-abe-karem-created-robotic-plane-transformed-way-modern-warfare.
36. Blair and Helms, "Swarm, the Cloud," 29–33.
37. Thomas P. Ehrhard, *Air Force UAV's: The Secret History* (Arlington, VA: Mitchell Institute Press, July 2010), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA525674.
38. Timothy M. Cullen, "The MQ-9 Reaper Remotely Piloted Aircraft: Humans and Machines in Action" (PhD diss., Massachusetts Institute of Technology, 2011), 129, 216, http://18.7.29.232/handle/1721.1/80249.
39. A prima facie case exists for the superiority of RSO in comparing hours of overwatch to resource cost and constraints as compared to traditional deployments. A full-architecture cost comparison between deployed operations and RSO depends greatly on modeling assumptions.
40. Blair and Helms, "Swarm, the Cloud," 21.
41. Anonymous subject, interview by the author, 2013.
42. Anonymous subject, interview by the author, 2012.
43. Matt J. Martin and Charles W. Sasser, *Predator: The Remote-Control Air War over Iraq and Afghanistan: A Pilot's Story* (Minneapolis: Zenith Press, 2010), 45.
44. Hernando Ortega, "Telewarfare," *Air and Space Power Journal*, forthcoming.
45. Ibid.
46. Peter W. Singer, "A Military Medal for Drone Strikes? Makes Sense," *Washington Post*, 15 February 2013, http://www.washingtonpost.com/opinions/a-military-medal-for-drone-strikes-makes-sense/2013/02/15/e90c0638-76e4-11e2-8f84-3e4b513b1a13_story.html.
47. Steve Stottlemyre and Sonia Stottlemyre, "Crisis Mapping Intelligence Information during the Libyan Civil War: An Exploratory Case Study," *Policy & Internet* 4, issue 3–4 (December 2012): 24–39.
48. John Pollock, "People Power 2.0," *MIT Technology Review*, 20 April 2012, http://www.technologyreview.com/featuredstory/427640/people-power-20/.
49. Ibid.
50. Ibid. See also John Reed, "Libyan Rebels' DIY Weapons Factory, Robots and All," Defense Tech, 14 June 2011, http://defensetech.org/2011/06/14/libyan-rebels-diy-weapons-factory-robots-and-all.
51. The Standby Task Force was among these volunteers. Although not directly aligned with the Libyan rebels, they were certainly in opposition to Gadhafi's actions. See "The [Unexpected] Impact of

the Libya Crisis Map and the Standby Volunteer Task Force," Standby Task Force, accessed 20 July 2015, http://blog.standbytaskforce.com/2011/12/19/sbtf-libya-impact/.

52. Pollock, "People Power 2.0."

53. Stottlemyre and Stottlemyre, "Crisis Mapping Intelligence Information," 10.

54. See John R. Boyd, "Destruction and Creation," 3 September 1976, http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf.

55. Manuel Castells, *Communication Power* (Oxford, UK: Oxford University Press, 2009), 47.

56. The linkers are like Gladwell's connectors and mavens. See Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston: Back Bay Books, 2002), 19.

57. The phrase "whose realm, his religion" is a foundation of the Westphalian system, which focused sovereignty at the level of the state rather than a superordinate structure such as Christendom or a flow-based structure such as the Hanse.

58. Castells, *Rise of the Network Society*, 147.

59. David A. Mindell, *Iron Coffin: War, Technology, and Experience aboard the USS Monitor* (Baltimore: Johns Hopkins University Press, 2012), 133–49.

60. Carl von Clausewitz, *On War*, trans. J. J. Graham, abridged ed. (New York: Penguin Classics, 1982), 119.

61. Melvin Kranzberg, "Technology and History: 'Kranzberg's Laws,' " *Technology and Culture* 27, no. 3 (July 1986): 544–60.

Maj Dave Blair, USAF

Major Blair (USAFA; MPP, Harvard Kennedy School; MA, PhD, Georgetown University) is the acting operations officer, assistant director of current operations, and MQ-1B evaluator pilot at the 3rd Special Operations Squadron, Cannon AFB, New Mexico. Most recently, he was a member of the initial class of the US Air Force chief of staff's Captains' PhD Scholars. He previously served as the assistant operations officer for war fighting and as an MQ-1B instructor pilot in the 3rd Special Operations Squadron, deploying several times as a liaison officer and an intelligence, surveillance, and reconnaissance battle captain in Afghanistan and on emerging fronts. Major Blair began his flying career as an AC-130 gunship pilot with three deployments to Iraq. He has also served in the Defense Attaché Office–Moscow and the US Naval War College's War Gaming Division. He writes on organizational structure, remotely piloted aircraft culture, and persistent airpower.