

THE SMALL AND THE MANY

MARTIN LIBICKI

Freer silicon, which portends the ability to collect enormous quantities of data, will alter war in several stages. Pop-up warfare describes the battlefield in which the means of war are quiet or hidden until they rise and engage. The growing and (for the time being) unchallenged ability of U.S. forces to lay a Mesh over the battlefield permits the tracking and targeting of increasingly small, quick, stealthy, and transient objects. The logical consequence of this capability's spread is Fire-ant warfare, a battlefield dominated by scads of sensors, emitters, and microprojectiles.

Today, platforms rule the battlefield. In time, however, the large, the complex, and the few will have to yield to the small and the many. Systems composed of millions of sensors, emitters, microbots and miniprojectiles, will, in concert, be able to detect, track, target, and land a weapon on any military object large enough to carry a human. The advantage of the small and the many will not occur overnight everywhere; tipping points will occur at different times in various arenas. They will be visible only in retrospect.

The triumph of the small and the many, of information technologies over industrial technologies, can be discussed in terms of its three phases. The first, pop-up warfare, is the expression of 1990's technology under the no-longer-valid assumption that the U.S. faces an enemy with comparable capabilities. The second, the Mesh, describes how U.S. military power (using technologies available over the next twenty years) might work against a foe with developed industrial but underdeveloped informational capabilities. The third, fire-ant warfare, assumes expensive sensors will themselves be vulnerable and have to give way to networks of inexpensive information elements.

Pop-Up Warfare

A tilt toward quality in the quality-quantity equation is a good sign that a military technical revolution has occurred. During the run-up to the Gulf War, Allied and Iraqi counts -- manpower, tanks and aircraft -- were

anxiously compared. War quickly made clear that the Iraqis could have fielded two or perhaps five times as many men, tanks, and planes without affecting the outcome much. Allied technology -- both equipment and our sophistication at using it -- was so superior (for the terrain) that exchange ratios were overwhelmingly in its favor. We could see and they could not. We could sneak up unnoticed and catch them by surprise. Our weapons could be precisely aimed while theirs were effective only against targets several miles wide (e.g., Tel-Aviv). We were on one side of a revolution and they were on the other.

Yet consider how differently we would have had to operate if they had had but a fraction of our capabilities (alternatively, what a conventional war against the Soviets in the 1990s would have looked like). Virtually everything we used on the battlefield would have been vulnerable had it been visible. We would have had to harden or hide our logistics dumps and command and control nodes. Our tanks, were they are to survive, would have to be hard to find except during those few moments spent scurrying or shooting. Surface ships would have been nearly useless anywhere near shore. Both sides would have been driven to pop-up warfare -- a mode in which elements are hidden and quiet except during those brief and dangerous moments of engagement or movement.

Among the various elements setting the stage for pop-up warfare, the precision guided munition (PGM) has probably been the most salient. With PGMs, any locatable object can be precisely targeted and, most likely, destroyed. Any object with a fixed latitude and longitude could be targeted (with cheap, accurate aiming systems) and struck. To do this, today's PGMs use complex homing and terrain-matching devices coupled with accurate gyroscopes and accelerometers. Tomorrow's will be helped by GPS-guided seekers. External systems would relay the latitude, longitude, and altitude of the target, then the PGM would zip to that point. More sophisticated systems would use real-time updates against relatively slow-moving targets and perhaps even local (or relative) positioning systems for greater accuracy. Moreover, with new assets in space, and the increasing sophistication of airborne sensors (e.g., AWACS, JSTARS), as well as seaborne sensor packages (e.g., Aegis Cruisers), the number of objects that would fall under target scrutiny would increase as well. Thus would fixed and slow-moving targets fare poorly on a pop-up battlefield.

Pop-up warfare puts a great premium on minimizing one's own signatures (e.g., stealth) and amplifying the enemy's (e.g., the data fusion capabilities of Aegis systems). Both sides would have to stay hidden most of the time, pop up just briefly to move or shoot, and then scurry back into the background. To succeed, forces would quickly have to distinguish threats from decoys and friendlies, determine the threats' location and bearing, fire, and then disguise and eliminate their own signature.

Can large, fixed, above-the-ground targets be defended? Some targets can shoot back against incoming missiles. Capital ships, for instance, are equipped with both anti-missile missiles and close-in weapons systems designed to disable incoming missiles with a hail of lead. Sufficiently valuable fixed sights might be protected by upgrades of the Patriot missile, or follow-on versions such as Erint, THAAD, or the Arrow. One proposal calls for hiding anti-SCUD missiles near potential SCUD sights to chase and overcome the latter while in boost phase.

Nevertheless, the betting has to be with the attackers rather than their targets. Targets are bigger than missiles, and missiles shoot first; they can succeed in aggregate by overwhelming the defense with numbers (many of which need only be cheap decoys). Defense against hyperkinetic projectiles could be far more challenging (the SCUD launches into Israel suggest such missiles are even more dangerous after they fall apart). A projectile that reaches Mach 10 or 20 and then releases a shower of darts clad with ceramic (to stay intact under reentry heat) can greatly damage soft targets. If the missile can elude destruction prior to decomposition, mission completion is only a matter of time.

The recent emphasis on knocking out anti-ground missiles in their boost phase suggests the realization that missiles will be very hard to hit once they stop radiating heat. As it is, today's missiles -- hard enough to hit as it is -- have yet to exploit a deep reservoir of stealth techniques. When they have done so, they will be far harder to hit. The logical consequence of the missile's superior penetration capability is that their targets would have to be dispersed, protected in very hard bunkers, or be moved around all the time.

Pop-up warfare will evolve as signatures can be harvested by unmanned objects: loitering missiles, unmanned drones, unattended submersibles, increasingly sophisticated mines. New techniques of data fusion can help correlated such signatures. Conversely, platforms will need more stealth to

survive. The F-117A, the B-2 and submarines are already stealthy, but stealth is also mooted for missiles, surface ships, and even tanks.

The contest between stealth and anti-stealth will be long and drawn-out, but again the betting has to be against stealth for any platform large enough to encompass a human. A hider must suppress a bit-stream of information that constitutes its signature. A seeker tries to amplify these signals in order to read them. As information technology advances, so does the ability to amplify bits. No such mechanism favors suppression. Indeed, an ecological axiom states that although removing half of a pollution stream is easy, each successive halving is harder. At very low levels, sophisticated devices to clean up one form of pollution often create another. Moreover, the cost of data collection and fusion drops with the cost of silicon. New stealth techniques, although effective, are not getting cheaper.

Thus even with stealth, everything ultimately can be found. All objects have mass and thus gravity. Every object moving in a medium creates vortices and must expend energy to do so. If nothing else, objects of a certain size have to occupy some space for some time. A set of sensors placed sufficiently close together can, in theory, eventually trap everything by getting close enough. A sufficiently fine web can intersect with any submarine. A line of sensitive receivers placed close enough together will find its line-of-sight path to a beaming object cut if a bomber -- no matter how stealthy -- rolls past. Neither architecture may be particularly cost-effective. Yet, both show how sensors of certain minimum discrimination placed close enough together can, at some epsilon, catch anything. Hence, the Mesh.

The Mesh

Chances are good that the United States will face a decade or probably two when it can apply military force against opponents with greatly inferior capabilities. Their strategy would not be to defeat American forces in the traditional way so much as to create as many casualties as possible in hopes that the United States would be dissuaded from further pursuit. Our strategy, in turn, is to use our longest suit to control the battlefield to the greatest possible extent to minimize exposure and casualties. As information gathering and processing capabilities continue to improve, our ability to see

into the battlefield will increase exponentially. This advance brings with it both great opportunity and problems.

Combat requires doing two things: finding targets and hitting them (while avoiding the same fate). PGMs allow their possessors to hit most anything. Tomorrow's meshes will allow their possessors to find anything worth hitting. Every trend in information technology favors the ability to collect more and more data about a battlefield, knitting a finer and finer mesh which can catch smaller and stealthier objects.

A long period can be expected in which elements of the Mesh coexist with current platforms. The United States, for instance, will probably be able to deploy fleets of light satellites for surveillance before others can target our existing stock of heavy low-earth orbiters. During that interim the choice of using platforms or the Mesh for any particular mission would depend on which worked better or was more cost-effective. Thus, an initial architecture for the Mesh need not have all capabilities at once as long as platforms to do the same job can survive.

The Mesh, at its outset, would be one part of a cue- and-pinpoint system. Today's airborne sensor system is a multi-layer system of satellites, large aircraft, UAVs, manned aircraft, and finally, PGMs themselves. Under the sea, certain types of sonobuoys detect the presence of submarines by passive sensors, followed by active sensors which localize the submarine by pinging it, followed by torpedoes which use acoustic means to land on top of it. Similarly, the Mesh will be composed of unmanned sensors, infiltrated into existing systems composed of large and expensive platforms. ARPA's Warbreaker project is experimenting with systems that proliferate sensors that allow scanning wide areas for certain types of signatures.

Challenges: Managing the enormous increases in information flow is probably one of the greatest challenges created by the workings of the Mesh. The technical problems -- filtering, fusion, and fanning -- are daunting enough, but the stickiest ones deal with the distribution of information.

Consider, for instance, a joint task force formed overnight to head off an unexpected incursion in some otherwise forgettable corner of the world. As the crisis starts, the relevant CINC will have a certain flow of information from existing sensors such as satellites, electronic listening posts, and perhaps fielded seismic and acoustic systems. Among his first acts will be to

duplicate his enormous monitoring capabilities to some joint task force commander. Shortly thereafter, a new flood of information will come from various data collection platforms such as AWACS, JSTARS, Aegis, and perhaps small satellites and UAVs. Suddenly, the relative trickle of information available to the commander starts to become a current sending forth far more data than any human can deal with. This flow must, in turn, be apportioned to various sector commanders for their action. Atop this flow comes a flood of information as various platforms start to deploy distributed air, water, and ground sensors in various formations. These, too, then have to be analyzed, dissected, and apportioned to the various sub-commanders each of which has a different array of capabilities. Managing such information blooming will require considerable practice.

Opportunities: The development of large effective information collection and analysis systems permits the United States to aid an ally without the commitment of military forces, and in some cases without fingerprints at all. So far, the Soviet Union has provided satellite imagery to Argentina (during the Falklands war), and we did the same for Iraq (fighting Iran) and the Angolan government (fighting UNITA). The denser the overhead information, however, the more help is available. Near real-time imagery of Serbian artillery, for instance, might help Bosnians more accurately target their return fire -- information as a real force multiplier.

In times past, the United States has helped allies by providing equipment: examples range from the Lend- Lease program to the provision of Stingers to the Afghan rebels. If these sensors and emitters become global commodities (not necessarily a happy development), the United States could still provide the equivalent of material support. It would silently supply the pattern recognition, data fusion, and command-and- control software that makes these systems function. Bytes leave no fingerprints.

Could demonstrating a Mesh, in detail, induce surrender without the need to use much force? To do so, requires persuading others that the ability to lock onto a platform's precise position is tantamount to ensuring its destruction. After all, the Gulf War allies did not have to shoot down every Iraqi plane to win air superiority. It sufficed to make a convincing demonstration of "You fly -- you die." Such correlation can be delivered through open broadcast (e.g., via one of tomorrow's virtually infinite channels). The potential victim is then given opportunity to demonstrate his distance from the targeted machine. The act of seeing oneself on television futilely trying to hide may

be very salutary. Thus might warfare become the child's game of hide- and-go-seek rather than the adult's game of hide-and- go-kill.

Force Sizing: The last implication of the Mesh is that it simplifies what would otherwise be a difficult problem for the United States -- sizing the forces. During the Cold War, our forces were sized against those of the Soviet Union; without so large an enemy, the task is far tougher. Force sizing based on war counting (e.g., one-and-a-half wars or win-hold- win) is likely to die a well-deserved death. The use of capabilities-based sizing cannot satisfy for long, either. The capabilities of others are a much better guide to weapons development strategies (where numbers are of limited relevance) than to weapons procurement strategies (where numbers are highly material). To say that military planners should disregard intentions and focus on the strength of others logically leads to a long-run planning goal of an armed forces capable of defeating every one else (including our own allies) in concert.

The rising importance of the Mesh suggests a force- sizing calculus that could be made independent of the precise size of the opposing threat. One precedent is the Navy's rationale for carrier battle groups. The argument was that the Navy needed three carrier groups in every area to keep one on station at all times. Before 1980, the four areas were the Atlantic, the Mediterranean, the eastern Pacific and the western Pacific. In 1980, adding the Indian Ocean suddenly raised requirements from twelve to fifteen. Any debate over the size of the threat (e.g., a putatively aggressive Soviet Union) could be finessed; the number of oceans rather than the size of the threat mattered. Similarly, force planners could start by estimating the establishment needed to deploy, operate, and service the targets generated by a Mesh. Such a Mesh should have minimal coverage everywhere and the ability to go to maximal useful coverage in however many trouble spots we have to simultaneously have to create targeting solutions for. Done right, such calculations should be robust against wide variations in the size and intentions of likely threats.

Fire-Ant Warfare

At some point in the development of the Mesh, our forces will encounter the paradox that those platforms whose capabilities make other platforms vulnerable are themselves vulnerable and ultimately untenable over the

battlefield. Our surveillance planes, for instance, not only come in highly non-stealthy platforms that do not move too fast, but they radiate like Christmas trees. Future engagements are likely to see even relatively backwards nations target major sensor platforms. Should they prove vulnerable, other ways of restoring their surveillance capabilities will have to be found, failing which, everyone returns to the days of the blind.

As argued above, an equally if not more effective way to weave a Mesh would be from millions of small objects. They are cheap, they can get closer to the target, and they are collectively most robust against deliberate attack. Deploy enough of them, and they are too cheap to kill.

An analogy to robots may better suggest the wisdom of distributing capabilities. People perceive robots as complex objects that, in every successive generation, come closer to resembling man. A new metaphor developed at MIT is that of robots as ants. Each one exhibits certain limited aspects of intelligence: some specialize in avoiding shadows; others, in walking without stumbling; yet others, in staying away from each other. Smart ants are less powerful than smart robots, but they are small, light, cheap, versatile, and easy to reprogram. Being cheap, they can be built in large numbers.

Battlefield meshes, as such, can be built from millions of sensors, emitters, and sub-nodes dedicated to the task of collecting every interesting signature and assessing its value and location for targeting purposes. Many of these sensors have already appeared, albeit in rudimentary form. In the future, they will be cheaper, more sensitive, and capable, collectively, of receiving signals from the various parts of the electromagnetic spectrum. Some would be optical sensors -- perhaps small charge-coupled devices tied to neural net processors; they could cover not only the visible range, but also near-ultraviolet, and all shades of infrared. Others would act like small radar detectors, either singly, or in computational harmony with its like-minded neighbors. Chemical sensors could detect the passage of machines or their men. Some would sense changes in magnetism, air pressure, sounds, vibration, or even gravity, and so on.

Why this proliferation of sensor types? The easy answer is that warfighting conditions differ. Some environments (e.g., open desert) and targets (e.g., surface ships) are easy to look at; other environments and targets are tougher. To detect the latter may require exploiting the inherent differences

between machinery and background which register on other senses. The hard answer is that single-sensor surveillance gives the target a single-dimension problem to solve. Tanks strive to be hard to see and thus employ camouflage and night movement. Submarines strive to stay quieter, using size, baffling, and ultra-smooth running machinery. Aircraft are stealthy by controlling their X-band reflections by engineering special shapes and coatings. Multi-sensor surveillance, however, complicates the single-dimensional problem by obviating techniques which dampen emissions of one type at the expense of another; moreover, the multi-dimensional problem they create becomes that much more difficult to solve.

No one sensor need necessarily detect every emanation from a target. The more capabilities a sensor combines, the more expensive it gets. Thus the fewer would be used and the easier each would be to find and kill. Alternatively, specialized, perhaps even single-purpose sensors, can each collect signatures, exchange them with subnodes and *collectively* form a picture of a target in its environment.

The Mesh would also contain cheap disposable emitters to illuminate targets with reflected radio waves, generate confusing signatures, and broadcast local positioning signals for precise targeting. Although accurate positioning systems are critical for the operation of a Mesh, full GPS capability need not be ubiquitous (GPS can also be jammed). Emitters that know where they sit and can broadcast relative distances to the other elements of the Mesh may suffice.

Some sensors may be equipped to move; they may have little cilia-like feet on land, fins in the water, and an airfoil (see below) in the air. Mobility would help right errantly laid sensors, take high ground (trees, houses, hills) in appropriate terrain, and cluster to where other cuing systems suggest the presence of target-rich environments. Movable sensors fitted with precise chemicals or explosives (e.g., for taking out a critical piece of electronics) could be the killing mechanism in some cases.

Perhaps the prototypical sensor would be a sandwich the size of a penny. On top would sit a photovoltaic energy source or optical sensors; next would be a sliver of microprocessor, perhaps a chemical or acoustic sensor, and then a penny-sized battery, a transmitter for an antenna jutting out to the side, and finally some anchoring pod on the bottom. Another design would make the sensor look like a weed plant of a meter or two length. The shaft would be

the antenna; the head a spectral sensor device capable of seeing as far as a human can, and the roots would be acoustic and vibration sensors, as well as anchors. To use yet another analogy, sensors might be the size of bottle caps; emitters, the size of soda straws; and miniprojectiles the size of coke bottles.

Architectures: The transition from single source sensors to distributed sensors has architectural implications that will take some getting used to. For instance, most radars today couple a relatively cheap emitter with a relatively expensive collector. Anti-radar missiles home in on the emitter and by so doing destroy the collector. Distributed architectures would require far more computation to translate the reflections into objects, but proliferating emitters and spreading them far from collectors complicates the targeting problem of the anti-radiation missile immensely. Emitters would survive longer and receivers would remain unscathed. When later generations of missiles learn to recognize receivers by their shape, the latter themselves could be distributed among smaller networked patches. Again, the computational requirements of putting together a big picture increase, but the cost of computation are continuing to decline.

Another advantage of distributing sensors both over space and by type is that it complicates countermeasures. An aircraft pursued by a missile knows it is being tracked, in effect, by only one sensor, and, more likely than not, in only one frequency. Thus dispersed flares, even though they travel far slower than planes, can be picked up as aircraft by IR missiles, which can recognize the bearing of a signal but not its distance (and thus speed). Tracking a plane using multiple sensors requires that the countermeasures exhibit the same three-dimensional behavior as aircraft do; using multiple sensors also requires all countermeasures to stay together rather than just appear aligned by the perspective of the missile (e.g., the flare, the jammer, and the chaff have to travel together). This is a far more complex undertaking.

Another feature of the Mesh is that it has the capability to replace man-to-man coverage of a battlefield with zone coverage. The pursuit of a given target, which is to say, its signature, need not be performed by chasing it. Instead the overall Mesh can selectively pay attention to zones over which the target is running. It tunes into successive sub-meshes by expanding the latter's communications bandwidth and triggering external sensors to concentrate on an area. This shift has more than metaphorical significance; it also alters one of the rationales of maneuver warfare. The latter has always

assumed that being there at the right part of the battlefield was paramount. But being there is not necessarily a prerequisite to seeing there, and not necessarily a prerequisite to hitting there if the range set of one's own weapons is sufficiently dense.

The last idea suggests the eventual waning of a currently popular theme in Army doctrine (first the Soviet's and now ours) -- the use of overwhelming force as a psychological disruption at the outset of an operation. This technique may not work as well as expected against a sufficiently well architected Mesh. One necessary feature in a Mesh is a sufficiently high degree of disaggregation so that the difference between engaging targets all at once or one at a time is relatively minor. The second feature is at least some practiced capability for graceful degradation so that a percentage loss of capability does not mean a total loss of effectiveness. The ideal is a Mesh that has no center of gravity and thus must be defeated in detail.

Tips of the Spear: Finding targets is one thing, but ending their useful life takes more than bytes. Tomorrow's weapons would likely resemble today's PGMs. Evolutionary improvements in energy chemicals suggest that the warheads and engines could be somewhat smaller but probably not so small as to be radically different creatures.

One big change would be increased use of weapons that do not have to be borne on manned platforms; mines are a good example. Radio contact with the weapon and external cuing systems for its launch would allow the weapon to be positioned closer to its potential targets without putting platforms in harm's way. Thus a battlefield can be seeded with air- dropped munitions which can be raised, oriented, and activated on command.

A second big change would be in the logic of the seeker -- or what is left of it. Today's PGMs have to find targets on their own. Sometimes they get external help (reflected laser tags or radar waves); sometimes their path is pre-programmed (e.g., cruise missiles); sometimes they have to take advantage of passive measures such as heat signatures or pattern recognition. In any case, they have a nontrivial computation to perform. Up to 90 percent of a PGM's cost is in the guidance and control, and most of that is in the guidance.

PGMs operating in a sensor mesh, however, can use the latter's intelligence. A PGM that is given a target's exactly location can get there on its own in

many ways. If GPS is jammed, it can use local positioning signals. If it knows where it starts from, its own gyroscopes and accelerometers will tell it where it is going. A purely ballistic flight path may work against slower targets. Others might simply home in on a sensor attached to the target. A PGM that needs less processing can use a simpler guidance system. Thus cheaper, it can be made in greater numbers and can defeat heavily defended targets by saturating them with multiple incoming warheads.

Logistics, Command and Control: The capabilities of even the most elegant military systems are useless without reasonable solutions to the problems of getting them there and talking to them when they arrive.

Getting Mesh components to where they are needed is a problem whose solution will depend on both circumstances and the architecture of the system employed. A platform to insert Mesh parts is a target no less than the platforms the Mesh was designed to fight against. Parts which are hardened can be dropped from air--even from space--or launched by artillery. Sometimes, special forces could distribute them into very small but critical areas. Micro-motors might even, at some point, allow them to walk into theater (but at no small demands on energy systems) or even drift into theater. Submarines and stealthy surface vessels may be able to lay down a naval Mesh. All these creatures can be also delivered by civilian means. A Mesh intended as a defensive field inside one's borders can be deployed as a mine field might be -- except that by separating the triggers (the sensors) from the explosives (the PGMs), both are far harder to detect).

Although command-and-control functions are integral to the Mesh's operation, because a Mesh sees no distinction between communications and operations, the two functions are integral rather than having the first overlaid atop the second.

The more information the sensors collect, the less they need send to a central collection point. Radio spectrum is limited (at the megahertz range; gigahertz spectrum is more available but requires more energy to tap) and battery life is precious. A high-definition video image of a scene (which is still far less than a human eye can see) requires 800 megahertz in raw form, and even 20 megahertz in compressed form. Audio input is continuous and also data-intensive. Only anomalies could be reported.

The challenge of distributed sensors is to identify an object by using disaggregated readings. Like neural nets, any such meshes would have to depend on a hierarchy of filtering and analysis. Some readings would be matched against pre-determined patterns. This matching requires that each sensor be able to make partial sense of a partial reading, and that these partial readings can be knit into a probabilistic assessment.

The route between sensing and determination is bound to be complicated. Some sensors -- e.g., a particularly good eye -- might determine a target on its own, but that would be the exception (if nothing else, two eyes are needed to perceive depth for absolute location). Many identifications will be probabilistic based on, say, sightings, heat signatures, sounds, and perhaps chemical emanations. This faculty will be critical when the other employs decoys -- not everything that appears to be a tank actually is one. Because battlefields will always feature new and different objects, sensor processors will have to be capable of some level of logic abstraction. Humans, as multi-sensor creatures, are for that reason very good at identifying objects. However, there is no inherent reason to pack two eyes, two ears, and a nose on every sensor if these functions can be distributed amongst many of them. (Perhaps one needs a hundred eyes as often as one needs ten ears or one nose.)

To coordinate, sensors each would have to talk to one another; their activities would have to respond to what others sense (comparable to moving eyes to follow something). Some of these sensors would have to act primarily as nodal processors, collecting information from other sensors to assess a pattern. These too would have to be proliferated to assured robustness; even higher level nodal functions would, in turn, be scattered throughout the battlefield in lesser densities, and so on down to those communicating directly to humans, off-site coordinators, and/or fire control units.

A key coordination problem among sensors is how to identify themselves upon disbursement. Each must indicate where it has landed, how well it is functioning, and who it is near (and thus will be talking to). Many sensors will die on arrival; others may be incapacitated by virtue of their poor placement. Inevitable gaps in coverage will require that sensors be added, moved around, or converted from one type to another (e.g., we have enough sensors listening to this, listen to that instead). Constant communications would then be needed to determine which sensors still work, which are

silent, and which are phony (digital signature can prevent spoofing but requires that sensors know who their neighbors are). Such communications also would indicate where more coverage is needed.

Vulnerabilities: The most prominent vulnerability of a distributed Mesh is that the links among sensors, emitters, and microprojectiles are key to its operation. Unlike complex platforms which couple their various capabilities internally, capabilities of the Mesh are coupled externally; thus they may be disrupted by what the Soviets called "radio-electronic warfare."

Sensor broadcasts can, in theory, be jammed or faked, just as those from platforms can. Yet, doing so may be harder than it looks. Jamming requires knowing exactly which frequencies are being used, but more important, where signals are coming from. Today's jammers tend to disrupt a signal from one point to another operating in support of a mission (e.g., confound reflections from a large radar meant to be bounced off an incoming bomber). With proliferated sensors, the only effective jamming technique would be to overpower radio signals by jamming continuously in all directions. This technique requires considerable energy--a fact that makes a jammer a highly visible target itself. Besides taking advantage of existing techniques to avoid jamming -- frequency hopping, spread spectrum, extreme directionality -- the Mesh might also use laser communications, acoustic means, hopping on enemy frequencies, or just not communicating for long periods of time. Indeed, frequent among Mesh communications might be the repeated admonishment to stay quiet for a while because the enemy is trying to smoke you out. Thus, no one could be really sure that all emitting elements in would be silenced (or just waiting for the right time to turn on).

Faking the broadcast of a digital emitter is even more difficult. By broadcasting a digital signature, a sensor can simultaneously ascertain that the message is actually coming from the sensor, and that the message received was actually that which was broadcast. (Corrupted messages would be internally inconsistent.) This technique requires that each broadcasting sensor have a unique signature and that each receiving sensor memorize the signature of each broadcasting sensor -- this is a memory burden, but one which becomes easier with every passing year. Moreover, techniques that allow a communicator to sign a message also permit them to send out false messages knowing that they will be ignored but hoping the enemy will, if not listen, then at least waste power jamming on a frequency not being used.

Platforms Against Fire- Ants

The fate of platforms can be illustrated by examining how they might fare against fire-ant elements.

Tanks: Consider the tank as it rolls over terrain littered with sensors and emitters backed by hidden microprojectiles. Such sensors may have arrived hours earlier or they may lie buried for years awaiting a wake-up call. Sensors to search for large ground objects need not be located on the ground. Much of the load may be carried by drones that can broadcast more information than today's models, stay aloft longer, operate more stealthily, and cost less. If costs get enough attention, the deployment of many good drones will be preferred to a few great ones.

An unfriendly tank passing by sensor fields could be brought down in several ways. The most direct solution, if available, is to broadcast the tank's location in real-time to an external missile (or some other fire-control solution). Sensors may also be rigged to take a more direct role. A sensor, for instance, that rides atop a passing tank (much as fleas on passing dogs) can serve as a homing device for an anti-tank round. Of course, it must work quickly before it is detected by the tank's smart skin and removed. Sensors may amble over to a tank's vulnerable parts, then kill it by eating its way through gaskets, fuzing moveable parts (e.g., a powdered aluminum-magnesium burst), befouling its air supply, jamming its electronics, smearing its optics, and so on. The latter methods may well evolve from current research on non-lethal warfare. To wit, the chemicals required to stop a tank without killing its crew may be far more compact and thus efficient than those required to blow it up.

Planes: Today's aircraft are optimized - - at great expense -- to win one-on-one (or one-on-not-too-many) duels against other aircraft and anti-aircraft ground units. The fate of fifty million dollars' worth of aircraft (roughly one) contesting fifty million dollars' worth of loitering sensors, emitters, microprojectiles may be far less satisfying.

An air-borne sensor screen might contain thousands of nasty objects that may collectively cue firing units in real-time by announcing a target's location and bearing, illuminating it with spattered chemicals, or by bouncing radar on it. Alternatively, if such objects exploded a rain of carbon

fibers or ceramic shards, they could take down the aircraft's engines on their own.

Although current technologies do not allow objects to loiter in the air very cheaply (helium balloons aside), today's drones can stay aloft for two weeks. A typical floater may, in a few decades, be the size and shape of a handkerchief, powered by a coat of photovoltaic paint, and girded by a semi-rigid skeleton acting as both antenna and air-sail. Its sensors and processors, no larger than fingernails, would allow it to sense wind movements and configure itself to bob up and down accordingly. Upon detecting hostile aircraft, it so signals to fire-control units or tries to get itself and thousands of its friends to find their way softly into the aircrafts' engines. To friendly aircraft, it sends what it knows about the not-so-friendly skies and otherwise gets out of its way. These floaters need not be stealthy; when deployed in the millions, they will simply be beyond the capability of anything to shoot down.

Ships: The same problem of coping with scads of hostile objects would also bedevil ships and submarines. The elements of a Naval mesh are presaged by sonobuoys -- cheap sensors routinely produced in the hundreds of thousands today. Lower power requirements, more efficient batteries, and perhaps tethered photo-voltaic collectors will give future versions longer lives. They will also be able to sense better, process more information themselves, and communicate both with their peers (vice overhead aircraft) and associated floating torpedoes. They may even be armed and could maneuver to where ships are most vulnerable. Anti-submarine aircraft squadrons will be used only for initial distribution. If sonobuoys can loiter for years until activated, a much smaller fleet of them could handled even this task.

Naval meshes might be supported by fleets of robotic submersibles -- perhaps just very large torpedoes -- that can chase fast or stealthy targets into heavily mined waters. To protect themselves, ships and submarines would have to physically sweep large stretches of sea before them. They may need a layered net swept fore and aft to a distance of several miles. This would slow them down considerably and reduce their efficacy in a power projection role.

Space: Tomorrow's space forces will combine very high earth orbiters with large fleets of very low earth orbiters. Their tasks will, however, be the same ones they carry out today: communications, observation, navigation.

One shift will be from strategic to tactical uses of surveillance (already being developed in the TENCAP program). To support targeting and treaty compliance, strategic surveillance needs very detailed pictures (e.g., 10 cm resolution) of compact spaces looking for installations that rarely move. Tactical surveillance, although it can use the detail, needs more real-time information. Coverage also needs to be wider because, in a typical tactical scenario (e.g., Bosnia) the field of action is not fixed; it can move quickly and unpredictably. Today's needs for wide-area coverage - - looking for certain high-energy events like the launch of a SCUD missile, for example -- are met by large satellites in geosynchronous orbit. At forty thousand kilometers up, such orbiters are usually too distant to localize such events precisely. Tactical operations need much denser coverage, and probably from much closer.

Large earth orbiters are also vulnerable to anti- satellite systems no better than those the United States demonstrated off the wings of an F-15 in the middle 1980s. Eventually, large earth orbiters will prove nearly impossible to hide because they are hard to camouflage against an earth background. Since every one must cross the equator fifteen times a day, constant searching can be confined to a small equatorial band. From a higher equatorial orbit, precise optics coupled with powerful on-board processing would make a first sighting inevitable. The movement of satellites, once spotted, can be predicted with great accuracy. Satellites that use energy to jerk into unpredictable orbits would emit characteristic energy plumes that would instantly cue seekers to the orbital path. Under such circumstances, a spacecraft would be hard put to get more than one or two passes over the battlefield before being targeted and destroyed.

Hence the watchwords will be to fly high (and thus get lost in far vaster reaches) or fly small and dense. The logic of space dominance would require getting the most capability into orbit the fastest and protecting it there against attack the longest. This capability would provide short-term tactical advantages at precisely the right moment. Satellites made small and cheap enough could proliferate and thus make their complete destruction complicated. Surveillance satellites might therefore survive better in the aggregate. Weapons satellites (if not forbidden by current treaties) might not

-- due to the added size and weight of a platforms required to carry a minimally effective warhead.

Continuous real-time coverage from space would remain unfeasible until satellites become far cheaper. The best look comes from orbiting 400km high (below which atmospheric drag pulls satellites back to earth, and above which complicates the optics problem). From there, a 30- degree field of view to each side yields a 400km swatch but requires 4000 birds (90 birds per each of 45 orbits) to maintain continuous coverage (between the north and south 60-degree parallels). Affording this fleet within a feasible \$20 billion investment budget would require that each bird and shot be less than \$5 million. Split 50:50 (assuming \$6000 per pound. to low-earth orbit) suggests that each satellite cost less than \$2,500,000 and weigh less than 400kg.

The data burden from such a system is big. To picture everything in the world in one meter resolution with 8-bit detail requires roughly 1,500 terabits. If each point is shot once a minute, a total send rate of 3,000 gigabits/second is required. Even with 10:1 image compression and 4000 satellites, each bird must broadcast 600 megabits per second (roughly equivalent to thirty TV signals). Further reduction is possible by sending only the difference between the actual and expected image, although this requires each bird to store 18,000 gigabytes (150 terabits) of image per bird - free silicon in the extreme. If the resolution doubles, the data collected must rise fourfold. Staring satellites can cover known swathes more efficiently, but successful use of the technique assumes the area covered is significantly smaller than Bosnia. Longer revisit times return us to the current system, which is unusable for real-time operations.

Looking up rather than down, denser information technology makes it easier to construct a functioning ballistic missile defense. A dense enough sensor system should be able to track missiles, which must be large (if they are to hold nuclear weapons) and fly against a fairly clear background. Destroying the missile once it is found, is considered the lesser half of the problem.

Broader Implications

By changing the conduct of war, the Mesh changes its nature as well. It raises serious questions about human command, affects the pace of conflict, and blurs the distinction between civilian and military on the battlefield.

Human Control: Current leitmotifs of information warfare suggest that because militaries possess a command core linked to field armies by command and control networks, killing the core leads to cheap victory. Yet advances in information technologies may mean that the core need not sit in any one location. Teleconferencing, for example, permits a command center to occupy dispersed locations. The core data base can be duplicated in many locations (or can be built as an distributed system to begin with).

Human command would also evolve. Information technology permits greater centralization -- because better telecommunications increase the amount of data that can be sent to core. However, it also permits greater decentralization -- because better computation allows units to handle more data from colleagues. Tomorrow's military systems will do both. Headquarters will be able to do more detailed unit control, but units will be able to undertake more functions in degraded communications environments.

Meshes could be engineered to take humans out of many decision loops. Complete removal from the loop is possible. Yet, a technology which *permits* less human oversight need not *compel* it. The bogeyman of an automated war machine will be no greater than it is today. As it is, many existing weapons lack call-back mechanisms. Most mines, for instance, have no man-in-the-loop between detection and explosion. Once a ship's close-in weapons system is turned on, its choice of targets is determined automatically. How different are a strategic ballistic missile that leaves human control once launched and a loitering cruise missile that searches for and destroys a target on its own?

Could fire-ant systems elude human control altogether? Hollywood likes making movies such as *Fail-Safe*, *Dr. Strangelove*, *War Games*, and *Terminator 2* that show strategic systems going autonomous. Accidental system autonomy in conventional systems is a lesser problem because they contain multiple decision points and do not have to make all decisions at once. Regardless of how complex the software, the inclusion of enough if-maybe-then-stop locks can limit the risks. An adversary may, however,

establish a doomsday ant- mesh system -- but these concerns are not new; they have been familiar grist to nuclear theologians for decades.

In a battlefield in which machines command others, foot soldiers -- whose relative ranks have been dwindling for a few hundred years -- may be the only humans left. Platforms already dominate low-density environments such as air, sea, plains, and deserts with their ample running room; these platforms, in turn will be supplanted by the Mesh. High-density environments such as cities, jungles, and mountains remain the preserve of the foot soldier; the Mesh will take over much more slowly in such realms. Foot soldiers can still benefit from technology. Helmets, for instance, may house cellular radio receivers, IFFN transponders, video display terminals embedded in pull-down visors, and computers. The latter would coordinate sensor inputs, generate tactical assessments of battlefield conditions, and transmit maps. Passwords or biological markers could ensure that only the owner be able to use them. The individual soldier could thus be made part of the military Mesh (as well as the commercial Net).

The Pace of Conflict: The Mesh may be tomorrow's version of what the Maginot line was supposed to be, a barrier through which no platform can transit without being detected and destroyed. The Maginot line -- despite its subsequent reputation -- succeeded where it was placed. Unfortunately, because it cost so much to build, France was unable to finish it, and Germany ran around it to the south. Mesh warfare favors defense. However, unlike the technology of World War I, which also favored the defense, in the next century each side will be able to bombard the other's civilian infrastructure with relative ease. Thus, it will be possible to destroy an opponent's above-the-ground civilization without being able to occupy its territory.

Conflict may then resemble siege warfare--perhaps even mutual siege warfare. The same *cordon sanitaire* technology that can protect a state against invasion can be used by invaders to blockade defenders. Offensive siege operations are a highly unsatisfactory way of going about war for all the usual reasons: they are slow, uncertain, and hurt the powerless while the powerful can claim scarce resources for their own ends. Iraq's experience after the Gulf War is a good example. Long-term maintenance is also a problem. In the 21st century, how long might technology allow a besieged party to endure a total blockade? Would modern polities have the patience or stomach to maintain sieges over years, as the besieged project pitiful images

of their victims? Would technology let the besieger blockade such electronic communications or douse the besieged with messages of panic or despair? If such sieges prove impossible -- societies always prove surprisingly resilient against aerial attack -- what other techniques would be available to contain aggressors one could not destroy?

Mesh warfare could simultaneously be faster and slower than current conventional warfare. Compared to the several months the United States needed to deploy to the Gulf, a mesh could be laid down in several hours. A heavy lifter could transit over the affected area, dispersing large quantities of sensors, emitters, microbots, and miniprojectiles. Upon landing, they would automatically configure themselves into a coordinated network. Some countries may leave heavy lifters on runways for precisely such contingencies. Perhaps the United States could protect a future Kuwait upon first hearing that it had been invaded, although such a policy would not be an unalloyed plus. The ability to promise quick commitments may deprive decisionmakers of the time needed to contemplate the long-run consequences of such decisions. National leaders could regret not leaving erstwhile allies to their own devices.

If both sides tried to set up meshes at the same time, would the race be destabilizing? Provided both mined inside their borders, setting up a fence might, at worst, compel an opponent to set up its. Often, however, such distinctions are not so pat. One party's fence may include disputed or third-party territory. Many collectors see over boundaries: airborne sensors can enjoy a 300km line of sight; sensitive seismic or acoustic sensors can monitor the entire world. Establishing the space component of the Mesh may also induce conflict particularly if the first up can prevent the second from getting up. World War I was supposedly accelerated by the competition among various countries to mobilize their troops at the border before the other side could. Once the trains, with their rigid timetables, started moving, momentum moved with them to war.

While a Mesh may be built quickly, its operation may retard war considerably. A recent RAND study argued that a squadron of B-2 bombers could destroy an invading armored column in the open. Knowing this, what country would be foolish enough to afford us such opportunity? Instead, unless an invasion could be completed in a few hours, a conventional invasion force opposing a high-information opponent would want to do so very gingerly, with methods similar to those submarine warfare. The

Achilles heel in any information system is the extent to which it can be spoofed -- a constant throughout military history. An effective strategy would have to combine false negatives (sneaking through untouched) and false positives (decoys). Some methods work better than others. To find a tank requires looking for a correlation among as many parameters as possible. Yet finders must be flexible to see that if something looks like a tank, walks like a tank, quacks like a tank, but does not smell like a tank, it may nevertheless be a tank. Conversely, a decoy does not have to simulate a tank in every respect to be classified as one -- just in all features considered important by the other side. It may require many decoys to find which parameters the opposing software deems important and thus uses for target identification. All this assumes, of course, that in an attrition conflict one can trade decoys for missiles and still emerge on top. Conversely, a Mesh may let a few tanks by to hide its true parameters. For these reasons, the offense will want to move very slowly while searching for weak spots in the system.

Another technique may take advantage of the fact that the ability to transmit information among many of the nodes may be limited by the small amount of spectrum they each have. Thus a strategy of flooding certain nodes with information may degrade the system. In a poorly engineered system, relevant signature information will be randomly dropped. Even in the best engineered system, concentrating on the important data will force the less highly ranked but still threat-defining data flows to be dropped. Either way, the defense deteriorates. However, determining the information architecture of the other side's Mesh to know exactly where it is weak is anything but easy.

It is not clear how one side's Mesh would combat another side's Mesh. Most sensors and miniprojectiles would not only be small, and at least partially buried, but quiet as well; they would be listening much and transmitting rarely. Might hunter-killer microbots be developed to search out and destroy their opposing numbers? Both the difficulty of the likely terrain and their slow speed suggest that such an effort would be extremely drawn out. Confirming that an area is safe is even harder, particularly if the Mesh lets a few items through as a trick.

Economics may also inhibit an ant-on-ant warfare strategy. By virtue of their mobility and additional sensors, hunter-killer ants are bound to be more expensive than their more passive victims. If the hunter-killers have to get close to passive sensors to find them, then a certain percentage of the victims

could be mined to blow up upon being jostled by a hunter-killer. At some percentage those employing hunter-killers must expend more resources than they disable. Killing from afar could easily require armament that is more expensive than the individual sensors themselves, and so on.

Civilian as Military: Mesh warfare not only makes it hard to keep platforms alive on the battlefield, but complicates the task of getting them anywhere near it. Logistics assets, notably airlift, sealift, and prepositioned supplies, are among the largest and slowest of military assets. The difficulty of getting there against an opposing Mesh should be of particular concern for the United States and others who help allies by projecting power over large distances.

Because, paradoxically, lift assets are among the most civilianized of military assets, the solution to the lift problem may be to consciously imitate civilian assets until very close to theater. A ship used to carry war material for West Island would be indistinguishable from one used to carry commerce to East Island. At some point its destination would be obvious, but by then, it might have already passed its load of sensors and emitters to where needed. East Island could counter this strategy by explicitly granting a digital signature to specific ships, planes, and messages it selects for its own trade. It is not clear whether other nations would cooperate in setting up an IFFN tracking system with a nation that attacks world commerce. Otherwise, East Island would have difficulty isolating West Island from military help without isolating itself from the commercial world it was increasingly networked to.

Wars are not just contests. Removing all platforms -- and thus those who man them -- from the field of war would not make war safe for everyone, but the opposite. If Meshes promote siege warfare or the civilianizing of military assets, then the distinction between military and civilian erodes to the great detriment of the latter -- a reminder, again, that not every advance in the art of war is tantamount to an advance in civilization.

Conclusions

Regardless of how the many implications of pop-up warfare, fire-ant warfare or the Mesh play out, one conclusion is inescapable. The days of the platform as the king of the battlefield are drawing nigh. With its eventual

demise comes a similar demise of organizations built around such platforms and the systems used in acquiring them.