# The Information Revolution and Post-Modern Warfare

by Steven Metz via rialator *Tuesday, Aug 29 2006, 6:08pm*
international / peace/war / opinion/analysis

**Armed Conflict in the 21st Century:**

Continued ....Part 3

ASYMMETRY AGAIN.

The notion that 21st century warfare will pit an omniscient postmodern U.S. military in lop-sided, lightning operations against 'evil' aggressors is enticing. But is it accurate? Perhaps, particularly in those instances where an aggressor does not expect American involvement. There may be times when the United States surprises an aggressor using Soviet-style equipment, tactics, and operations. Such wars would be a reprise of Desert Storm. Opponents who do anticipate and plan for American involvement, though, are likely to attempt to counter the prowess of the U.S. military through asymmetric means.

To some extent, current official thinking recognizes this. In fact, asymmetry has become a central concept in official American thinking about future warfare. While Joint Vision 2010, which was released in 1996, does not explicitly mention asymmetry or asymmetric counters, all key planning documents now do. The Air Forces' Global Engagement notes that "hostile countries and non-state actors [will] seek asymmetric means to challenge US military superiority"; the 1998 Annual Report of the Army After Next Project contends that "major competitors will probably develop creative asymmetric strategies"; and the 1999 Joint Strategic Review provides an in-depth analysis of the implications of asymmetric methods.

The reason is fairly simple: the Gulf War seemed to show that the United States cannot be defeated by conventional Soviet-style methods. If anything, the gap between the American military and opponents who might attempt force-on-force combat in open terrain is growing. No potential enemy will soon undergo an information-based revolution in military affairs and develop a postmodern force.

But enemies still feel the need to challenge the United States or, at least, to make themselves impervious to American intervention. The question then becomes: what forms of asymmetry will be most common and, more importantly, most problematic for the United States? Enemies using precision munitions or weapons of mass destruction to complicate deployment into a theatre of operations could pose a serious challenge to some of the most basic tenets of American strategy.

Since the campaigns of Ulysses Grant and William Sherman, the "American way of war" has called for the build-up of massive amounts of materiel and supplies in a theatre of operations, and then the use of this material advantage to attain decisive victory through a strategy of annihilation. This is contingent on the enemy's absence of effective power projection to strike at the rear bases.

In the American Civil War, the Confederacy simply did not have the force necessary to capture Union depots at places like City Point, Virginia. In the European theatre of World War II, the English Channel, the Royal Air Force, and the Royal Navy kept the rear bases safe until adequate American forces were deployed. And, in the Gulf War, American airpower and landpower protected the rear bases.

In a future where enemies have some precision guided munitions and weapons of mass destruction (along with delivery systems), in-theatre sanctuaries may not exist. Even air superiority and theatre missile defence would be inadequate against a nuclear-armed enemy, since they cannot assure the sort of 100 percent effectiveness that is necessary. Given this, the future American military may confront an enemy using a counter-deployment strategy in which precision guided munitions and ballistic missiles, whether with nuclear, biological, and chemical warheads or conventional ones, are used to attack U.S. bases and staging areas both in the United States and in a theatre of operations, and to threaten states that provide support, bases, staging areas, or overflight rights to the United States.

An enemy using a counter-deployment strategy would have to be met with a combination of strategic airpower, naval strike forces, theatre air superiority, theatre missile defence, focused logistics to minimize the supplies needed in theatre, and a range of methods to limit the need for a lengthy build-up of forces, equipment, and supplies. As the 1997 National Defence Panel wrote, “The days of the six-month build-up and secure, large, rear-area bases are almost certainly gone forever. WMD will require us to increase dramatically the means to project lethal power from extended ranges.” The capacity to deploy forces and resupply them directly from the continental United States into a theatre of operations could prove invaluable, minimizing the chances that states in the theatre of operations could be coerced into denying U.S. forward bases or staging areas.

The need to protect U.S. forces from strikes launched by an enemy using a counter-deployment strategy suggests the need for what might be called “theatre reconfiguration areas” rather than traditional fixed bases. Such theatre reconfiguration areas could be located in remote areas of nations, which agree to host them, with a landing strip as the only fixed part of the base. All of the other things needed to prepare equipment and troops for combat could be mobile, concentrating just before an inbound aerial convoy arrived and dispersing as soon as it left. The inventory of supplies at a theatre reconfiguration area would be kept to a minimum, and replenished only as necessary. Repair and hospital facilities would also be mobile and dispersed.

Theatre reconfiguration areas could be protected by conventional concealment methods, electronic masking, and a laser-based missile and air-defence web combining ground-based fire platforms, long-loiter and quick-launch UAV fire platforms, and space-based sensor and fire platforms. Autonomous sentry systems which fall somewhere between a full-fledged robot and a 21st century mobile, smart mine could provide local security. Host-nation support would be kept to a minimum to protect operational security. To complicate targeting by enemies, several decoy theatre reconfiguration areas could be set up in each country that allowed them. Such a “shell game” could provide effective deception and thus complicate any attempts to strike at the theatre reconfiguration areas with missiles.

A counter-deployment strategy is only one of several asymmetric approaches that future enemies may attempt. They might also resort to terrorism, either in conjunction with a counter-deployment strategy or in lieu of it, to deter American involvement in a regional conflict. In an era when weapons of mass destruction are becoming more common, the terrorism problem is so pressing that some security analysts have begun advocating a retrenchment from global activism is order to lower the chances of provoking terrorism.

It may eventually come to that. In lieu of retrenchment, countering an enemy relying on terrorism would require a three part strategy. The first would be to make terrorist attacks more difficult by effective intelligence and by the further hardening of targets. Clearly emerging information technology, including new forms of sensors and new methods for transforming sensor data into usable intelligence, provide part of the solution.

The second part would be to institute a policy stating terrorist strikes against the American homeland will provoke a declaration of war against those who use terrorism or sponsor it. Such an approach is a traditional part of war. World War I, after all, began by Serbian sponsorship of terrorism against the Austro-Hungarian Empire. Future sponsors of terrorists—whether the Taliban regime in Afghanistan, Iran, Libya, or some new one—should know that they are performing an act of war and pay accordingly.

The third part would be to assure that if the American homeland is struck by terrorism, the result is public support for effective action against the perpetrators rather than disengagement from the conflict that first led to the problem. Of all forms of asymmetry, urban warfare may be the most problematic and the most likely. In 1996 Ralph Peters wrote, "The future of warfare lies in the streets, sewers, high-rise buildings, industrial parks, and the sprawl of houses, shacks, and shelters that form the broken cities of our world... in the next century, in an uncontrollably urbanizing world, we will not be able to avoid urban deployments short of war and even full-scale city combat." But as Thomas Ricks notes, urban warfare is one arena where the innovation associated with the revolution in military affairs so far "hasn't helped."

Even the General Accounting Office has noted the inability of the U.S. military to conduct urban operations. Admittedly, few military activities are more difficult than combat in a modern city. Major General Robert H. Scales writes:

A large urban center is multi-dimensional. Soldiers must contend with subterranean and high-rise threats. Every building could be a nest of fortified enemy positions that would have to be dug out, one by one. Moreover, an experienced enemy could easily create connecting positions between buildings.

With limited manoeuvering space, the urban environment precludes mobility operation and largely negates the effects of weapons, while minimizing engagement ranges. The proximity of buildings plays havoc with communications, further adding to command and control difficulties. Finally, the psychological effects of combat on soldiers are magnified. While the array of threats from multiple dimensions has a debilitating effect on soldiers, it further hastens the disintegration process that haunts all military units locked in close-combat operations.

Such fighting involves six key dilemmas: (1) coordination among military units is complicated by separation into small units and by the fact that tall buildings can limit the range of radio signals; (2) it is slow and tedious, nullifying the advantage in manoeuvre and decisional speed that an advanced military has over less-advanced opponents; (3) it is difficult to distinguish combatants and non-combatants; (4) the battlefield is often thick with non-combatants; (5) holding control of an area is often more difficult than the initial clearing, since enemy troops may reinfiltrate; and (6) since cities are concentrations of communications and information links, operations there will be transparent, broadcast around the world by a variety of means from cell phones to web cams linked to satellite modems.

In combination these dilemmas pose an extraordinarily thorny problem. There are actually three different types of operations that the U.S. military might have to perform in urban areas: policing, raids, and sustained combat. Of these, sustained combat is the hardest. As the 1997 report of the National Defence Panel phrased it, "Urban control—the requirement to control activities in the urban environment—will be difficult enough. Eviction operations—the requirement to root out enemy forces from their urban strongholds—will be even more challenging.”

Part of the solution is better doctrine, training, and rules of engagement. The U.S. Marine Corps is far ahead of the other services in this arena. In their Urban Warrior experiment, which took place in Oakland, California in 1999, the Marines explored the utility of existing technology like palm-held computers, unmanned aerial vehicles and parachutes steered by the Global Positioning System in an urban battle. At the same time, the Marines are exploring different ways of organizing units involved in urban combat, particularly less hierarchical, more networked structures. During military revolutions, organizational and conceptual change is nearly always more difficult than the adoption of new technology. This certainly holds for urban combat. Joel Garreau notes, “An electronic network may give the Marines unprecedented flexibility, adaptability and competitiveness, but it may also fundamentally unravel the way the Marines have worked for more than 200 years.”

Even existing technology is inadequate for urban operations. Two types of technology, though, might help alleviate some of the challenges: non-lethal weapons and robotics. The utility of stand-off, lethal strikes, even if they are substantially more precise than those available today, will remain limited in urban warfare. City fighting involves close combat, often in the presence of non-combatants. Non-lethal capabilities might enable the U.S. military to overcome enemy forces from urban environments with minimal civilian casualties and limited risk to American forces.

If non-lethal weapons were developed which could temporarily incapacitate people, separating combatants and non-combatants would entail much less risk to U.S. forces. To hold areas already cleared, non-lethal weapons could limit the risk to U.S. soldiers on sentry duty and lessen the chances that non-combatants wandering through cleared areas would be harmed. For refugee control—which is a vital but often overlooked dimension of urban combat—non-lethals could help stop riots and assist U.S. forces in dealing with any combatants who attempted to hide among refugees.

An Army-sponsored workshop at the Jet Propulsion Laboratory, which brought together military professionals and robotics experts, was prescient when it noted that robots hold particular promise for information gathering, the highest priority mission in urban combat operations.

Satellites and overhead sensors can never provide the sort of dynamic, three-dimensional picture necessary for urban operations. Robotics have the potential to offer the horizontal perspective to augment overhead sensors. In addition, robotics can form part of a dynamic perimeter” to guard prisoners and prevent the re-infiltration of cleared areas.

The most useful way of penetrating enemy controlled areas might be through networks of very small but relatively low resolution robotic sensors, with a full intelligence picture developed through data fusion. The utility of robotic systems is almost endless. In armed conflict they could not only perform reconnaissance functions but also serve as mine detectors and sweepers, smoke or other obscurant dispensers, obstacle deployers or breachers, communication relays, target designators, decoys, ambulances, logistics “mules,” mobile shields, or offensive strike systems.

Scientists also predict that coming decades will bring a biomechanical revolution as engineering devices are blended with organic ones, thus leading to various types of cyborgs. In early 2000, scientists combined a human cell with an electronic circuitry chip. By controlling the chip with a computer, scientists say they can control the activity of the cell. The computer sends electrical impulses to the cell-chip, triggering the cell’s membrane pores to open and activating the cell. Scientists hope they can manufacture cell-chips in large numbers and insert them into the body to replace or correct diseased tissues.

From a military perspective, such cyborg platforms may be easier to field than purely mechanical robots. For instance, scientists note that it will be several decades before robots the size of cockroaches will have the mobility of cockroaches, but substantial progress has been made in implanting devices in living cockroaches which allows them to be "steered." In future urban warfare, sensory-carrying cockroaches may be maneuvered by soldiers thus providing information dominance.

Broadly speaking, the opening decades of the 21st century will see both symmetric formal war pitting two modern states, and asymmetric formal war pitting a postmodern military against a modern one. There will be reprises of both the Iran-Iraq War and the Gulf War. In the former, the United States may become indirectly involved, providing support of one kind or the other to an ally. As more and more nations acquire nuclear weapons, formal war between them may come to look more like the India-Pakistan war of 1999 than the Iran-Iraq War.

Combatants may launch a few limited conventional strikes and perhaps some cyberattacks, but rely primarily on proxy aggression to remain below the threshold of either massive retaliation by their opponent or economic and political pressure from the rest of the world. It remains to be seen whether another postmodern military will emerge to challenge the United States or whether, as American strategic thinking posits, the postmodern U.S. military will always be able to overcome the asymmetric methods used by modern militaries.

## INFORMAL WAR.

Informal war is armed conflict where at least one of the antagonists is a non-state entity such as an insurgent army or ethnic militia. It is the descendent of what became known as low intensity conflict in the 1980s. Like today, future informal war will be based on some combination of ethnicity, race, regionalism, economics, personality, and ideology. Often ambitious and unscrupulous leaders will use ethnicity, race, and religion to mobilize support for what is essentially a quest for personal power.

The objectives in informal war may be autonomy, separation, outright control of the state, a change of policy, control of resources, or, "justice" as defined by those who use force. Informal war will grow from the culture of violence, which has spread around the world in past decades, flowing from endemic conflict, crime, the drug trade, the proliferation of weapons, and the trivialization of violence through popular culture. In many parts of the world, violence has become routine. Whole generations now see it as normal. To take one example, Debbie Stothard, an expert on refugees who campaigns for democracy in Myanmar, said of the guerrilla groups there:

> These are people who have not had access to a good education and for whom violence is a way of life. It never occurs to them that mounting a siege on a hospital is actually wrong. They have not lived in a world where detaining someone with force is actually unacceptable. It's as though they came from a different planet . . . This is not an isolated case. In Latin America, the Middle East, South Asia, Central Asia, Sub-Saharan Africa and, to some extent, the inner cities of the United States, a culture of violence has become so pervasive that it is impossible to quell.

In this setting, informal war will remain common, in part because of the declining effectiveness of states. Traditionally, governments could preserve internal order by rewarding regions or groups of society, which supported the government, punishing those that did not, and, with wise leadership, pre-empting conflict and violence through economic development. In a globalised economy, the ability of governments to control and manipulate the economy is diminished, thus taking away one of their prime tools for quelling dissent and rewarding support. In regions where the state was inherently weak, many nations have large areas of territory beyond the control of the government. And, as political, economic, and military factors constrain traditional cross border invasion, proxy aggression has become a more attractive strategic option.

Regimes unwilling to suffer the sanctions and opprobrium that results from invading one's neighbours find that supporting the enemies of one's neighbours is often overlooked. This is not likely to change in coming decades. Finally, the combination of globalisation and the Cold War have fuelled the growth of an international arms market at the same time that the international drug traffic and the coalescence of international criminal networks have provided sources of income for insurgents, terrorists, and militias. With enough money, anyone can equip a powerful military force. With a willingness to use crime, nearly anyone can generate enough money. Informal war is not only more common than in the past, but also more strategically significant.

This is true, in part, because of the rarity of formal war but also because of interconnectedness. What Martin Libicki calls "the globalisation of perception"—the ability of people to know what is happening everywhere—means that obscure conflicts can become headline news. There are no backwaters any more. As suffering is broadcast around the world, calls mount for intervention of one sort or the other. Groups engaged in informal war use personal and technological interconnectedness to publicize their cause, building bridges with a web of organizations and institutions.

The Zapatista movement in southern Mexico is a model for this process. The Zapatistas, in conjunction with a plethora of left-leaning Latin Americanists and human rights organizations, used of the Internet to build international support with web pages housed on servers at places like the University of California, Swarthmore, and the University of Texas. This electronic coalition building was so sophisticated that a group of researchers from the RAND Corporation labelled it "social netwar." Undoubtedly, more organisations will follow this path, blending the expertise of traditional political movements with the cutting-edge advertising and marketing techniques that the information revolution has spawned.

During the Cold War the strategic significance of low intensity conflicts was determined by their potential to spark superpower confrontation or to escalate into wider fighting. Today and in coming decades, strategic significance of informal wars will be determined both by their potential for contagion through refugee flows or terrorism, and by the global image of them which coalesces or is created, whether by participants or other interested parties. A defining feature of the information revolution is that perception matters as much as tangible things. This will certainly hold for informal warfare. Future strategists will find that crafting an "image assessment" or "perception map" of a conflict will be a central part of their planning. While 20th century military strategists like Eisenhower and Marshall took their cues from industrial management, 21st century military strategists must learn from the advertising and marketing industries.

Combat in future informal war is likely to remain "hands on," pitting the combatants in close combat. In many cases, fighting will take place in heavily populated areas. Warriors will be interspersed among non-combatants, using them as shields and bargaining chips. At times, refugee disasters will be deliberately stoked and sustained to attract outside attention and intervention. Informal wars will also be the kind where passion—that most dangerous element of Clausewitz's trinity—plays the greatest role. Unlike formal war, where the trends are toward precision and depersonalisation through stand-off capabilities, informal war will remain dirty and bloody, driven by hatred more than science.

In failed states, informal war may be symmetric as militias, brigand bands, and warlord armies fight each other. At other times, it may be asymmetric as state militaries, perhaps with outside assistance, fight against insurgents, militias, brigands, or warlord armies. For the United States, the asymmetric form will be especially important since the American military may be asked to support friendly regimes, contribute to multinational intervention forces, provide humanitarian relief, or even participate in direct combat. This might involve stability operations where U.S. forces, in conjunction with allies, will seek to restore order or facilitate humanitarian relief, and then turn over responsibility for long-term amelioration of the conflict to some other agency or organization.

In all probability, multinational mechanisms for the reestablishment of stability and for conflict resolution will grow and improve in coming years. Quite possibly, this will be the major task of the United Nations. Quick operations to restore stability will be taxing but feasible.

Counterinsurgency, which uses military forces to attain not only the short-term restoration of order but also ultimate resolution of the conflict that led to disorder in the first place, is a different and more difficult matter. It involves long-term engagement and alteration of a country's political, economic, security, and even social order. Current American thinking on the security environment and military strategy discounts insurgency and counterinsurgency.

Ten years ago they received a moderate amount of thinking in doctrine and strategy: now they are largely ignored. If insurgency is defined solely as rural leftist warfare—its most common and successful variant from the 1940s to the 1990s—then it might make sense to relegate it to history. Maoist "peoples war" is unlikely to pose serious problems in the 21st century. But if insurgency is seen more broadly as protracted, asymmetric warfare waged by an organization with a strategic perspective, then the chances are that it will mutate, re-emerge and pose challenges to American allies in coming decades. Just as in the 1960s and 1980s, the future U.S. military will have to rediscover counterinsurgency and relearn the lessons of the past.

As external sponsors have faded away and state militaries began to understand Maoist people's war, the chances of it working declined. Future insurgents will have to develop new strategies. Every insurgent strategy must have three components: a method for defending the movement against government security forces; a method of raising support; and, a method of attaining ultimate success.

In Maoist people's war, insurgent movements defended themselves by tactical dispersion, interspersion among non-combatants, the use of complex terrain such as jungles, mountains, or cities, high internal morale, and effective intelligence and counterintelligence. They supported themselves by using political and psychological means to mobilize internal backers, by taxing citizens and businesses in "liberated" or semi-liberated zones, by capturing arms and supplies from security forces, and by external patronage, whether from a state like the Soviet Union, Cuba, China, and Libya, or a network of ideological allies like a diaspora community (e.g., the Malaysian communists raised money from Chinese communities throughout the Asia-Pacific region, Irish insurgents have used their ethnic brothers in the United States, and so forth). Finally, old-style insurgents sought success by exhausting the government, weakening it through guerrilla war, terrorism, and political warfare, and simply outlasting it.

Future insurgents would need to perform the same functions of defence, support, and the pursuit of victory, but will find new ways to do so. In terms of defence, dispersion is likely to be strategic as well as tactical. There will be few sanctuaries for insurgent headquarters in an era of global linkages, pervasive sensor webs, and standoff weapons, so astute insurgents will spread their command and control apparatus around the world. Information technology will make this feasible.

Right wing anti-government theorists in the United States have already developed a concept they call “leaderless resistance” in which disassociated terrorists work toward a common goal and become aware of each other’s actions through media publicity. The information revolution will provide the opportunity for “virtual leadership” of insurgencies which do not choose the anarchical path of “leaderless resistance.” Mao Zedong, Ho Chi Minh, Pol Pot, Daniel Ortega, Jonas Savimbi, Fidel Castro and other 20th century insurgent leaders needed physical proximity to their top lieutenants.

Twenty-first century insurgent commanders will be able to exert at least a reasonable degree of control from a lap top computer with a satellite modem and web cam situated anywhere in the world, with their transmissions encrypted and bounced throughout the web in order to complicate tracing. The top leadership might never be in the same physical location. The organization itself is likely to be highly decentralized with specialized nodes for key functions like combat operations, terrorism, fund raising, intelligence, and political warfare.

In many cases, insurgent networks will themselves be part of a broader global network unified by opposition to the existing political and economic order. For instance, an insurgent network attempting to overthrow the government of a state friendly to the United States might cultivate loose ties with a range of titular allies including global criminal cartels, anti-government groups within the United States, or other political groups seeking to constrain American power. Unless some sort of new ideological division emerges among the world’s great powers—which is not inconceivable—future insurgents will be unlikely to find state sponsors. The trend will be toward “stand alone” insurgent movements that rely on the open market.

Because of this, the revenue-generating node of an insurgent movement will be one of the most important. This commercialization of insurgency has been underway ever since the end of the Cold War cut off ideological patronage. In Colombia, Peru, Kosovo, and other areas, insurgents have found drug trafficking a lucrative source of income. In Sierra Leone and Angola, it is diamond smuggling. But reliance on a single source of income is a vulnerability. Future insurgents may be diversified in their fund-raising methods, using cybercrime as well as traditional methods like extortion, robbery, kidnapping, smuggling, and drug trafficking.

They might even move into legitimate commercial ventures, undertake fund-raising among “like thinking” organizations around the world (making heavy use of the Internet), and “tax” co-ethnic diasporas. Money will allow future insurgents to contract out key functions such as fundraising, intelligence and, perhaps, even direct military action. Well-financed insurgents will be able to buy the state-of-the-art talent in key areas like information security or offensive information warfare, thus making them equal or superior to the security forces confronting them. And by contracting out their armed actions, they will lessen the risk to themselves.

Countering new style insurgency will not be easy. There is no formal doctrine for dealing with networked opponents, be they existing criminal cartels or future insurgents. To be successful against future insurgents, the U.S. military will need better intelligence, better force protection, and greater precision at the tactical and strategic levels. In part, these things require new organizational methods. For instance, John Arquilla and David Ronfeldt contend that to match networked opponents, governments must develop network/hierarchy hybrids like those taking shape in the corporate world. The American military also must refine its conceptual tool kit. Ideas like phased operations and centres of gravity, which originated in response to industrial age warfare against hierarchical enemies, will provide little insight into dealing with networked ones.

Emerging technology also holds promise. Again, non-lethal weapons and robotics may prove the most vital. Robotic sensor webs could help with intelligence collection, which is always one of the most difficult and most vital aspects of counterinsurgency. With better intelligence, greater precision becomes possible. It might be possible, for instance, to identify and neutralize insurgent leaders with little or no collateral damage or civilian casualties. Removing insurgent leaders does not automatically lead to victory: that requires amelioration of the tensions that opened the way for the insurgency in the first place. But solving root causes is certainly easier with insurgent leaders and cadre out of the way. Non-lethal weapons and robotics also hold great promise for helping to protect any American forces that become involved in counterinsurgency. The lower American casualties, the greater the chances that the United States would stick with a counterinsurgency effort over the long period of time that success demands.

Informal war in the coming decades will not represent a total break with its current variants. It will still entail hands on combat, with non-combatants as pawns and victims. Insurgents, militias, and other organizations that use it, will seek ways to raise the costs of conflict for state forces. State forces, whether modern or postmodern, will simultaneously seek ways to impose stability or, in some cases, defeat their opponents at an acceptable cost. It is vital to remember, though, that informal and formal war will be inextricably linked. Interconnectedness and the proliferation of weapons of mass destruction are raising the costs and risks of formal war.

States that use traditional force against enemies will often run the risk of retaliation by weapons of mass destruction or, at least, of severe economic pressures from the global financial community which does not look favourably on the market dislocations caused by war. As a result, states will turn more and more to proxy violence through which they might gain their objectives while staying below the threshold which would lead to the use of weapons of mass destruction or to serious economic consequences. The core strategic dilemma for future leaders will be identifying that threshold.

## GREY AREA WAR.

As the Cold War ended defense analysts like Max G. Manwaring noted the rising danger from “grey area phenomena” that combined elements of traditional warfighting with those of organized crime. Grey area war is likely to increase in strategic significance in the early decades of the 21st century. To an extent, this is a return to historical normalcy after the abnormality of the Cold War. Militaries have long confronted both “big” and “small” enemies, protecting state territory from foreign invasion while fighting bandits, pirates, and brigands.

When foreign invasion was a major concern, armed forces tended to concentrate on it. When it was not, they often spent more of their time and effort on internal order or “small” enemies. This is certainly within the American tradition. Throughout most of U.S. history the Army and, to a lesser extent, the Navy focused on bandits, pirates, and brigands rather than preparing to fight other states in major wars. Today, grey area threats are increasing in strategic significance. Information technology, with its tendency to disperse information, shift advantages to flexible, networked organizations, and facilitate the creation of alliances or coalitions, has made grey area enemies more dangerous than in the past. For small or weak countries, the challenge is particularly dire.

Not only are their security forces and intelligence communities less proficient, but the potential impact of grey area threats is amplified by the need to attract outside capital. In this era of globalisation and interconnectedness, prosperity and stability within a state are contingent on capital inflows. Except in nations that possess one of the very rare high-payoff natural resources like petroleum, capital inflows require stability and security. In places like Colombia, South Africa, Central Asia, and the Caucuses, foreign investment is diminished by criminal activity and the insecurity it spawns. This makes grey area threats a serious security challenge. It also means that the United States, as the engineer of world order, must take them more seriously.

Grey area war involves an enemy or a network of enemies that seeks primarily profit, but which has political overtones and a substantially greater capability for strategic planning and the conduct of armed conflict than traditional criminal groups. Like future insurgents, future networked grey area enemies may have nodes that are purely political, some political elements that use informal war, and other components that are purely criminal.

This greatly complicates the task of security forces that must deal with them. Because grey area enemies fall in between the realm of national security and law enforcement, the security forces that confront them must also be a “grey” blend of the military and the police. Like the military, security forces must have substantial firepower (both traditional or informational), and the ability to approach problems strategically (i.e., to integrate agencies and elements of power, undertake long-term force development, and to think in terms of ultimate objectives and phased programs to attain them). But these security forces also must have characteristics of law enforcement, working within legal procedures and respecting legal rights.

In the opening decades of the 21st century, it will make sense to talk about both strategic and astrategic grey area war. The strategic form will be that used by some coherent organization or, more likely, network of organizations driving toward a specific purpose. Even though the objective will be monetary rather than purely political, violence will be goal-oriented. Astrategic grey area war will consist primarily of turf battles between armed gangs or militias. It may be related to refugee movements, ethnic conflict, ecological degradation, or struggles for political power (as in Jamaica in the 1990s, where political parties used street gangs to augment their influence). When astrategic grey area war is linked to struggles for political power, the armed forces (such as they are) will be serving as mercenaries only partially controlled by their paymasters, rather than armed units under the actual command of political authorities.

Even astrategic grey area war, though, will have security implications since it can deter investment and growth, draw in outside intervention, and, potentially, spark wider armed conflicts. As with many types of future war, the challenge will be the connections and linkages. A single grey area war alone may not be a serious challenge to a major state or a major alliance, but when a number of grey area organizations are linked, or when grey area organizations are connected to other types of threats, the danger will increase.

Since grey area war overlaps and falls in between traditional national security threats and law enforcement issues, states must often scramble to find the appropriate security structure to counter it. Nations with a French administrative tradition have an advantage in that they are comfortable with the idea of a national gendarmerie which overlaps military and police functions.

As the debate within the United States over the use of the military to counter grey area enemies intensifies in coming years, creation of an American national gendarmerie should be considered. Such an organization could combine elements of the military, the intelligence community and law enforcement agencies like the Drug Enforcement Agency and Federal Bureau of Investigation. It could form its own alliances with similar security forces around the world and operate more effectively against grey area enemies in an interconnected security environment and globalised economy.

Grey area war will also pose serious legal and civil rights questions. Should enemies that use it be treated as criminals, with full legal protection, or as military combatants, protected by the law of armed warfare? And, what sorts of legal and ethical frameworks will apply as grey area war spills across borders and becomes increasingly transnational? Even today the United States creates political problems by applying domestics laws on drug trafficking and terrorism to the citizens of other countries, sometimes ignoring normal extradition procedures.

This problem is likely to escalate as grey area enemies proliferate and coalesce into networks. The logical response may be an updating of the traditional international law dealing with piracy, which gave any nation the right to apprehend and punish a pirate on the high seas. Perhaps this should also apply to future grey area pirates operating in arenas like cyberspace. The danger from grey area problems should not be underestimated. If left unchecked, grey area conflict can mutate onto informal or even formal war, as one state uses pressure or even force against another which is providing sanctuary to criminals (or, at least, is looking the other way). As a general rule, the lower the level that an armed conflict can be resolved, the less the danger. Concerted effort to thwart grey area war in coming decades can prevent it from becoming even more dangerous.

## STRATEGIC INFORMATION WARFARE.

Formal, informal, and grey area war are all logical extensions of existing types. Technology, though, could force or allow more radical change in the conduct of armed conflict. For instance, information may become an actual weapon rather than simply a tool that supports traditional kinetic weapons. Future war may see attacks via computer viruses, worms, logic bombs, and trojan horses rather than bullets, bombs, and missiles. This is simply the latest version of an idea with recent antecedents in military history.

Beginning with the writings of people like Guilio Douhet in 1930s, some strategic thinkers held that it might be possible to defeat an enemy state by attacking its homeland directly, bypassing its military forces in the field. Strategic bombing alone did not bring Germany to its knees in World War II (although the theory was more nearly implemented against Japan, which still had a very large proportion of its army intact in the summer of 1945). But for its advocates, this did not disprove their position but simply showed that the technology of the time was immature.

Eventually nuclear weapons did make it possible to destroy a state without fighting a single engagement with its armed forces. But the political utility of nuclear weapons was always subject to question. Their destructiveness was so immense that even a state that waged a “successful” nuclear war would have found it a Pyrrhic victory.

By the 1960s, the arsenals of the nuclear powers were extensive enough that it seemed that the only real purposes of these weapons was to deter their use by others and, possibly to deter full-scale invasion of the homeland. Very much the ultimate hammer, nuclear weapons could not be used in instances that called for the modulated use of force.

Proponents of strategic warfare contend that technology now allows their theory to be applied. Information technology might provide a politically usable way to damage an enemy’s national or commercial infrastructure badly enough to attain victory without having to first defeat fielded military forces. During World War II, the Germans and Japanese mitigated the effects of strategic bombing by dispersing their productive capacity. The only counter response of the Allies was massive, sustained bombing of every conceivable target. This was inefficient and caused extensive collateral damage (which would now be politically unacceptable). Modern economies are so tightly linked and interdependent that destroying a few key components, particularly communications and power grids, could lead to a cascading collapse of the whole system.

Today strategic information warfare remains simply a concept or theory. The technology to wage it does not exist. Even if it did, strategists cannot be certain strategic information warfare would have the intended psychological effect. Would the destruction of a state's infrastructure truly cause psychological collapse? Would the failure of banking, commercial, and transportation systems crush the will of a people or steel it? After all, everyone who has attempted to use concerted strategic bombing, whether the Germans and the Allies in the World War II or the Americans in Vietnam, underestimated the willpower of their enemies. But until infrastructure warfare is proven ineffective, states and non-state actors that have the capacity to attempt it probably will, doing so because it appears potentially effective and less risky than other forms of armed conflict.

Future infrastructure war could take two forms. In one version, strategic information attacks would be used to prepare for or support conventional military operations to weaken an enemy's ability to mobilize or deploy force. The second possible form would be "stand alone" strategic information warfare. This might take the form of a sustained campaign designed for decisive victory or, more likely, as a series of raids designed to punish or coerce an enemy.

Facing a future Iraq or Serbia, for instance, the United States could conceivably use strategic information attacks rather than aerial bombardment, in part because of the belief that such actions would provoke less political opposition. All of this is, however, speculation. Today the technological feasibility, psychological effect, and legal ramifications of strategic information warfare remain unclear.

But should cyberattacks, whether as part of strategic information warfare or as terrorism, become common, the traditional advantage large and rich states hold in armed conflict might erode. Cyberattacks require much less expensive equipment than traditional ones. The necessary skills exist in the civilian information technology world. One of the things that made nation-states the most effective organizations for waging industrial age war was the expense of troops, equipment and supplies.

Conventional industrial-age war was expensive and wasteful. Only organizations that could mobilize large amounts of money, flesh, and material could succeed at it. But if it becomes possible to wage war using a handful of computers with internet connections, a vast array of organizations may choose to join the fray. Non-state organisations could be as effective as states. Private entities might be able to match state armed forces. Private or commercial organizations might even wage information war on each other—cyber "gang wars" played out on servers and network backbones around the world rather than in ghetto alleys.

As one of the world's most "wired" nations, strategic information warfare could be particularly problematic for the United States, forcing policymakers and military strategists to examine some of their most basic beliefs about warfighting and national security. For instance, the very existence of an infrastructure attack as well as its source could be hidden, at least for a while. An extensive series of problems and system failures induced by an infrastructure attack could occur before the United States understood that it was under attack. It is easy to imagine how tempers would flair if some American defence official in the future had to tell the president that the United States was at war but it was impossible to identify the enemy.

Strategic information warfare would raise a plethora of ethical, political, and legal issues. If the United States was facing a high-tech insurgent, criminal, or terrorist movement, for instance, could the American military (or some other branch of government) strike at its information and financial assets even though they were spread out in computer networks in dozens of sovereign nations? Should cyberattacks be answered only in kind or might traditional weapons be used to respond to them? And, how does the concept of collateral damage apply to cyberattacks? At an even broader level, who is responsible for the defence of a nation's information infrastructure? The government? The military? Private industry?

At the same time that basic policy issues are being discussed, the Clinton administration has begun addressing organizational questions. The first major step was the creation of the President's Commission on Critical Infrastructure Protection. Efforts to protect U.S. information systems have cantered on the National Infrastructure Protection Centre of the FBI. This includes representatives of the FBI, the Central Intelligence Agency, the Defence Department, the Secret Service, NASA, and the U.S. Post Office. In addition to assisting with criminal investigations of cyberattacks, it makes information on weaknesses in software available to the public.

Following a number of major denial-of-service hacker attacks on large commercial Internet sites in February 2000, President Clinton announced an initiative to create a voluntary, private-sector network to monitor and respond. Participants will include Charles Wang, chairman of Computer Associates International Inc.; Howard Schmidt, chief information security officer at Microsoft Corp.; Harris Miller, head of the Information Technology Association of America; and "Mudge," a member of a hacker think tank that does security consulting under the name AtStake.

The President plans to ask Congress for $9 million to help create the centre. According to the White House, the centrepiece of the federal government's efforts in this area will be the Institute for Information Infrastructure Protection, for which the President has requested $50 million in his Fiscal Year 2001 budget. While substantial movement is underway on the defence of national information infrastructure, offensive information warfare is more controversial. Following the 1999 air campaign against Serbia, there were reports that the United States had used offensive information warfare and thus "triggered a super weapon that catapulted the country into a military era that could forever alter the ways of war and the march of history."

According to this story, the U.S. military targeted Serbia's command and control network and telephone system. Other press reports, though, suggested that whatever offensive information warfare capabilities the United States had were not used against Serbia due to ethical and practical problems. Since the cascading effects of information attacks cannot be predicted or controlled given current technology, there were fears that their use would make American military commanders liable to war crimes charges.

In January 2000, though, U.S. Air Force General Richard Meyers, then commander of U.S. Space Command, announced that his organization will be given the mission of "computer attack." The irony is that pressure exists to make the use of force both less lethal and more precise. At the end of the 20th century, information warfare is less lethal but also less precise than conventional force. If this changes, strategic information warfare could be catapulted to a central role in U.S. military strategy.

## TECHNOLOGICAL TRANSFORMATION.

There are glimmerings of changes in war even more profound than strategic information warfare. While they will not alter the essence of war, new technologies or new combinations of technology have the potential to alter not only tactics and operational methods, but military strategy itself by the second or third decade of the 21st century. One of the most important trends in military strategy between the 18th and 20th centuries was the broadening of its focus. In the 18th century, one needed only to destroy the enemy's field army or, in some cases, seize control of key forts or territory. With the emergence of "total war" in the 20th century, an enemy's entire society and infrastructure became the targets of military operations.

Modern technology allowed war to move toward a “total” form described by Clausewitz, reaching ever-greater levels of destruction. The conundrum faced by political leaders today is that there is still a need to use armed force, but interconnectedness and other factors have made it difficult to mobilize and sustain the level of passion and hate necessary for total war. Strategists thus need some way to coerce or punish an enemy elite or, at least, to disrupt their plans, without the wholesale destruction of infrastructure or killing of non-combatants. This is the reason that precision is such an integral element of the current revolution in military affairs.

Within a few decades, technology may provide solutions to this strategic conundrum. After the Gulf War, American military leaders bragged that technology allowed them to not only select the building a bomb will hit, but to select which window of the building the bomb entered. Soon technology, particularly mini- or micro-robots, may allow military planners to select which individual or physical object in a building is to be destroyed. For the first time, it might be possible to target only the aggressor’s leaders, leaving non-combatants untouched. Within a few decades the technology might exist to construct killer robots the size of a grain of sand that could search for and kill future Saddam Husseins.

Like all new military technology, such fine-tuned precision will bring new risks, costs, dilemmas, and unintended side effects. Americans have long struggled with the ethics of deliberate assassination of enemy leaders. Such acts were rare even in the midst of declared war. During World War II, the only known instances were the American downing of the plane carrying Admiral Yamamoto, a British attempt to kill Erwin Rommel, and a German plot to kill Dwight Eisenhower. Today, assassination of enemy leaders outside of declared war is proscribed by presidential directive.

But as the technology to target enemy elites becomes available, Americans (and any others who develop a postmodern military) may rethink the ethics of using it. Future armed conflict may no longer pit one society against another, but one leadership cadre against another. While much speculation on future war focuses on the proliferation of weapons of mass destruction and the spread of terrorism and thus contends that non-combatants will be prime victims of future wars, the opposite is at least feasible. With brilliants robots, future armed conflict, like much of medieval war and 18th century European war, may be a sport for elites that leaves the masses relatively untouched.

This is only the tip of the technological iceberg. Coming decades are likely to see the proliferation of robots around the world and in many walks of life. Hans Moravec, for instance, contends that mass produced robots will appear in the next decade and slowly evolve into general purpose machines.

Ray Kurzweil takes the argument even further and holds that by the end of the 21st century, human beings will no longer be the most intelligent entities on the planet. However fast the evolution of robotics proceeds, it will invariably affect armed conflict. As one of the most avid customers of new technology, this will certainly affect the American military in the years after 2020. Initially, the prime function of military robots will be to replace humans in particularly dangerous or tedious functions. Examples might include evacuation of casualties under fire; operating in environments where nuclear, biological, or chemical weapons have been used; mine clearing; fire fighting; and reconnaissance, surveillance, and target acquisition.

The real breakthrough and decision point will come when robots advance to the point that they have the potential for combat use. This will take some time, particularly for land warfare, which takes place in a much more challenging operating environment for autonomous systems than does air, space, or sea warfare. Robots intended for battlefield use will have to be orders of magnitude “smarter” than those used for less stressful functions such as loading and moving material.

Current thinking about the technological characteristics of future military robots moves along two parallel tracks, each synthesizing robotics and other emerging technologies. The first envisions autonomous systems that employ sensors, computing, and propulsion very different from that used by people. One of the goals in this arena is miniaturization. Mini or micro-robots could be easily carried, yet perform a range of difficult or dangerous military missions.

The Pentagon already has a $35 million program under way to develop a bird-like, flapping-wing micro-air vehicle for battlefield reconnaissance and target acquisition. But this is just the beginning; the true revolution could come from the maturation of micro-electro-mechanical systems or MEMS which many leading scientists contend will be developed within 30 years with a dramatic impact in many endeavours. MEMS technologies construct very tiny mechanical devices coupled to electrical sensors and actuators. According to the Defense Advanced Research Projects Agency (DARPA):

The field of Microelectromechanical Systems (MEMS) is a revolutionary, enabling technology. It will merge the functions of compute, communicate and power together with sense, actuate and control to change completely the way people and machines interact with the physical world. Using an ever-expanding set of fabrication processes and materials, MEMS will provide the advantages of small size, low power, low mass, low-cost and high-functionality to integrated electromechanical systems both on the micro as well on the macro scale.

MEMS is based on a manufacturing technology that has had roots in microelectronics, but MEMS will go beyond this initial set of processes as MEMS becomes more intimately integrated into macro devices and systems. MEMS will be successful in all applications where size, weight and power must decrease simultaneously with functionality increases, and all while done under extreme cost pressure. Eventually MEMS could open the way for an even more profound revolution in nanotechnology, which is based on “bio-mimicry” manufacturing. A report from the U.S. Commission on National Security/21st Century states:

The implications of nanotechnology are particularly revolutionary given that such technologies will operate at the intersection of information technologies and biotechnologies. This merging and melding of technologies will produce smaller, more stable, and cheaper circuitry that can be embedded, and functionally interconnected, into practically anything—including organic life forms.

In the military realm, MEMS and nanotechnology could allow things like a “robotic tick” the size of a large insect which could attach itself to an enemy system such as a tank, then gather and transmit information or perform sabotage at a designated time. In a fanciful but technologically feasible description of the future battlefield, James Adams writes:

MEMS opens a window on a new generation of technology that will literally transform the battlefield. Tomorrow’s soldier will go to war with tiny aircraft in his backpack that he will be able to fly ahead of him to smell, see and hear what lies over the hill or inside the next building. Additional intelligence will be supplied by sensors disguised as blades of grass, pockets of sand or even clouds of dust.

However radical such a notion might seem, it is, like the official vision of the future, essentially new technology used in old ways. By contrast, futurists like Martin Libicki have speculated on modes of warfare to make maximum use of MEMS-based technology. In fact, Libicki’s alternative vision of future war is one of the most profound and creative seen to date. Its essence is that information technology, among other things, is shifting the advantage in warfare to “the small and the many” over “the large, the complex, and the few.”

This is in stark contrast to orthodox American strategic thinking that seeks ever more capable systems that are, by definition, more expensive, and thus acquired in smaller numbers, but is a logical development of the concept of distributed robotics under exploration by DARPA. Libicki describes three stage in the ascendance of "the small and the many." He calls the first "popup warfare." This is based on extant technology in a security environment characterized by the proliferation of precision guided munitions (PGMs). While Joint Vision 2010 and other official documents expect many states to have precision guided munitions, they assume that the American military can overcome enemy PGMs by stealth, operational dispersion, and speed. Libicki is more skeptical. "The contest between stealth and anti-stealth will be long and drawn-out," he writes, "but...the betting has to be against stealth for any platform large enough to encompass a human...even with stealth, everything ultimately can be found."

The result will be "popup warfare" where both sides stay hidden most of the time, pop up just briefly to move or shoot, and then "scurry into the background." Libicki's second stage of future warfare, which he calls "the mesh," uses technologies available over the next 20 years against an enemy with developed industry but underdeveloped informational capabilities. To a large extent, this is coterminous with the official vision that calls for an interlinked mesh of sensors and information technology to give American commanders a clear and perfect view of the battlefield while their opponents remain in the dark. Reinforcing the assumptions found in Joint Vision 2010 and other official documents, Libicki writes, "Tomorrow's meshes will allow their possessor to find anything worth hitting." Libicki's third stage represents the ultimate ascendance of "the small and the many." He contends that eventually enemies will develop their capabilities to the point that the platforms that compose the American military's "mesh" will be vulnerable to attack.

The solution is to weave a mesh composed of small, moderately priced objects rather than a handful of very large and very expensive ones. "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." This is where MEMS-based robotics becomes significant. Libicki speculates on the value of ant-like robots with each one having a fairly limited capability, but the weaving together of their collective capabilities generates extensive capabilities. The inherent redundancy of the mesh in what Libicki calls "fire ant warfare," in which small, relatively simple weapons and sensors swarm onto a large complex one as a means of attack, would make it much more robust than the one envisioned in official documents.

While initial thinking about robotics concentrates on miniaturization and the integration of networks of small robots with relatively limited functions, partially organic robots may prove nearly as useful. According to a recent report from the U.S. Commission on National Security/21st Century, "Notions of 'androids,' cyborgs,' and 'bionic' men and women have dwelled exclusively in the realm of science fiction. But at least the beginnings of such capabilities could literally exist within the lifetime of today's elementary school children." Soon it might be possible to mount cameras or other sensors on dogs, rats, insects or birds and to steer them using some sort of implant.

Simple cyborgs like this may be only the beginning of an even more fundamental revolution or, more precisely, the marriage of several ongoing technological revolutions. Lonnie D. Henley, for instance, argues that a melding of developments in molecular biology, nanotechnology, and information technology will stoke a second generation revolution in military affairs. Nanotechnology is a manufacturing process that builds at the atomic level. It is in very early stages, but holds the real possibility of machines that are extremely small, perhaps even microscopic.

http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=226

Cleaves Alternative News. http://cleaves.lingama.net/news/story-295.html