How Global Communications Are Changing the Character of War

by Audrey Kurth Cronin

Ordinary communications technologies are changing the character of war, enabling a form of popular mobilization that belies our predictions of how conflict would evolve in the twenty-first century. Any student of Carl von Clausewitz's *On War* knows that war has both changing and unchanging aspects. War's essential nature never alters: its violence, chance, danger, friction, and inherent unpredictability are timeless and unchanging. However, aspects related to how and why people fight *do* evolve dramatically, and here we are experiencing a paradigm shift like the one that occurred at the end of the eighteenth century. Today's dynamic social, economic, and political transitions are as important to understanding the present and future of war as were the changes of the French Revolution that Clausewitz observed. The twenty-first century's version of the *levee en masse* is the mass networked mobilization that emerges from cyberspace and explodes into physical reality. Yet, the extent of the tectonic shift in connectivity and conflict is misjudged, underestimated, and mistakenly seen as tangential to ordinary military planning, leaving the United States and its allies to react to its effects.

Communication is a key driving force that affects the causes and execution of modern war. Major war in the industrial age involved widespread mobilization of societies, tapping into the economic potential of states to field traditional conventional military forces that fought over territory. While insurgencies and small wars also proliferated, the most effective response to those challenges was to cordon off a region, focus on a population in a circumscribed territory, gradually divide the people from the cause, and target the insurgents.[1] The main stakes of war were typically control of territory, economic resources, type of government, collective good will of an indigenous population (hearts and minds), and national self-determination. The telephone, television, telegraph, and radio all played important roles in achieving these ends and were supported by a superstructure of satellites, transmitters, broadcast stations, and state regulation. During the twentieth century, communications technologies shaped and reflected an emphasis on the state, often strengthening its ability to govern, to mobilize, and to prosecute and win wars.

Audrey Kurth Cronin is Distinguished Service Professor at George Mason University's School of Public Policy and Senior Research Associate at Oxford University's Changing Character of War Programme.

While the traditional stakes of national power continue, today the state's long-standing approach to mobilizing and inspiring its population is undercut by the availability of individually accessible communications tools such as computers, DVDs, tablets and cell phones. The Internet, an effective vehicle to spread civil society and democratic ideals, also provides a means to disseminate violent ideologies, coordinate criminal behavior, share combat tactics, research powerful weapons, and undermine traditional tools of order. For all their wonderful qualities, including a spreading of knowledge, connectivity, and commerce, these new media platforms are also having unexpected effects on everything from the nature of intellectual discourse to the development of mass movements and mob psychologies. They are changing the shape of domestic and international violence. From the global spread of Islamist-inspired terrorist attacks, to the violent attacks on US Embassies in Muslim majority countries, to the rapid evolution of insurgent tactics in Iraq and Afghanistan, and well beyond, the global non-territorial nature of the information age is having an impact on the evolution of conflict.

Transformation is taking a new form. It is driven by nontraditional actors using cheaply accessible, modern technologies such as the Internet, cell phones, CDs, and DVDs to spread targeted messages through mediums such as Facebook, YouTube, Twitter, websites, email, blogs, text messaging, and photo services. Many benefit from these technologies, including states and advanced military organizations. There has been much US attention to the threat of aggressive cyber-attacks launched by major states such as China, Russia, and Iran, for example, although their virtually effortless collection of anti-US intelligence is a more immediate risk.[2] Proportionate to their size, however, nontraditional actors are benefiting much more than states. Operating at the intersection of technology, terrorism, crime and war, these actors can leverage communications connectivity to outflank more technologically advanced conventional powers. There is no reason why this need be the case, as targeted state countermeasures exist; but if the United States does not jettison tired old arguments and face up to the broad cultural reality of what is happening, it will be too late to adapt more effectively and recover the initiative.

A Trifecta of Change

The nature and extent of the paradigm shift arising from twenty-first century connectivity has three key features that affect war. First, common individuals are more powerful; from the conventional soldier, to the contractor, smuggler, insurgent, terrorist operative, religious extremist, or garden variety trouble maker, ordinary individuals have greater potential to wreak havoc. The United States military has focused on the super-empowered soldier for some time, but this increased individual leverage affects a broad array of non-traditional actors as well.[3] Second, the audience plays a greater role. Spectators can be instantaneously informed, individual by individual, with data or images often not filtered, monitored, or interpreted by knowledgeable leaders or experts. And unlike earlier eras, ordinary viewers can both receive a message and answer back, giving them real time influence over the course of conflicts, sometimes even as they unfold. Third, and most important, the means and ends of mass mobilization are changing, no longer requiring the involvement or inspiration of the popular state that was the hallmark of the French Revolution at the outset of the modern era. Conflict more frequently engages individuals who are mobilized, singly or in groups, to attack for objectives that are new and unexpected, but little analyzed. While effective state responses can be devised for all three of these changes, first we must explore their historical context in greater depth.

Historical Context: Communications, Technological Change, and War

The intricate, intertwined relationship between war and technological advances has existed throughout human existence. Changes in military technology are familiar: analyzing the impact on warfare of the stirrup, gunpowder, the machine gun, the tank, nuclear weapons, and so forth is well-trodden ground for military historians and strategists. However, changes in communications technology have been just as transformative, not only determining relative advantage but also influencing the shape of conflict itself.[4] For example, in the twentieth century, the relationship between telephone networks and armies in World War I contributed to the stalemate of trench warfare.[5] Laying the telephone wires along the trenches not only ensured coordinated operations but also contributed to the sclerotic battles that followed. World War II, the first wireless war, saw the innovative use of radio and radar, with countermeasures such as the code-breaking machines Enigma and Ultra responsible for dramatic advantages that arguably decided the outcome of the war. It was no mere coincidence that a transition to maneuver warfare accompanied the military's shift to the airwaves. Yet these were communications assets for armies and fleets to use; they were not truly revolutionary, in the sense of overturning the established order. They shifted the advantage from one opponent to another, but mainly complemented the bureaucratic structure of the state and its military.

A shift to an analysis of wider societal concepts of "communications" and their strategic implications happened gradually during the Cold War years, with the West's broad information campaign directed at the Soviet bloc, and the analyses of television's effect on the Vietnam War, the so-called CNN-effect in the Iraq War of 1991, and so on. Yet, curiously, most American military analysts studying the relationship between warfare and communications at the end of the twentieth century reverted to narrowly analyzing tactical advantages or vulnerabilities of the more technologically advanced side and misread the broader implications of the democratization of communications.

In the 1990s, growing awareness of the sweeping changes in information technology instead drove American military planners to concentrate on transformation and the so-called "Revolution in Military Affairs." This phrase was variously defined but fundamentally meant the use of the tools provided by advanced communications technologies to carry out high technology netcentric warfare, making war a "cleaner", more precise, and more efficient enterprise. Taking a cue from the dramatic changes occurring in the global marketplace, netcentric operations were designed to integrate military operations, providing a transparent picture of the battlefield available at every level of the command hierarchy down to the individual soldier.[6] The goal was to remove the need to engage with an enemy directly and to use high technologies from a distant platform, delivered through advanced means, preferably before the enemy even realized he was targeted. It was a type of warfare meant to be more humane in its reduction of casualties and its careful discrimination and targeting of the use of force. In a sense, it was crafted as the ultimate modern application of the *jus in bello* tenets of the just war tradition, with pinpoint discrimination becoming a key characteristic in achieving rapid, efficient, even "clean" victory. Today's widespread use of drones echoes this thinking.

Yet looking at the nature of conflict in the so-called Information Age as mainly a military or technological question was too narrow. The typical focus of military planners on using high-end tools for tactical connectivity was overdone and missed the point. Instead, what was unfolding was a widespread egalitarian development in communications more akin to the eighteenth century deregulation of the printing press than the whiz-bang technological advances of the late twentieth century.[7] And it had important practical implications for war.

Tapped to "transform" the traditional military forces of major states, these technologies were actually transforming willy-nilly the patterns of communication and the mobilization of a wide swath of ordinary human beings. Deprived of a major enemy and elated by the economic opportunities of the global marketplace, the US and its allies concentrated on intervening in small wars and conflicts when necessary, while taking advantage of an increasingly interconnected world economy. However, the economic prism too thoroughly pervaded military thought, with the so-called revolution in military affairs driven by a desire to translate the spectacular successes of e-business to war.[8]

The result of economic free marketplace thinking for early twenty-first century American strategy was a number of serious distortions. Among other things, it focused only on the supply side, forgetting that military organizations cannot be run like profit-making businesses. It assumed the kind of commonality of interests that exists between buyer and seller, wholly inappropriate to the realm of war. The result was odd concepts like "capabilities-based planning," whereby decisions about acquisition were made within a closed-loop reasoning cycle, in the absence of a threat. With very little pushing against them, American military planners were suddenly writing in a vacuum, reacting mainly to the changes observed in their own cultural and institutional context, forgetting the adaptability and dynamism of the enemy.

In fairness, there was a reason for this narrowness of view. The Internet's initial purpose was to prevent decapitation and the disabling of US communications in the event of a nuclear attack. The concept was brilliant; the technology was designed to be decentralized, redundant, persistent, and survivable. After the break-up of the Soviet Union, the World Wide Web consortium was created by the US Defense Advanced Research Projects Agency, with the goal of facilitating the spread of Internet connectivity. Fortunately or unfortunately, the break-up of the Soviet Union and the popular access to the web that followed provided those advantages to ordinary people, including businesses, non-governmental organizations, and advocacy groups, but also notably to members of criminal networks, terrorist groups, traffickers, and insurgents. The removal of the Soviet threat caused a relaxation of standard controls over connectivity and indirectly resulted in the dot-com boom that followed. It is not surprising, therefore, that the focus shifted to protecting US technological capabilities and preventing cyber-attacks that could cripple the US economy.

As the 1990s evolved, however, the broader global context was rapidly changing in more subtle ways that had pervasive and immediate impact. Removing control over information in the post-Soviet era opened the vast amount of knowledge available on the Internet to individuals. As more and more people tapped into the rich chaotic realm of cyberspace, the dark side of freedom of speech, indeed freedom of thought, became apparent. What is truly authoritative on the web? Whose ideas have legitimacy? What is worth fighting for? What is definitive when all pieces of information seem equally valid to the untrained, unanalytical or ungrounded mind?

Thus, in addition to changing how conflicts were fought, changes in technology and communications began changing the means of participation and the reasons why they were initiated. This included the spreading of radical ideas, myths, and disruptive techniques. Communications had always influenced the course of conflicts; now, through their use for widespread popular mobilization, they were actually helping to shape the *causes* of wars. What unfolded was not a revolution in military affairs but a revolution in human affairs. It affected everything from how humans communicated, to how they disseminated and analyzed knowledge to, most importantly for our purposes, how they mobilized and fought wars. The individual's ability to act on these changes also increased dramatically, which is the first of the three innovations to be examined here.

The Super-Empowered Individual

The opening of the global marketplace has strengthened the role and power of the individual in many ways. There is broad awareness of this phenomenon when it comes to commerce, but it is just as directly relevant to war.[9]

The employment of fully mobilized, massed national armies has been in decline for some time, but the changing social, political, and economic context has accelerated the slide. With the breaking down of borders, the growth of trade, both legal and illicit, has astonishingly increased; the increasing connectivity achieved through cell phones, DVDs, CDs, and the Internet has enhanced the capability of individuals, or very small networks of individuals, to operate both below and above the level of the state, its regulations, and its use of force. The ability to make money, to move products, to evade state regulation, to transfer mass quantities of people, goods, and services without detection is having an effect on the actors, the means, and even the causes and objectives of conflict.

Increasing access to advanced military technology to buy, sell, and use has dramatically enhanced the ability of any individual to engage in conflict and to do so with much more lethality. More powerful means in the hands of individuals then lower the threshold for engaging in war, making victory seem cheaper and more achievable. And ordinary communications systems, combined with more high-tech computer-supported technology, enable those foes to exploit victories, spread ideas, and find followers, again shifting the power relationship toward individuals and perpetuating the cycle.

INCREASING ACCESS TO ADVANCED MILITARY TECHNOLOGY TO BUY, SELL, AND USE HAS DRAMATICALLY ENHANCED THE ABILITY OF ANY INDIVIDUAL TO ENGAGE IN CONFLICT AND TO DO SO WITH MUCH MORE LETHALITY.

In the United States, a trend toward individual effectiveness in combat is apparent, long-standing, and the natural culmination of US-led advances from the twentieth century. It is not mere coincidence that the US Army's recruiting slogan is "An Army of One." American soldiers are the most technologically advanced fighters the world has ever seen. From night vision goggles, to laser training helmets, to heads-up display computer monitors, the individual soldier is in a narrow, technical sense more knowledgeable about his battle space than any of his historical predecessors. Not only does he know more, he also has an astonishing capacity to do more about it: the lethality of the individual soldier or small unit has increased significantly, to the extent that he now has a killing capacity comparable to much larger organizations in the past. Images flashing before the soldier can also be instantaneously available to the commander. Thermobaric weapons and laser eye-damaging weapons have joined more traditional high caliber sniping systems, rocket-propelled grenades, thermal imagers and enhancers, and highly lethal explosives to further increase the soldier's capability. Today's American soldier is arguably more connected, more protected, technologically smarter, and more supported than any warrior in history.

But war has a yin and yang dimension. The counterpart to the super-empowered US soldier is the individual terrorist, insurgent, smuggler and criminal who has also developed greater lethality and greater ability to conceal his weaponry. To take the most well-known example, the potential intersection between terrorists and so-called weapons of mass destruction, especially nuclear weapons, is widely considered to be the most serious immediate threat to international security. The potential lethality of the individual involved in smuggling a chemical, biological or nuclear weapon is obvious.[10]

Individuals have access to more lethal conventional weapons, as well as a greater capability to initiate or change the course of conflict. It used to be said that the black market was flooded with weapons in the wake of the Cold War; now they are so openly available that there is no need even to refer to the market as "black." Such complex markets operate in a confusing spectrum of shades of gray, with few purely legitimate trades. Highly lethal explosives, rocket-launched grenades, overstock mines, assault rifles, missile launchers, and many more sophisticated weapons are commonly available. The degree to which the market is flooded with ordinary small arms and man-portable weapon systems is beyond measurement and contributes to the continuing ability of warlords, insurgents, and petty criminals in places like Libya, Somalia, Sudan, Afghanistan, and Chechnya to inspire and equip local armies.[11] The trend of the 1990s was the story of the individual who used increasingly available weaponry to ignite a local conflict, insurgency, or civil war; that scenario has expanded to include not only a panoply weapons but also types of violence, such as riots, acts of terrorism, assassinations, civil wars, and a dizzying array of crime.

Not just weapons but also tactics have shifted toward the empowered individual. Looking specifically at terrorism, the increasing use of suicide attacks was a natural outgrowth of the individualization of conflict. Suicide attacks on average achieve more casualties and deaths per incident than do other types of attacks. For example, in Israel between 2000 and 2002, suicide attacks represented only 1 percent of the attacks but resulted in 44 percent of the casualties, a powerful force multiplier.[12] In the dynamic nature of twenty-first century warfare, this method is logical, if distressing and tragic. In a sense, suicide attacks are the flip side of the super-empowered, high technology soldier; they are the ultimate exploitation of the "power of the individual" achieving maximum effect. Indeed, the long-standing focus of political scientists and the military on the offense/defense dynamic in warfare at the operational level is misplaced. What we are witnessing is the offense/defense dynamic at the *individual* level determining the relative advantage in warfare.

State-on-state war is not obsolete. But states will also find their forces engaging in warfare with and against a wider array of ever more powerful individuals, or small groups of individuals, that can tap the resources of a more inter-connected world. With the power of ordinary communications, each of these conflicts will aim not only at local effects but also—and more importantly—at far flung observers. This expanded audience is the second crucial element in the evolving environment.

The Ubiquitous Audience

As empowered as the individual warrior, terrorist, warlord, or criminal is in the new international context, the role of the audience is in many ways far more important in its unforeseen, unpredictable effects on war. Because of the changing global context, the audience is more than ever a direct strategic actor.

It is not news that when a democracy goes to war, the effects on domestic audiences are crucial. Deployed Western forces are accustomed to dealing with the press and thinking about the characterization of their actions in stories that appear back home. Those with experience, training, and education in counterinsurgency tactics also focus on the effects of military operations upon indigenous populations, for example in the recent US wars in Iraq and Afghanistan. Parallels with Malaysia, Northern Ireland, Algeria, and Vietnam abound. The emphasis is on population control and winning "hearts and minds", classic counterinsurgency concepts.

But the point here is a little different. With our increasingly connected world and its proliferation of audiences, the phenomenon is both more fractionated and ubiquitous than any of our historical parallels. Digital camcorders, cameras, high-quality audio recorders, cell phones, email, and satellite networks all make the media far more anarchic than it used to be.[13] No effective filtering of images through broadcast networks like CBS, CNN, Al Jazeera, or Al Hurra can be controlled, or even easily influenced, by a state media operation. Today's audience members often get their information through millions of individualized channels that may be direct, difficult to monitor, distorted, and bear little relation to the facts. Information may or may not be instantaneous, as when broadcast in the late twentieth century by CNN, but it has become something even more powerful: tailored, voluntary, self-selected, specialized, and often self-reinforcing.

As was repeatedly demonstrated in the recent wars in Iraq and Afghanistan, if the audience is receptive, it can be easy for individuals to affect the course of a conflict or catalyze a violent incident. Videos of American soldiers torching dead bodies in Afghanistan recorded by local natives,[14] tapes of British troops beating civilians in Iraq filmed by fellow soldiers,[15] and photographs of the infamous Abu Ghraib prison sent home with personal emails[16] all had lasting strategic effects. Violent images are regularly posted where audiences can seek them out and self-select the "reality" they wish to see, over and over again. Fictional productions likewise reinforce inherent biases or simply infuriate viewers. The 14-minute film trailer "Innocence of Muslims" that in September 2012 catalyzed a wave of anti-US violence in Egypt, Yemen and other Muslim-majority countries was a vulgar amateur film apparently made by a few right-wing dissidents living in the United States.[17] The Danish cartoons depicting the Prophet Mohammad in 2005 were similarly explosive. These wild cards take governments by surprise: officials may not even know about them, or unravel what is going on and why, until it is far too late to offset the consequences.

Concepts of public diplomacy, communications forces, media management, and spinning or shaping a story are anachronistic when the enemy can directly pass a message or an image to the particular audience he wishes to target. Insurgents and terrorist groups have effectively used the Internet to support their operations for at least a decade. The tools of the global information age have helped them with administrative tasks, coordination of operations, recruitment of potential members, and communications among adherents. Individuals and small groups can move easily across many borders, collecting information, moving goods, and establishing cells even as military organizations and states are hampered by laws and territorial restrictions. Fund-raising is well established: groups as diverse the Revolutionary Armed Forces of Colombia (FARC), Hezbollah, and various Chechen groups are well known for their skill in raising money over the web.[18] The use of the Internet, satellites, cell phones, DVDs and social media to pass a message or an image to targeted constituents has far outpaced the ability of states to control or even keep track of them. Growth in connectivity in the developing world now represents the key force behind the global expansion of the Internet, with the percentage of individuals using the Internet in developing countries increasing from 9.4 in 2006 to 26.3 in 2011.[19] The increasing popularity of mobile phones is particularly notable in countries with poor fixed-line infrastructure, where wireless networks enable users to connect despite poor state services; in 2002, for the first time the number of mobile phones per capita exceeded the number of traditional telephone lines.[20] And, although not everyone has a computer, cable television, or cell phone on which to send or receive images, enough people do, have friends who do, can access them at a school or mosque, or can pay the paltry fee necessary to log on in an Internet café.

Communications on the Internet are not only broadly accessible but also intellectually egalitarian, giving equal credence to interpretations of the Koran that ignore or negate centuries of scholarly theological debates as they do to time-honored and well-respected clerics. Many who log on, tune in, text-message, or blog today are seeking a moral clarity that gives them an anchor in a turbulent world. The new media provide an unprecedented opportunity to perpetuate myths. According to one estimate, almost half the clerics in France's one thousand mosques lack religious training and download Friday sermons directly from radical Islamist websites.[21] Violent images and videos disseminate radical beliefs, socialize potential participants, and normalize violent behavior, whether by radical Islamists or white supremacists.[22] This is by no means the first time that the line between fact and fiction has blurred in the media, but personalization of the message makes the outcome more powerful, more instantaneous, more effective, and less controllable.

MANY WHO LOG ON, TUNE IN, TEXT-MESSAGE, OR BLOG TODAY ARE SEEKING A MORAL CLARITY THAT GIVES THEM AN ANCHOR IN A TURBULENT WORLD.

Even in areas of the world where Internet connectivity is relatively low, the effects of propaganda are enhanced by the use of older technologies like photocopiers and audio and video cassette tapes. It is the combined means of communications and not just the internet-based tools that are new. Images from Palestinian territories, Chechnya, and Iraq have been very influential in radicalizing and motivating young Muslim men, contributing to a belief that the 'West' is anti-Muslim, while constructing a worldwide Muslim identity and solidarity that did not formerly exist.[23] Today's connectivity has low barriers, largely by-passes most states, and has nearly instantaneous effects, and all of these are bringing individual audience members directly into contact with images that influence the nature, direction and outcome of today's conflicts. [24]

Cyber-Mobilization: A New Levee en Masse?

Third and most important of all, the means and nature of mass mobilization are changing, by-passing the role of the state that was the hallmark of the French Revolution. The result is an emerging sociology of popular mobilization being carried out through new communications tools that will affect how, where, and why future war is waged.

The US perspective has been too narrow: this battle is not the sci-fi net-war of cyber-planning or cyber-terrorism that military experts predicted at the end of the century. An obsession with information age technology has obscured the human conflict element of what is happening. New media communications are enabling the recruitment, training, convincing, compiling, and motivating of individuals by individuals, in unpredictable ways, through unpredictable links, with unreliable, unvetted information. The broader challenge goes beyond cyber-attacks toward mobilization that sometimes translates into violence in the physical world.[25]

Popular communications technology in the Internet age affects the causes, objectives, and targets of armed conflict. Today's communications technology has staying power, low cost, and lasting effect. Through the use of computers, cell phones, videotapes, and the internet, disparate individuals' disgruntlement, humiliation, and rage are given a greater voice and the tools to coordinate themselves to take effective group action. Was the anger always there? Perhaps or perhaps not; there were certainly objective reasons in many cases for it to exist. But projecting provocative images internationally can now engender a powerful group response among those who are poised to react, at little cost to those who post them. New technologies, or new combinations of technologies, are enabling individual frustrations to be rapidly shaped, exploited, formed, and mobilized into violent expression by territorially disjointed groups who are then able to act together.

This new form of mobilizing people and resources has an impact in many settings, whether the goal is terrorist attacks on civilians, insurgent movements in Iraq, or civil disturbances and crime. One of the earliest incidents in this new era was the Fall 2005 riots in France. They appeared to be spontaneous uprisings in the immigrant suburbs of Paris, sparked by anger at the death of two young African immigrants who electrocuted themselves while apparently fleeing from the police. French authorities were deeply frustrated by the unpredictable and decentralized nature of the violence. The violence was being driven by exhortations in blog messages posted on the web and text messages on cell phones for specific attacks. Cell phones were also handy for avoiding the police. The unrest spread across France to Toulouse and Marseille in the south, Cannes and Nice on the Riviera, and Strasbourg in the east.[26]

These were neither new technologies nor techniques: the innovation was the end toward which these means were used. The use of cell phones had been copied from a variety of earlier movements, including the 2003 Rose Revolution in Georgia, the 2004/5 Orange Revolution in Ukraine, anti-globalization protests by long-standing groups like Direct Action, and many other types of grass roots campaigns. The peace movement against the war in Iraq used email lists to mobilize demonstrations virtually instantaneously. In February 2003, the organizations MoveOn.Org and International Answer in a period of six weeks helped coordinate anti-war demonstrations in a way that took years of work during the Vietnam War.[27] These new means of communication had been drawing people together for years, and also crafted a narrative of the struggle—whether the motive was justice, democracy, rage, hatred, or civil war.

The democratization of communications has had many practical implications, some good and some bad, but all of them important. The point is to appreciate the astonishing organizational and ideological power inherent in these ordinary tools and to grasp their strategic implications for all human political activity, including war. It is a mistake to see this as a communications phenomenon between states and non-state actors: this is a paradigm shift that affects both. Being by far the strongest actor in the international system, the state is quickly catching up and learning to more effectively monitor, consider, and employ these means of mobilization, both defensively and offensively; however, some states are harnessing and exploiting them more quickly than others and, for good or for ill, gaining relative advantage for their own ends.

Practical Implications and Policy Recommendations

If this new context for war is altering the very reasons why people fight, not to mention how they perpetuate a campaign once begun, then the practice of dealing with so-called *information operations* as an adjunct to traditional military operations is wrong. Connectivity is a core strategic element of both offensive and defensive campaigns that is just as crucial to the outcome of future war as popular conscription, industrial capacity, logistics, operational art, or technological prowess have been to past wars. The challenge of adapting has two dimensions: the first is to establish short-term practical defenses and countermeasures to the violence perpetuated through these means; the second, much more difficult challenge is to respond to the powerful selective narrative being advanced, acting as the engine for the first. While the former costs people and property, the latter costs legitimacy and is infinitely more significant in its long-term implications. Both are met through the same basic methods.

Sadly the age of elation over the democratization of communications is over. It is time to recognize the fact that the violent exploitation of the stateless, anarchical realm of cyberspace forces upon us a need for better tools and countermeasures. Previous leaps in cross-border communication such as the telegraph, radio, and telephone engendered counteracting developments in code breaking, monitoring, interception and wiretapping. Twenty-first century countermeasures to the violence perpetuated through these means lag well behind, for many reasons. Most important, the challenge is presented as a clash between values of openness and measures taken against the new technologies. We are stuck in the old arguments of civil liberties or security, the right of freedom of speech or the spreading of radical ideologies and suicide techniques, and petty battles about control over the Internet by the US or by other major powers. These arguments are all beside the point. This threat naturally thrives in the narrow crevices within our value system, the areas of ethical ambiguity that make us uncomfortable. It will not be enough to rely upon the typical state regulations and treaties that have been proposed and quibbled about at the national and international level. This evolution requires more agile and creative thinking toward new practical solutions, a counter offensive, if you will.

It is time to recognize the fact that the violent exploitation of the stateless, anarchical realm of cyberspace forces upon us a need for better tools and countermeasures.

First, we must develop a broad range of smart counter messages, carefully tailored to the many target audiences that have a large presence on the world wide web. We must know who these audiences are and what they are seeing in order to present them with sophisticated, high-quality, legitimate, culturally appropriate, and interesting images and sites to access. Outdated and stilted government websites and official statements should be replaced by sophisticated alternative sites and images attractive to a new generation. The United States has shown a stultifying ignorance of the world's many audiences, paying most attention only to its own domestic constituencies.

Second, we must exploit and enlarge the differences between groups and the differing motivations that drive them by learning the languages, spending time watching their web sites, and picking up on the plethora of mistakes that enemies make. In particular, the obvious differences between nationalist groups and jihadist groups—or the groups that have only recently reflected jihadist rhetoric—should be clarified and highlighted. This is not just a matter of supporting warring factions against each other. Far more important over the long term, it is a matter of exploiting the contradictions in arguments disseminated to vulnerable audiences over the web.

Third, violent radical groups' mistakes must be publicized unflinchingly. When terrorists, criminals, or insurgents kill children, their actions should be reported on the web. Relatives should be interviewed and pictures of the dead should be shown in order to take the romance out of the use of brutal tactics such as suicide attacks, beheadings, and car bombs. One proven way of ending terrorism is to divide the people from the cause by graphically demonstrating the horrors that have been carried out in their name.[28] Not only is the United States failing to accomplish this, the lack of serious engagement in the debate is yielding vital ground.

Fourth, the emphasis must be shifted off of United States' values and culture, and instead concentrate on counter-mobilization, role models, and sources of hope within the context of local communities. The US must turn the spotlight of the new communications back toward local concerns, and return terrorism, crime, and insurgency to their traditional place as local issues, to be resolved primarily by local communities.

Finally, the US should do everything in its power to shore up international norms against illegitimate uses of force, including terrorism and all deliberate killing of noncombatants, for whatever reason. Prohibiting terrorism, insurgency, criminality, piracy, and other irregular types of violence, regardless of the motivation, on the grounds that they specifically target noncombatants provides a common global denominator, a source of legitimacy that will answer the moral relativism that Western governments are accused of. Doing so will shift the narrative to more solid, defensible ground.

Conclusions

Having unleashed communications connectivity and perpetuated its use during the last decade, the US is now failing to understand its full implications. The Internet and other means are crucial to the evolution of conflict in the twenty-first century, and US military organizations are foolish to treat their own web presence as if they were afterthoughts. A serious debate about the legitimacy of the use of force is happening through selective presentation of images, arguments, and evidence over means of communication that directly reach audiences in an unprecedented way. The US and its allies have fallen behind in directing the narrative—indeed failed even to offer informed input into the global debate—and is thereby losing the war on the web.

The evolution of conflict within the evolving historical context of super-empowered individuals, fractionating audiences, and cyber-mobilization will affect not only the irregular warfare that has been witnessed throughout the last decade but also the shape and outcome of any state-to-state violence that follows. Of course, all three of these phenomena have historical precedents. It is not utterly new for individuals to control high levels of lethality: the leaders of nuclear powers such as the Soviet Union, France, Britain, China, and the United States were more empowered than the individuals described here. But those individuals were leaders of states. The authoritarian state's direct access to audiences in the twentieth century was more powerful than the cyber-connections achieved by relatively minor actors such as Al Qaeda or Hezbollah. The traditional power of major industrialized states dwarfs any exhortations to violence via the Internet, cell phones, or video tapes. But history also demonstrates that over time the power to frame the ideological narrative, the story that incorporates popular passions, can eclipse the physical power of armies. States ignore this dimension of conflict at their peril.

In the current evolving context, the grass-roots connections described here are increasingly likely to affect, even catalyze, the actions of states. The modern secular state's ability to mobilize and to inspire its population is being undercut by the availability of individually accessible communications that present a powerful alternate narrative. Thus the unintended consequence of the drive to empower individuals in the late twentieth century has been the accompanying fractionation of conflict in the twenty-first. This tectonic shift is not tangential to war; it is at its heart and should be an integral part of any serious US grand strategy going forward.

Notes

[1] The literature on twentieth century counterinsurgency is vast. Classics include David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Frederick A. Praeger, 1964); and Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (Fort Leavenworth, Kansas: U.S. Army Command and Staff College, January 1985).

[2] James Adams, "Virtual Defense," *Foreign Affairs* (May/June 2001), 98-113.

[3] See, for example, Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999, http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm.; and Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (New York: Zenith Press, 2004).

[4] Emily O. Goldman, ed., *Information and Revolutions in Military Affairs* (London: Routledge, 2005).

[5] Martin Van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York: The Free Press, 1989).

[6] U.S. Department of Defense. *Network Centric Warfare*, Report to Congress (Washington DC: Government Printing Office, 2001), http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf.

[7] Audrey Kurth Cronin, "Cybermobilization: The New Levee en Masse," *Parameters* (Summer 2006), 77-87.

[8] Ibid.

[9] Thomas Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus, and Giroux, 1999).

[10] Numerous sources discuss this threat: Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Henry Holt and Company, 2004); Charles D. Ferguson and William C. Potter, *The Four Faces of Nuclear Terrorism* (Monterey, California: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004); Michael Levi, *On Nuclear Terrorism* (Cambridge, MA: Harvard University Press, 2007). For a dissenting view, see John Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda* (Oxford, UK: Oxford University Press, 2010).

[11] Moises Naim, *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy* (New York: Doubleday, 2006), pp. 41-42. ;Virginia Hart Ezell, "Small Arms: Dominating Conflict in the Early Twenty-first Century," *The Brown Journal of World Affairs* IX, no. 1 (Spring 2002): 305-310.

[12] Assaf Moghadam, "Palestinian Suicide Terrorism in the Second Intifada: Motivations and Organizational Aspects," *Studies in Conflict & Terrorism* 26 no. 2 (March-April 2003): 65.

[13] James Stavridis, "Deconstructing War," *Proceedings Magazine* 161, no. 12(December 2005).

[14] Richard A. Serrano and John Hendren, "U.S. Fears Fallout Over Reported Abuse of Bodies," *Los Angeles Times*,October 21, 2005, http://articles.latimes.com/2005/oct/21/world/fg-desecrate21.

[15] "Blair Promises Iraq 'Abuse' Probe," *BBC News*, February 12, 2006;

http://news.bbc.co.uk/1/hi/uk/4705482.stm.

[16] Reuters, "Iraq Abuse Images Aggravate Arab Hostility to West," February 17, 2006; at http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=iraq-abuse-images-aggravate-arab-hostility-to-west-2006-02-17.

[17] Robert Mackey and Liam Stack, "Obscure Film Mocking Muslim Prophet Sparks Anti-U.S. Protests in Egypt and Libya," *The New York Times*, 11 September 2012, http://thelede.blogs.nytimes.com/2012/09/11/obscure-film-mocking-muslim-prophet-sparks-anti-u-s-protests-in-egypt-and-libya/.

[18] Audrey Kurth Cronin, "Behind the Curve: Globalization and International Terrorism," *International Security* 27, no. 3(Winter 2002/2003): 30-58.

[19] "Key ICT Indicators for Developed and Developing Countries," International Telecommunications Union, 16 November 2011; http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html.

[20] A. T. Kearney, "Measuring Globalization: Economic Reversals, Forward Momentum," *Foreign Policy* (March/April 2004).

[21] Arnaud de Borchgrave, "European Disaster Zone," *The Washington Times*, November 24, 2005, http://www.washingtontimes.com/news/2005/nov/23/20051123-100556-8420r/?page=all.

[22] Institute for Strategic Dialogue, "Radicalisation: The Role of the Internet," A PPN Working Paper, http://www.strategicdialogue.org/allnewmats/idandsc2011/StockholmPPN2011_BackgroundPaper_FINAL.pdf.

[23] Adam Ward and James Hackett, eds., "The Jihad: Change and Continuation," *IISS Strategic Comments* 11, no. 7 (London: International Institute for Strategic Studies, September 2005).

[24] Audrey Kurth Cronin, *Ending Terrorism: Lessons for defeating al-Qaeda* (London: International Institute for Strategic Studies, 2008), pp. 11-22.

[25] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters* (Spring 2003), 112-123.

[26] Craig S. Smith, "As Rioting spreads, France maps tactics," *The International Herald Tribune*, November, 6 2005, http://www.nytimes.com/2005/11/06/world/europe/06iht-france.html?pagewanted=all&_r=0; Mary Papenfuss, "Rioters use cell phones, Net to fuel flames," New York Daily News, November 9, 2005, http://www.nydailynews.com/archives/news/rioters-cell-phones-net-fuel-flames-article-1.610150.

[27] Dan Frost and Carrie Kirby, "Aftermath of War: Internet Changes the Way United States Experience [sic] War," *San Francisco Chronicle*, May 12, 2003, http://www.sfgate.com/business/article/AFTERMATH-OF-WAR-Internet-changes-the-way-2617157.php.

[28] Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton, N.J.: Princeton University Press, 2009).