12

Information Flows in War and Peace

James Der Derian

IT'S THE INSTANTANEOUS NATURE of cyberattacks that has rendered defenses against them obsolete. Once an enemy finds a chink in U.S. cyberarmor and opts to exploit it, it will be too late for the United States to play defense (it takes 300 milliseconds for a keystroke to travel halfway around the world). Far better to be on the prowl for cybertrouble and—with a few keystrokes or by activating secret codes long ago secreted in a prospective foe's computer system—thwart any attack. Cyberdefense "never works" by itself, says the senior Pentagon officer. "There has to be an element of offense to have a credible defense."[1,2]

The spread and impact of information technology on global politics have left many a scholar in the dust. Methodologically, politically, geographically, the academic disciplines have been too specialized, parochial, or just not up to speed to comprehend the tsunami-like effects of networked information technology. Bound by a state-centrism, my own area of study, international relations, has been slow to consider the impact of information technology on war and peace. Curiously, law schools have been among the first of university bodies to take up the slack, deploying pragmatic, critical, and cross-disciplinary approaches to assess the global impact of information technology. This development hit home when I was invited to present in a single week at the

Columbia and Yale law schools, respectively, on "internment" and "flow"—or, more specifically, on how the technologies of both were affecting the traditional functions of national boundaries and state sovereignty. The two events highlighted what is often presented as the new global divide between "good" and "bad" information technology. On the one side, the rise and spread of information technology was viewed as increasing global communication, transparency, and productivity, thereby ameliorating the human condition. On the other, darker side, information technology was enabling new forms of Big Brother surveillance, terrorism, and war. So within the Ivies two stark contrasts emerge: new technologies condemned as the electronic prison gates of a new virtual incarceration and celebrated as interconnective switch gates for a new open source society. Rather than take sides or pretend that there might be some happy medium of interpretation, I want to consider both positions as just one more symptom of the *sturm und drang* induced by the information revolution. And as a first step in symptomology, one has to ask what other, more subtle, and less polarized signs are being ignored or neglected by the narrow pursuit of celebrating or denigrating information technology.

To Go (or Not) with the Flow

Any inquiry into the impact of information technology on world politics must address not only an increase in speed and volume but also the change in character and content of global information flows. This is most apparent as the flow of images begins to produce more powerful effects and supplant the flow of words. In the yet-to-be-written history of the transition from the Cold War to the information age, images trumped words over and again in political crises that punctuated shrinking periods of stability and order. We watched, literally and visually, as the dual promises of a peace dividend and information revolution after 11/9/89 were reversed and traduced by the events of 9/11/2001 and the "Long Wars" of counterterror and counterinsurgency that followed. In the process, new grammars of security and terror were produced.

As verb, code, and historical method, "to terrorize" has consistently been understood as an act of symbolically intimidating and, if deemed

necessary, violently eradicating a personal, political, social, ethnic, religious, ideological, or otherwise radically differentiated foe. Yet, as noun, message, and catchall political signifier, the meaning of "terror" has proven more elusive. From Robespierre's endorsement to Burke's condemnation during the French Revolution, from the Jewish Irgun blowing up the King David Hotel to the Palestinian Black September massacre at the Munich Olympics, from bin Laden the Good fighting the Soviet occupiers of Afghanistan to bin Laden the Bad toppling the twin towers of New York, terrorism, terrorists and terror itself have morphed into the political pornography of modernity: One knows "terrorism" with certainty only when, literally, one sees it. But in a blink of the eye, the terrorist can become the freedom fighter, and vice versa, for at one time or another nearly everyone, from righteous statesmen who terror-bomb cities to virtuous *jihad*ists who suicide-bomb women and children, seems to have a taste for terror.

Without engaging in nostalgia, one can recognize that the most powerful model of terror, which inscribed the most powerful borders of inclusion and exclusion, mutated at the end of the Cold War. With the decline (if not the total demise) of a logic of deterrence based on a nuclear balance of terror, so too eroded the willingness and capacity to inflict mutually unacceptable harm that had provided a semblance of order if not an actual state of peace or justice to the bipolar system. In its place a new model has emerged, an *imbalance of terror*, based on a mimetic fear and hatred coupled with an asymmetrical willingness and capacity to destroy the other without the formalities of war.[3]

This cannot be reduced, as much as leaders on both sides of the conflict have tried, to merely a post-9/11 phenomenon. Its origins can be traced at least as far back as 1992, with the Pentagon's secret effort written by Paul Wolfowitz to model seven post–Cold War "war scenarios," including the rise by the year 2001 of an "REGT" (Resurgent/Emergent Global Threat).[4] It was publicly established in the 1998 US Defense Policy Guidance, which shifted from a strategy of *deterring* to *destroying* the enemy (subsequently reiterated in the Quadrennial Defense Review). And on the other side of the information divide, in 1998 bin Laden issued his pseudo-*fatwa* that decreed Christian and Jewish civilians legitimate targets of the *jihad*.

As in the older, tidier balance of terror, the doctrine of taking civilians hostage and if necessary killing them still held for both sides, but it now operated as a contingent factor of an asymmetrical relationship. Regardless of nomenclature—"terror" or "counter-terror"—high numbers of civilians would (and continue to) be killed in the process. It might be small solace to the victims whether they were primary targets as opposed to "accidental" or "collateral" victims, especially with casualty rates being terribly skewed in both cases. When one takes into account how war-related fatalities have been reversed in modern times, from a hundred years ago when one civilian was killed per eight soldiers, to the current ratio of eight civilians per soldier killed, then compares the combatant-to-noncombatant casualty figures of 9/11, the Afghan War to the Iraq War and now back again to the Afghan War, the terror/counterterror distinction begins to fade even further.

Ageism

Looking back, it does seem remarkable how the age of terror so easily displaced the information age and other competing descriptors of modernity. Historic moments all too often appear to be speaking for themselves. Think of the "Middle Ages," the "American Century," the '60s. Consider 2001, a year that signified awe for an extraterrestrial future in Kubrick's film—that is, until airplanes piloted by kamikaze Al-Qaeda terrorists brought the year, and the World Trade Center (WTC), crashing to earth. We clearly cannot begin to understand the transformation of the Cold War to the age of terror without studying the fundamentalist religious and political beliefs of the major combatants.[5] But we also need to pay more attention to how the information flow of powerful images acted as catalysts for these transitions.

Fueled by a revolution in the digitization and networking of information, the forces driving the information age spread fast and penetrated deeply. From its embryonic moments in the 1940s (when Claude Shannon wrote the first paper on information theory, transistors were invented, and ENIAC, the first computer, was built) to its accelerated takeoff in the 1990s (when packet-switching, personal computers, HTML, and the Internet produced a World Wide Web), the information revolution outpaced, outlasted, and outperformed all commensurable comers.

However, the information age never warranted the status of a *longue durée*. Although the information age might stretch in the United States from Silicon Valley to Silicon Alley and globally from Bangalore to Singapore, the distinguishing characteristic of the information age is a spatio-temporal *intensivity* rather than a geopolitical *extensivity*—that is, a capacity to intensify global effects through a collapse of time and distance. Developing unevenly within and across nation-states, and beset by rapid cycles of dot-com booms and busts, the information age is short on universality and long on instability. When a revolution stops auguring change and begins signifying an age, it usually means that a regime has been stabilized, a cultural shift codified, predictability restored.

Not so with the information revolution at the palpitating heart of the information age. The only constant is fast, repetitious, and highly reproducible change: a kind of hyperspeed Nietzschean "eternal recurrence" that defies—in spite of efforts by democratic peace theorists (with Thomas Friedman leading the pundits' charge)—the predetermined logic of progressivist teleologies. Modernity in an information age manifests not as a more advanced era succeeding an earlier backward one but as rapid oscillations of message and medium (signal-to-noise ratio), regressive repetitions of images (feedback loops), and phase shifts between order and disorder (or complexity).

Eight Propositions for Studying Infoflows

If not the era, can the promise of the information age be salvaged? Only if one first intellectually confronts and publicly compensates for the dark side of infotech and infloflow. I am sure there are more, but I have eight preliminary propositions for getting beyond 9/11 and back to the best the information age had to offer.

First, the most obvious: Infotech is producing new networks of power in IR that must be managed, regulated, and channeled for the amelioration of global, not national, security. Best defined by Kevin Kelly as "organic behavior in a technological matrix," networks are challenging and changing the nature of state power through new lattices of relatedness and responsiveness.[6] Obviously, the United States has emerged as the dominant military and economic power, and even in the worst-case

nightmares of global realists, it is difficult to identify a potential "peer competitor" on the horizon. However, post–Cold War, post-9/11, we have witnessed the emergence of competing sources and mediations of power: what I call a *global heteropolar matrix*, in which different actors are able to produce profound global effects through interconnectivity. Varying in identity, interests, and strength, ranging from fundamentalist terrorists to peace activists, new global actors gain advantage through the broad bandwidth of information technology rather than through the narrow stovepipe of territorially based sovereign governments. Enhanced by IT, nonstate actors have become super-empowered players in international politics. Traditional forms of statecraft have become transformed and in some cases undermined by infowar, cyberwar, and netwar. The technologies of weapons of mass destruction, networked terror, accidental crises, and global media have transformed the meaning and discourse of national security.

Second, networked infotech provides new global actors the means to traverse political, economic, religious, and cultural boundaries, changing not only how war is fought and peace is made but making it ever more difficult to maintain the very distinction of war and peace. The West might enjoy an advantage in surveillance, media, and military technologies; but the rest, including fundamentalist terrorist groups, nongovernmental organizations, and anti-globalization activists, have tapped the political potential of networked technologies of information collection, transmission, and storage. We need to undertake a full-scale investigation of how global political actors force-multiply their influence in war and diplomacy through networked infotech.

Third, new global informational and technological networks of power require new modes of comprehension and instruction, and the social sciences have not been quick to take up the challenge. The virtual nature and accelerating pace of infotech is partly responsible: Actualizing global events in real time across traditional political, social, and cultural boundaries, infotech resists the social-scientific emphasis on discerning rational behavior, applying static models, and conducting incremental research projects. Moreover, the study of infotech requires a dialogue among technological, scientific, military and other nonacademic circles that has been notably lacking in discipline-bound university programs and politically

oriented think tanks. Taking into account the heteropolar as well as multicultural nature of global politics, we need a strategy that endorses plural, conceptual, and multidisciplinary approaches to investigate what we consider to be the most challenging issue of the twenty-first century: the global application and management of IT in war and peace.

Fourth, we need to recognize that the impact of infoflow is now largely measured by infotech's capacity to produce a *moving* image of the world. In both senses of the word, this multimedium is *e*-motive, a transient electronic effect conveyed at speed. At the emotional level, this means image-based sentiments of fear, hate, and empathy now dominate word-based discourses of ideas, interests, and power. At the electronic level, the speed of the transmission—with real time currently the gold standard of media—matters as much as the content of the message. Paul Virilio, urban architect and social critic, has spent a lifetime demonstrating how this media-driven acceleration has produced what he calls an "aesthetics of disappearance," in which the political subject, be it the accountable leader, participatory citizen, or the deliberative process itself, is diminished and quickly engulfed by a growing "infosphere."[7]

Fifth, infotech—increasingly, repetitively, unavoidably—not only acts as trigger and transmitter of the global infoflow event but also affects how we respond to the event.[8] From the actual moment to the eventual interpretation—for better or worse—infotech records, relays, represents, and informs our response to global events. Infotech also shapes how we remember or forget their significance: We are back to chronology. We are all familiar with the contemporary production and transformation of multimedia by networked information technologies, from increased CPU speeds and broadband access, to real-time cable news and CNN effects, to embedded journalists and network-centric warfare. The global networking of multimedia that makes up the information flow has become unstoppable, and I believe that its effects may well have accelerated beyond our political as well as theoretical grasp. A public attention deficit disorder leaves little time for critical inquiry and political action by a permanently distracted audience.

Sixth, infotech has become essential for the global circulation of power, the waging of war, and the imagining of peace. Information tech-

nology is now an unparalleled force in the organization, execution, justification, and representation of global violence, as witnessed in the first Gulf War, the Kosovo air campaign, and the terrorist attacks of September 11. With the war in Iraq, the global effects of infotech became inescapable. We witnessed how antiwar organizers used the Internet globally to muster millions of protesters in large metropolitan areas; U.S. military commanders leveraged technological superiority to wage network-centric warfare; and embedded journalists provided influential battlefield reports by satellite videophones in real time. A glut of information (if a dearth of knowledge) drew viewers by the millions, not only to primetime TV and cable news but also to instantly updated online press sites and unofficial war blogs. We witnessed the first, but certainly not the last, networked war.

Seventh, the darker side of infoflow, although freighted in the occasional media spasm, continues to evade the sustained attention of IR theory as well as the concern of international institutions.[9] Networked terror; network-centric warfare; network attacks by the Blaster, Nachi, and SoBig viruses; and a hot summer of electrical network failures had a tremendous transnational impact. Networked technologies merged issues of national, corporate, and personal security (and liberty) into an interconnected global problem. Yet the new global risks of interconnectivity, including negative synergies, unintended consequences, and the pathologies of networks like viruses, worms, and Trojan horses, often failed to make the global political agenda at all.

Eighth, the infotech/flow transformation of global politics requires new conceptual approaches. We need to interrogate as critical pluralists (rather than corroborate as social scientists) the extant knowledge of how information flow operates in international relations. My predilection for multimedia montage over parsimonious rationalist approaches is as much a response to these technological changes as it is a reflection of my earlier critiques of social scientific theory's failure to keep up with the pace of these changes. This is not an antitheoretical position. Rather, it shifts our intellectual priorities from the slow, incremental development of theory to the more supple and strategic application of concepts. Put pragmatically, theory informs, concepts perform.

From Infowar to Infopeace

The signs of rapid change are often pathologically manifested: Information, to paraphrase William Burroughs, has become a virus, and the immune response is often worse than the original contagion; densely networked systems produce negative as well as positive synergies with cascading effects; and everywhere global institutions of governance are failing to keep up with the new global risks of interconnectivity. We must adopt new strategies, concepts, and polices for the new dangers and opportunities presented by IT. As a preliminary step, we need to adapt and update a pair of concepts that capture the full spectrum potential of information flow, to enable the continuation of violence through *infowar*, as well as to provide the means to prevent, mediate, and resolve conflicts through *infopeace*. The concepts provide a sense of the complex, paradoxical, and often contradictory nature of the technologies that convey, generate, regulate, and stop information flows.[10] They emerge from but can also help us decouple information flows from the state of emergency that transforms technologies of security into weapons of mass distraction, deception, and destruction.

Information warfare, or infowar, has become the umbrella concept for understanding cyberwar, hackerwar, netwar, virtual war, and other network-centric conflicts. It has a history that goes back at least as far as Sun Tzu, who considered defeating an enemy without violence to be the "acme of skill" in warfare. From its earliest application in the beating of gongs and drums, to more sophisticated uses of propaganda and psychological operations, infowar has traditionally been deployed by the military as a "force-multiplier" of other, more conventional forms of violence. In this sense, infowar is an adjunct of conventional war, in which command and control of the battlefield are augmented by computers, communications, and intelligence. With the development of mass and multiple media, infowar has taken on new forms and greater significance. As the infosphere engulfs the biosphere; as the global struggle for "full spectrum dominance" supplants discrete battlefields; as transnational business, criminal, and terrorist networks challenge the supremacy and sovereignty of the territorial state, information warfare has ascended as a significant site for the struggle of power and knowledge. Infowar wages

an epistemic battle for reality in which opinions, beliefs, and decisions are created and destroyed by a contest of networked information and communication systems.

Infowar couples sign-systems and weapons-systems. Command and control, simulation and dissimulation, deception and destruction, virtual reality and hyperreality—all are binary functions, sometimes symbiotic, other times antagonistic. Networks of remote sensing and iconic representation enable the targeting, demonization, and, if necessary, killing of the enemy. In its "hard" form, infowar provides "battlespace domination" by violent (GPS-guided missiles and bombs) as well nonlethal (pulse weapons and psychological operations) applications of technology. In its "soft" form, infowar includes a virus attack on a computer network or the wiping out of terrorist organisations' bank accounts. In its most virtualized form, infowar can generate simulated battlefields or even create *Wag the Dog* versions of a terrorist event. In any of these three forms, information warfare can be offensive (network-centric war, Trojan horse virus, or intelligence dissimulations) or defensive (ballistic missile defence, network firewall, or preventive media).

In spite of the official spin, infowar is not a precision munition. It might seek to discriminate in its targeting of enemies, but it is as broadcast forms of media that it is likely to produce all kinds of collateral damage, blowback, and newly resentful enemies.

At the other end of the information spectrum lies infopeace: the production, application, and analysis of information by peaceful means for peaceful ends. Starting with Gregory Bateson's definition of information as "a difference that makes a difference"[11]—this is war, that is peace, this war is here, that war is over there, this war is now, that war was then—infopeace seeks to make a difference through a difference in the quality of thinking about the global contest of will, goods, and might. Measuring information in terms of quality rather than quantity, and assessing quality by the difference it makes in the reduction of personal and structural violence, infopeace opens up possibilities of alternative thought and action in global politics. Unabashedly utopian yet pragmatic, it counters a "natural" state of war with an historicized state of peace.

Infopeace seeks to prevent, mediate, and resolve states of war by the actualization of a mindful state of peace. Positing the eventual aboli-

tion of violence as a global political option, peacemindedness ranges from the prevention, admonition, and mediation of violence to the outright disavowal of violence to resolve problems in the international arena. It draws on a long tradition of peace-thinking, exemplified in early Christian pacifism and Eastern philosophies, in which the need for peace begins internally and proceeds outwardly. It starts by embracing a wholeness of the individual and expands to families, communities, countries, and beyond. The notion of Gaia as a self-regulating biosphere contributes to the rhetoric of peace-thinking, but it is the networked reality of an expanding infosphere that makes peace an attainable and ever more vital necessity.

Infopeace stresses the actualization of peace through the creative application of information technology and public diplomacy. As a form of critical imagination, infopeace resists a technological determinism that increasingly circumscribes human choices. Further, infopeace integrates a strategy in which difference, conflict, and antagonism are recognized as essential aspects of human relations. It aims to develop an awareness of how these aspects can be addressed by nonviolent means.

The Banality of Terror

Let me conclude by returning to the images that take us to war and that can lead us to peace. As we know from medical pathology, the autoimmune response can kill as well as cure. The response to the most powerful images—the towers toppling, the bin Laden tapes, the Abu Ghraib photos—bears this out. Heinous crimes were revealed, public outrage was expressed, official apologies were proffered, congressional hearings convened and courts-martial put into place. In the case of the Abu Ghraib photos, once established as authentic, they took on a singular significance: a crisis for the Bush administration and America's reputation in the world. Numerous reports of earlier instances of dissimulations, groupthink acts of self-deception, and outright lies by the U.S. government—from claims about Iraqi ties to Al-Qaeda, the presence of weapons of mass destruction, and the likelihood of a swift postwar transition to peace and democracy—all paled in comparative political effect to the digital images of simulated sex, bondage, and mock lynchings. However,

the surfeit of images also produced a reverse effect: Overexposed to images of prisoner abuse, Islamicist hip-hop videos, and brutal snuff films of hostages, many preferred to remove the realities of war with the flick of a channel, the click of a mouse. The way was clear for a banalization of terror.

We now see how the infoflow of terror and counterterror produces an iconic, virtual, and, even worse, increasingly banal effect. In her study of the "thought-defying" nature of evil that earmarked the killing machine of Nazi Germany, Hannah Arendt identified the political effects of this banalization. Citing Arendt and the "banality of evil" can, admittedly, be just another way of not really thinking through the pervasive and perverse state of emergency that shapes so much of world politics today. However, a more obscure observation by Arendt, captured during an interview from late in her life, leaves us with a sense of what radical measures are needed when the most destructive information flow takes on a banal character:

> It is indeed my opinion now that evil is never "radical," that it is only extreme, and that it possesses neither depth nor any demonic dimension. It can overgrow and lay waste the whole world precisely because it spreads like a fungus on the surface. It is "thought-defying," as I said, because thought tries to reach some depth, to go to roots, and the moment it concerns itself with evil, it is frustrated because there is nothing. That is its "banality." Only the good has depth and can be radical.

Notes

1. "U.S. Cyberwar Strategy: The Pentagon Plans to Attack," Mark Thompson, Time.com (2 February 2010).

2. "Inter arma silent leges." (In wartime, the laws fall silent.) Cicero, *Pro Milone* (52 BC) Justice Antonin Scalia, *Hamdi v. Rumsfeld* (2004).

3. "The art of deterrence, prohibiting political war, favors the upsurge, not of conflicts, but of acts of war without war." See Paul Virilio, *Pure War*, trans. Mark Polizotti, New York: Semiotext(e), 1983, p. 27.

4. See Patrick Tyler, *New York Times* (February 17, 1992), p. A8.

5. See James Der Derian, *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*, Boulder and Oxford: Westview Press, 2001.

6. Kevin Kelly, *New Rules for the New Economy* (London: Fourth Estate, 1999), 31.

7. See Paul Virilio, *The Aesthetics of Disappearance*, trans. Philip Beitchman (New York: Semiotext(e), 1991), and James Der Derian, 'Introduction', *The Paul Virilio Reader* (Oxford: Blackwell Publishers, 1998), 1-15.

8. See *Philosophy in a Time of Terror: Dialogues with Jurgen Habermas and Jacques Derrida*, ed. Giovanna Borradori (Chicago, IL and London: University of Chicago Press, 2003), 85–90.

9. This was borne out at the December 2003 World Summit on the Information Society held in Geneva, at which the techno-optimists, vamping the political, cultural, and developmental promise of technological interconnectivity, had center stage while critics—especially American ones—were marginalized and kept out of the main planning sessions.

10. Even before Sun Tzu wrote his informative study of war, it seems that the Chinese well understood the nature of this contradiction, as demonstrated by the actual Chinese character for "contradiction": a combination of the ideograms for sword and shield.

11. Gregory Bateson. *Steps to an Ecology of Mind* (Chicago: University of Chicago Press, 2000), 459.