Studies in Intelligence Vol. 48 No. 4 (2004)

The New Face of War: How War Will Be Fought in the 21st Century

Intelligence in Recent Public Literature

By Bruce Berkowitz. New York: Free Press, 2003. 272 pages.

Reviewed by Eric Haseltine

Nicholas Negroponte, head of MIT's Media Lab, observed that the information age is fast replacing atoms with bits; movies on film with packets on the Internet; print media with digital media; and wires with digital radio waves.

Negroponte does not apply the bits-for-atoms principle to warfare, but Bruce Berkowitz, in *The New Face of War*, does. According to Berkowitz, a senior analyst at RAND and a former intelligence officer, future wars will not be won by having more atoms (troops, weapons, territory) than an opponent, but by having more bits . . . of information.

Berkowitz argues that atoms that used to be big winners will become big losers to information technology. Reconnaissance sensors will quickly find massed troops, enabling adversaries to zap those troops with precision-guided weapons. Fortifications will tie armies down to fixed locations, making them sitting ducks for smart bombs. Cheap cyber weapons (*e.g.*, computer viruses) will neutralize expensive kinetic weapons (*e.g.,* missile defenses).

Berkowitz sums up the growing dominance of bits over atoms: "The ability to collect, communicate, process, and protect information is the most important factor defining military power." The key word here is: "**the** most important factor." *The New Face of War* gives many historical examples of information superiority proving to be **an** important factor in defining military power, such as the allies breaking German and Japanese codes during World War II and Union forces employing disinformation to mislead Confederates in the Civil War. But the digital revolution has transformed information from supporting actor to leading lady.

Evidence that this revolution has already occurred abounds. In the 1990 Gulf War, smart weapons turned Saddam's strength (concentrated troops and tanks) into liabilities. More recently, al-Qa'ida used the global telecommunications net to coordinate successful attacks by small, stealthy groups who triumphed through information superiority (knowing more about their targets than their targets knew about them).

Perhaps the biggest effect of information technology on warfare will be the elimination of the concept of a front, according to Berkowitz. If fronts persist at all, they will live in cyberspace

where info-warriors battle not over turf, but over control of routers, operating systems, and firewalls. Even so, *The New Face of War* argues that there will be no electronic "Pearl Harbors" on the emerging battlefield of bits because disabling a nation's information technology (IT) infrastructure will be too hard even for the most sophisticated cyber-warriors. Well-timed, pinpoint computer network attacks will be much more likely.

Dr. Berkowitz's vision of the future is probably right in many respects and off target in a few others. But, regardless of its accuracy, his book surfaces critical questions for the Intelligence Community.

First, the things he gets right and what these mean for intelligence: Information technology has changed warfare not by degree, but in kind, so that victory will increasingly go to combatants who maneuver bits faster than their adversaries. Thus, intelligence services will need an increasing proportion of tech-savvy talent to track, target, and defend against adversaries' IT capabilities. As countries like China, India, Pakistan, and Russia grow their IT talent base—and IT market share—faster than the United States, the strengths of their intelligence services will likely increase relative to those of US intelligence.

Because cyber-wars will be played out on landscapes of commercial IT, intelligence agencies will need new alliances with the private sector, akin to existing relationships between nation states. And the Intelligence Community will have to confront knotty problems such as: performing intelligence preparation of cyber battlefields; assessing capabilities and intentions of adversaries whose info-weapons and defenses are invisible; deciding whether there is any distinction between cyber defense and cyber intelligence; and determining who in the national security establishment should perform functions that straddle the offensive, defensive, and intelligence missions of the uniformed services and intelligence agencies.

The growing importance of IT in warfare will also change the way intelligence agencies support atom-based conflicts. New technology will collect real-time intelligence for fast-changing tactical engagements, but the mainstay product of the Intelligence Community, serialized reports, is far too slow for disseminating these high-tech indications and warnings. Faster means of delivering—and protecting—raw collection must be devised, so that real-time intelligence can be sent directly to shooters without detouring through multiple echelons of military intelligence analysts. Also, remote sensors designed to report on the capabilities, intentions, and activities of armed forces, will not find lone terrorists. Radically new sensing networks that blanket the globe will be needed to collect pinpoint intelligence on individual targets.

The distinction between intelligence and tactical operations data (such as contact reports and significant activity reports) will blur as national intelligence means are focused on real-time tactical missions. All-source analysts will need to add tactical operations reporting to their diet of HUMINT, SIGINT, IMINT, OSINT and MASINT.

Now, the areas in which *The New Face of War* misses the mark: First, military power in the future will not flow solely from precision zapping and deployment of small, networked forces. Some missions, such as peacekeeping, will always demand the highly visible presence of large forces. And if numbers do not matter anymore, as Berkowitz suggests, why worry about North Korea's million-plus army? The bottom line is that as intelligence agencies get better at tracking and collecting on individuals terrorists, they will still need robust targeting and force protection capabilities against large conventional forces.

The evolution of media, with which we began this discussion, teaches powerful lessons about

the folly of too quickly abandoning the old for the new. The printing press did not abolish handwriting; motion pictures did not kill live theater; television did not doom radio; and the Internet did not extinguish magazines. For each of these transitions from old to new, there were plenty of pundits who prophesized the demise of legacy forms of communication at the hands of new information technology.

Berkowitz is in good company, though. The US Air Force was so sure that close air combat was obsolete, that the first F-4 fighters did not have cannons. They relied instead on high-tech air-to-air missiles—until the F-4s fell victim to the cannons of North Vietnamese MIGs in "obsolete" air combat. Low-tech weapons on the F-4 ultimately did not yield to high-tech missiles; they simply moved over and made room for them. And today's newest generation of fighters still retain cannons.

There is an important lesson here for intelligence agencies: As novel collection, analytic, and dissemination technologies are acquired, traditional tradecraft should be retained to cope with traditional adversaries and tactical situations. Just as missiles did not replace cannons, legacy tradecraft will need to be preserved but continuously improved to track changes in conventional warfare. For example, imaging satellites will always be essential, but they will have to steadily increase resolution and dwell time. Ditto for traditional SIGINT and MASINT collection systems.

I also disagree with Berkowitz's contention that there can be no electronic Pearl Harbors. The inexorable migration to the Internet of such diverse functions as telephony, power plant control, commercial data networks, and defense communications has already created a "one-stop-shop" target for info-warriors. In essence, industrialized nations have done in cyberspace what Berkowitz says is so perilous in physical space: namely, concentrated all their eggs in one basket. Intelligence agencies should not, therefore, abandon the hope of severely crippling a cyber enemy, nor should they assume a cyber enemy could not return the favor.

Despite these shortcomings, *The New Face of War* is an eminently enjoyable read, jam-packed with fascinating historical examples of information technology at war. Dr. Berkowitz's experience as an intelligence officer comes through clearly in his book, providing important context and relevance for intelligence collectors, analysts, and disseminators.

Put another way, whether consumed as atoms or bits, *The New Face of War* is a must read for all intelligence professionals.

Dr. Eric Haseltine is the Associate Director for Research at the National Security Agency. This article is unclassified in its entirety.
