Rethinking War: The Mouse's New Roar?

by Martin Libicki

For most of history, the oft-cited correlation between the size of one's battalions and the odds of military victory had a firm foundation in reality. In classic terms, larger forces won more battles. When technology began to matter, large industrialized nations proved uniquely capable of mobilizing the resources to develop trump cards such as nuclear arms or spy satellites.

The rise of globalization over the last half century has now given analysts cause to question such received wisdom. Today, almost every element of power can be acquired in the global marketplace. Information technologies have given nearly everyone a potential voice in the world arena. And so it seems that the small have caught up with the strong and that size does not matter, at least as it once did.

But while in some ways small nations can fend off superpowers more effectively, in others they are more at their mercy. The most obvious paths to power, such as the ability to hold others at risk through weapons of mass destruction, or, speculatively, through information warfare, may turn out to be show rather than substance. Instead, non-superpowers can exploit globalization in more subtle ways. By making use of the technologies of the "revolution in military affairs," small countries can tilt the odds against an invading army and remove the certainty of success that once made aggression worthwhile. They also

MARTIN LIBICKI *is a senior policy analyst at the* RAND *Corporation in Washington, D.C.*

have an unprecedented opportunity to manipulate the burgeoning global media to their advantage, whether by courting world opinion or undermining an adversary's domestic base of support.

It's a Micro World

The ability of the small to fend off the large is not entirely a new phenomenon. Small rich countries have often withstood aggressions from large poor ones, as both Israel and Taiwan (with a little help from their friends) have demonstrated. Small impoverished nations can also frustrate large wealthy ones if they believe deeply enough in their cause and are willing to die in its defense: The respective victories of North Vietnam and Afghanistan over the two cold war juggernauts, the United States and the Soviet Union, are two noteworthy cases. Small nations frequently benefit from their greater ability to focus. A superpower has multiple interests and the affairs of an irritant are not central to its existence. Smaller nations know no such luxury.

To understand how globalization might affect this equation, it helps to take a short detour into technology. As with military strength, the reigning paradigm of progress had long been correlated with size: scientific megaprojects, larger factories, taller buildings, heavier supertankers, wider roads, longer runways, and rockets large enough to lift men to the moon and underwrite the nuclear age. But in the 1970s, energy shortages, intolerable pollution, integrated circuits, gene splicing, and scanning tunneling microscopes began to herald a new direction. Thereafter, the vector of progress began to come from detail, the ability to engineer features and control defects at the micro scale. Technologies of choice are now microelectronics, microbiology, and, coming soon, microstructures. With small size and low cost come replicability and diffusion, rather than uniqueness and concentration.

Computers are an obvious example: All that progress in silicon has fostered not the hyper-intelligent HAL of Stanley Kubrick's *2001* (or even the vaunted fifth-generation computer of Japan), but the ubiquitous Internet. The next application of intelligence is showing up in smaller packages: laptops, PalmPilots, and cell phones. The ability of large countries to develop (and hoard) large-scale technologies has lost much of its relevance. Micro technologies are like Tinkertoys: Anyone can buy them and a large container's worth helps, but they are no substitute for clever construction and the ability to tailor the results to one's specific needs.

Whereas miniaturization has made technology more accessible, globalization has been the engine driving its diffusion. The Internet, for instance, can easily permit a backwater research institution in the developing world to access the same physics articles that a university in a developed country has long taken for granted. During the cold war, the United States declassified advanced technologies slowly and restricted sales to an inner circle of allies. Today, the race among nations to secure a niche in lucrative high-tech markets, combined with the collapse of trade barriers worldwide, has made dual-use components such as high-speed transmitters and receivers available to all. Existing export controls serve more as speed bumps than real barriers. The sale of U.S. supercomputers abroad is restricted, but a combination of enough computers, some networking gear, and the right software can build an apparatus that solves many problems that hitherto required supercomputing capability.

Although technology and globalization, coupled with the cold war's end, have changed the instruments of power, do they necessarily bring the small up to par with the large? The ultimate objective of war is to project power. And the ultimate definition of power is the ability to bend adversaries to your will, to force them to do what you want. Power can be obtained through either control or coercion. Control implies the ability to incapacitate opponents and force them to do what you dictate (the U.S. occupation of Japan in the aftermath of World War II is a prime example). In the case of coercion, your opponents have multiple options, but the penalty for not making the decision that you want is so devastating that there is no real choice (such as the Soviet Union backing down during the Cuban missile crisis when faced with the threat of nuclear war). The threshold for control or coercion is quite high—it is not enough to be able to inflict pain on an adversary, whether it is through cruise missile strikes or terrorist bombings. The outstanding question is: Has globalization provided small nations with the tools that allow them finally to cross that threshold?

The Ecology of Terror

Over the last two decades, globalization (and a certain winking at where products end up) has enabled small and relatively backward countries to acquire chemical plants from Europe, biological research equipment from the United States, or missile technology from the former Soviet Union. But their ensuing development of missiles and

weapons of mass destruction may not necessarily tip the scales. The ability of a small country to drop an explosive warhead on the city of a superpower may give the latter pause and remove the cloak of impunity behind which superpowers plot. As such, superpowers cannot contemplate military action against a missile-armed foe without the risk of civilian casualties. Yet, once that psychological barrier is breached and action proceeds, long-range missiles are nothing more than fancy artillery. Larger countries will always have more.

Since smaller countries are outgunned, weapons of mass destruction—chemical, biological, and nuclear—are often touted as the great equalizers. Chemical weapons, the so-called poor man's bomb, are cited as the quintessential example of superpower status on the cheap. Clearly, the scare potential of chemical weapons is higher than conventional weapons, and thus, putatively, so is the pause that may refresh a superpower's thinking. But, again, once the barrier is breached, superpowers have a decided advantage in throwweight, and large nations may more easily lay waste to small ones than the reverse. Iraqi President Saddam Hussein intuitively understood that relationship: He chose not to use chemical weapons against U.S. forces during the Gulf War when then Secretary of State James Baker made it clear that such an action would invite a "devastating" response. Furthermore, the first user of chemical weapons risks the world's obloquy. And users will also rediscover why chemical warheads, despite being widely tested in World War I, never replaced high explosives within military arsenals; only in selected situations do they have more military value.

What about biological weapons? Notwithstanding what horrors may emerge tomorrow from some gene-splicing laboratory, today's best weapon remains anthrax. A 110-pound bag of dried anthrax spores could very well kill 100,000 within a city of 500,000—in theory. However, getting anthrax into dried spore form with the exact and consistent size suitable for even halfway efficient aerosolization is so hard that the trick was pulled off neither by the Aum Shinrikyo (with as much as $1 billion in financial resources at their disposal) nor the Iraqis—who had to settle for a liquid slurry with far fewer viable organisms and much less efficient dispersion. No one has ever killed people using biological warfare delivered from the nose cone of a moving missile. Demonstrated failure at biological warfare, meanwhile, would more surely bring on devastating reaction from the rest of the world. Ugliness is no proof of military utility, much less of coercive force.

That leaves nuclear weapons, which (a) actually work and (b) actually have military utility. In a world of ongoing nuclear coercion, their possession is taken very seriously—so seriously that the nonproliferation community (more cynically, the exclusive club of existing nuclear powers) devotes great resources to making the acquisition of nuclear weapons difficult. They pay particular attention to the nuclear fuel cycle (on the theory that the mechanical apparatus is easier to develop). A lucky country on the way to the bomb may sometimes be rewarded—such as North Korea, which was offered a grab bag of incentives, including subsidized oil shipments, in exchange for adhering to nonproliferation standards. But the scent of imminent success may also add urgency to a military response, such as the Gulf War coalition's decision to take the offensive against Iraq in Operation Desert Storm.

Another downside for small nations that aspire to become nuclear powers is that their neighbors are unlikely to sit by idly. As the case of India and Pakistan shows, one nation's acquisition is often matched by another's. (And as the earlier efforts of Argentina and Brazil suggest, even one nation's pursuit of nuclear capability may be so matched.) The result is continued stalemate at higher levels of risk—both in terms of greater civilian deaths and in the possibility of outside intervention.

If weapons of mass destruction are not the express lane to superpower status, then what about a more circuitous route? Small nations, it is often said, can exploit the chinks in the armor of the great powers through information warfare and terrorism. Even the smallest of countries can make use of a single connection, a cheap computer, and a clever hacker to disrupt or corrupt any of the world's major information systems: funds transfer, transportation control, air traffic safety, phones, electric power, oil and gas distribution, and even military systems.

Or so Hollywood would have us believe. Were cyberterrorism or blackmail so easy, one or another malevolent party would have done it long ago to the United States or other advanced economies [see box on page 38]. Such societies have already been computerized for decades (hacker stories in comic strips and movies date back to 1983 or earlier), and the United States has had enemies whose best time to conduct information warfare has clearly come (and often gone). One could ask why the Irish Republican Army never struck Great Britain's infrastructure; Hamas, Israel's; or the Kurdistan Workers Party, Turkey's.

Paradoxically, the difficulty of using information warfare as a tool of coercion stems not from computers being too secure, but from not being

secure enough. Consider, for example, the metaphor of a homeowner who lives in a lousy neighborhood and always leaves the front door open. If the house were robbed, you would be inclined to blame the homeowner, not the burglar—and the homeowner would (hopefully) learn a lesson and lock the door in future. Similarly, too many computer networks are far less secure than they could be. Systems can be put at risk only because their gates, both external and internal, have been left ajar. Many known techniques such as digital signatures, read-only system files, and semantic filters can secure important systems quite well. Thus, in the event of a cyberassault, rather than reacting by groveling in front of the attacker, the more likely response of a government would be to blame the victims whose sloppiness made them vulnerable—and use the incident as a rallying point to tighten security. In the meantime, government law enforcement has proved surprisingly effective in deterring some hackers.

With rare exceptions, small nations have no comparative advantage over a garage full of webheads when it comes to computer hacking.

Is blaming the victims a wise response? Absolutely. A superpower that gives into one nation's information warfare can be held hostage by not only other nations, but also by anyone with an agenda or an attitude. With rare exceptions, small nations have no comparative advantage over a garage full of webheads when it comes to computer hacking (indeed, the open global networks that hackers use to stay abreast of the latest techniques have a strong advantage over the closed institutions that characterize most government intelligence agencies). But small nations intent on information warfare face some rather unpleasant comparative disadvantages. Information warfare is spectacularly heir to blowback. The virus unleashed in the global infrastructure may come home to roost, either in their computer networks or in the networks of an ally. And governments can be targets of retaliation if they upset someone else badly enough.

The same paradox governs garden-variety terrorism. In order for terrorism to be effective as a form of coercion, there must be a link between the sponsoring nation and the terrorist act. The ability of citizens from a small country (e.g., Chechnya—or so it is alleged) to murder civilians en masse in another country (e.g., Russia) certainly gets attention. Globalization in the form of more porous borders makes terrorism

easier. Globalization in the form of media attention makes echoes ring louder. But if the link between terror and the small country can be established in the mind of the big country (and political leaders are more likely to blame outsiders for disasters), the game could easily change. Indeed, this fall, public outrage over terrorist bombings that killed close to 300 Russians prompted Moscow to forsake its cease-fire agreement with Chechnya and launch a brutal offensive that had, as of November, captured one third of Chechen territory.

Practically speaking, terrorism has not been a particularly efficacious form of conflict for nations. So-called rogue states such as Iran, Libya, and North Korea have all faced political and economic isolation for sponsoring acts of international terrorism. When terrorism is at sufficiently high levels as to become guerrilla warfare, its chances of success may be greater; but few are the small states that can exploit a population of disaffected compatriots across the border to make this work.

Don't Tread on Me

Small countries now have the means to be serious annoyances, but they still have a long way to go before they can inflict sufficient pain to coerce the large powers. However, globalization has made it easier for small countries to resist efforts at control and incapacitation by an invading superpower. In the realm of conventional warfare, the means exist for sophisticated countries from large to small to undertake what has been called a revolution in military affairs. Traditionally, victory in combat was a matter of mobilizing, deploying, and utilizing the larger battalions (or battle fleets, or air squadrons). Skill counted, but numbers ultimately were the deciding factor.

The revolution in military affairs, however, is changing that balance. The development of precision-guided munitions (PGMs), which first came of age 20 years ago, has meant that the ability to see a target is tantamount to being able to hit and kill it. PGMs can be expensive, but if a small country is willing to settle for a weapon shot within 10 miles of its target, it is possible to get good capability for roughly $50,000 a shot—wasteful against people perhaps, but quite cost-effective against the kind of machinery that superpowers like to bring to battle. To be useful, however, PGMs have to be told where to go and that, in turn, puts a premium on being able to see the battlefield and communicate its relevant features to the operator—in a word, information.

Harder Than It Looks

Several years ago a former intelligence official claimed that with 20 good hackers and a few tens of millions of dollars he could bring the nation's infrastructure—and thus the country—to its knees.

Are advanced societies really so vulnerable?

Until hackers take over an electricity grid or a phone system, no one will really know for sure. But there are three reasons why nations may be harder to take down than people think:

First, the ease with which a corporate Web site can be breached reveals little about the vulnerability of core processes such as power distribution systems, call control centers, funds transfer mechanisms, or new product engineering. The former is engineered to be publicly accessible; after all, what good is an e-commerce Web site if no one can see it? Anecdotal evidence suggests that, over the last two to five years, many companies have cut back on the connectivity between the more open and closed parts of their networks.

Second, taking control of a system when no one is looking is not the same as keeping control over a system once people are alerted. Brief control suffices to steal information, but it requires more than a flicker or a temporary busy signal to cause real damage to societies. Defenders, in turn, have several built-in advantages: law enforcement (the longer hackers stay online the easier they are to trace), detailed knowledge of their own systems, and physical control not only of network connections but of data storage and access sites. In some cases, the machinery controlled by information systems can revert to manual or default settings and carry on.

Third, the assumption that modern civilization will collapse without its network-based infrastructures can be overly glib. Granted, electricity is central to modern times. Even so, agriculture, construction, many heavy industries, the military, and even education can continue functioning without it (temperature permitting). At the other end of the scale, people managed to live normal well-adjusted lives before cellular telephones and the World Wide Web—and with sufficient ingenuity and the force of circumstance they could learn to do so again.

–M.L.

Increasingly, the key to victory on the battlefield is making use of advanced information technology. Most of what is needed to achieve information superiority in times of war is now available over the counter in the global marketplace. Computers are commodities and cheap ones at that; so are digital cellular phones and message-bearing pagers. Handheld Global Positioning System receivers retail for around $200. Digital cameras that can capture 2 million picture elements (pixels) retail for several hundred dollars; so do 500-line video cameras. Want a hilltop view? More than 20 countries make unmanned aerial vehicles that could sell for as little as $10,000. Want access to space? Despite bankruptcies at Iridium and ICO Global Communications, some sort of global mobile phone system is inevitable. The launch of the Ikonos II satellite this September can let anyone with a few thousand dollars purchase a shot of any spot on Earth that can resolve details as small as one meter.

Although such photographs are subject to (the constitutionally unproved) imposition of U.S. shutter control, an upcoming launch by a company registered in the Cayman Islands could yield equal resolution with fewer questions. Lesser capability may be quite cheap: A British company, SSTL, spent less than $10 million to develop and launch a 10-meter resolution satellite. Want to hand-carry that information? The same five-gigabyte DVDs (digital video disks) used for videos can also hold a compressed 256-color map of Belgium accurate to one meter. It's all a matter of smart shopping. When assembled, such a collection of technologies may permit small countries to wage a tough hedgerow defense against large invaders—whose forces must necessarily move across hostile terrain to achieve their aims. A combination of seeing and hearing sensors can give possessors a good clue of impending military actions and even pinpoint the machinery behind it. Packet-switched networks—wherein information is broken down into short bursts of data, disseminated through varied paths, and assembled at the receiving end—make it possible to send messages even if a large percentage of a country's infrastructure has been destroyed. Portable or remotely controlled munitions should make it hazardous to put armed forces within—or even just beyond—the territory of a small country.

Is it that simple? Of course not. Putting all of these pieces together to form an effective defensive posture requires cleverness at systems integration, a devotion to maintenance, diligent training, flexibility in doc-

trine, and repeated (and honest) experimentation to get it right. These are attributes not of size but of smarts—and large nations do not have a monopoly on them. And the raw materials for systems integration (e.g., software), maintenance (e.g., repair manuals), and training (e.g., simulations) can all be delivered in byte-sized form over the Internet.

But if a large power can't control a small nation, then it can undertake a strategy of coercion. The difficulty of conquering a shrewd and spiky little country may have already occurred to the superpowers. Even without information age technologies (and the U.S. Seventh Fleet) a country such as China must regard the conquest of Taiwan as no sure thing. However, many of the advantages of mounting a hedgerow defense do not apply if a large power wants merely to coerce a small one. Here, a strategy of standing back, lobbing a sufficient quantity of missiles and bombs, and throwing in a blockade for good measure may work better—a modern version of siege warfare.

Large states risk being ostracized for actions that would have gone unreported earlier.

Does it work? Strategic coercion requires the consent, albeit grudging, of the coerced. If the victims are especially stubborn or fanatic, coercion is no substitute for control. A divided Japan yielded to U.S. coercion in 1945 only after a spectacular demonstration of an unexpected weapon, a history of unremitting defeat, and a looming invasion—but a fanatic Germany did not. A cynical and calculating Serbia yielded an outlying province after nearly three months of unanswered attacks by NATO.

Globalization here may work against small countries if their elites prefer flight to fight; the volume of passports acquired by the elite of Hong Kong indicates such a choice. By one estimate, roughly one quarter of Taiwan's doctors were out of the country by the time provocative Chinese military maneuvers and missile testing concluded in March 1996. Globalization makes flight easier. When status is based on fungible financial resources, wealth is based on footloose knowledge, friends and family (and customers) are worldwide, and immigrants (especially those with bank deposits) are welcome, then, yes, "you can take it with you." The threat of doing so makes it less likely that some small nations as a whole will persist in defiance.

The Whole World Is Watching

The globalization of perception—the ability of everyone to know what is happening in minute detail around the world and the increasing tendency to care about it—is another way that the small can fend off the large. Exploiting this trend, a small nation can portray itself as a victim of aggression and often in time for the world community to react meaningfully. Large states risk being ostracized for actions that would have gone unreported earlier. Such reprobation may serve to inhibit the large from striking—or at least prevent aggression from being legitimized so that it may one day be reversed.

Three developments create this leverage. The first is the advent of global media networks that permit news to be reported instantly and in greater detail. The second is the increasing proliferation of surveillance devices—from small cameras to remote sensing satellites—that are peering into the world's dark corners. Taken together, these factors create an unprecedented level of transparency. The third development is the end of the cold war, which has freed people (at least in the West) to hold the actions of states up to universal norms rather than use strictly constructed national interest as the test of approval.

Some small and middle-ranking powers have learned the hard way that transparency, coupled with norms, is starting to matter. The plight of Kosovar Albanians provided the impetus and justification for NATO's united assault on Serbia. Indonesia found itself on the receiving end of global condemnation for its unwillingness to protect residents of East Timor against militias.

But transparency can also work in favor of small states. When the United States bombed the al-Shifaa pharmaceutical plant in Khartoum last August, did the Sudanese respond with a military or terrorist attack? No, even worse, they responded with a public relations offensive, aided by an inquisitive world press that has cast significant doubt on whether the targeted factory ever produced chemical weapons agents. Televised images of civilian casualties or refugees can undermine domestic support or international legitimacy for a military campaign waged against a small nation. It's hardly surprising that one media analyst has suggested that small countries are better off deploying CNN reporters than tanks to their borders.

Countries that wish to play the victim successfully must set the stage carefully and choose the background music well. Transparency, after all, cannot ipso facto deliver clear-cut judgments about who

wears the white hat. Is Kuwait a sovereign country attacked by its large neighbor or an artificial British invention filled with the undeserving rich? Is Saddam Hussein a modern-day Saladin driving the infidels from the holy places or a reincarnation of Hitler? Is Serbia a small state victimized by NATO or a medium-sized state engaging in ethnic cleansing? Are Chechen or Kashimiri fighters suffering minorities of nations whose majority is of other faiths or fundamentalists bent on violence and intent on establishing intolerant theocracies?

Making sure the answers come out right requires understanding what makes sense to the audience; that is, the historical and moral context within which today's events can be mapped. And what makes sense to an American audience will not necessarily resonate the same way to a Russian or Chinese one. For this trick, size is no help; sophistication is what counts. Small nations that survive by understanding how to get along in the world ought to have an inherent advantage over large nations whose size makes them more parochial or impervious to the opinions of others.

Small countries cannot rest their security on others without some well-founded nervousness. The ability of the media to stir popular outrage predates the 20th century. Think of the Hearst newspapers hastening the Spanish-American War or the British public's condemnation of Turkey's Balkan policies even though Turkey was a counterweight to Russia. Yet only recently has the 20th century been kind to small states. And today's kindness is contingent on nothing more serious being at stake—a global depression or a new cold war could make such flowers of concern fade fast.

Want to Know More?

Many of the techniques that can be exploited by small states to coerce or fend off large ones are still hypothetical. Among the more comprehensive investigations of the impact of globalization and the information age on the conduct of conflict is John Arquilla and David Ronfeldt, eds., ***In Athena's Camp: Preparing for Conflict in the Information Age*** (Santa Monica: RAND, 1997), as well as two reports from the Center for Strategic and International Studies: Stuart J.D. Schwartzstein, ed., ***The Information Revolution and National Security: Dimensions and Directions*** (Washington: CSIS, 1996) and its companion volume, Ryan Henry and C. Edward Peartree, eds., ***The Information Revolution and International Security*** (Washington: CSIS, 1998).

The literature on apocalyptic threats tends to be, well, apocalyptic. Nevertheless, Keith B. Payne's ***Deterrence in the Second Nuclear Age*** (Lexington: University Press of Kentucky, 1996) and Paul J. Bracken's ***Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age*** (New York: HarperCollins, 1999) attempt to come to grips with the new nuclear threat environment. For a balanced examination of lesser threats, see Ian O. Lesser et al, eds., ***Countering the New Terrorism*** (Santa Monica: RAND 1999). Richard A. Falkenreath, Robert D. Newman, and Bradley A. Thayer have addressed this issue in ***America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*** (Cambridge: MIT Press, 1998)—which, despite its title and evident intent, is oddly reassuring when the authors explain why disaster has not happened yet.

George Smith casts a critical eye upon information warfare in **"An Electronic Pearl Harbor? Not Likely"** (*Issues in Science and Technology*, Fall 1998). For a good compilation of incidents and threats, see Dorothy E. Denning's ***Information Warfare and Security*** (Reading: Addison-Wesley Publishing Company, 1998).

For an evaluation of how broad media access has affected the course of international affairs, see James Rosenau's **"States and Sovereignty in a Globalizing World"** in *Understanding Globalization: The Nation-State, Democracy, and Economic Policies in the New Epoch*, by Rosenau et al., (Stockholm: Swedish Ministry for Foreign Affairs, 1998). A classic treatment of transparency in the space age can be found in Ann M. Florini's **"The Opening Skies: Third-Party Imaging Satellites and U.S. Security"** (*International Security*, Fall 1998). Florini examines the conflict between transparency and national sovereignty in **"The End of Secrecy"** (FOREIGN POLICY, Summer 1998).

Finally, some of Martin Libicki's own works on these subjects, such as **"What is Information Warfare?"** (Washington: Institute for National Strategic Studies, 1995), can be found on the Web site of the **National Defense University** or via the author's home page.

For links to these and other Web sites, as well as a comprehensive index of related FOREIGN POLICY articles, access **www.foreignpolicy.com**.