WIRED

May 2007

A Farewell to Arms

By John Carlin

For those on the ramparts of the world's sole superpower, the digital winds are blowing an icy chill through the triumphant glow of the post-Cold War.

People in Washington play lots of games, but none for higher stakes than The Day After. They played a version of it in the depths of the Cold War, hoping the exercise would shake loose some bright ideas for a US response to nuclear attack. They're playing it again today, but the scenario has changed - now they're preparing for information war.

The game takes 50 people, in five teams of ten. To ensure a fair and fruitful contest, each team includes a cross-section of official Washington - CIA spooks, FBI agents, foreign policy experts, Pentagon boffins, geopoliticos from the National Security Council - not the soldiers against the cops against the spies against the geeks against the wonks.

The Day After starts in a Defense Department briefing room. The teams are presented with a series of hypothetical incidents, said to have occurred during the preceding 24 hours. Georgia's telecom system has gone down. The signals on Amtrak's New York to Washington line have failed, precipitating a head-on collision. Air traffic control at LAX has collapsed. A bomb has exploded at an army base in Texas. And so forth.

The teams fan out to separate rooms with one hour to prepare briefing papers for the president. "Not to worry - these are isolated incidents, an unfortunate set of coincidences" is one possible conclusion. Another might be "Someone - we're still trying to determine who - appears to have the US under full-scale attack." Or maybe just "Round up the usual militia suspects."

The game resumes a couple of days later. Things have gone from bad to worse. The power's down in four northeastern states, Denver's water supply has dried up, the US ambassador to Ethiopia has been kidnapped, and terrorists have hijacked an American Airlines 747 en route from Rome. Meanwhile, in Tehran, the mullahs are stepping up their rhetoric against the "Great Satan": Iranian tanks are on the move toward Saudi Arabia. CNN's Christiane Amanpour, in a flak jacket, is reporting live outside the US embassy in Addis Ababa. ABC's Peter Jennings is quizzing George Stephanopoulos on the president's state of mind.

When suddenly, the satellites over North America all go blind ...

God, Voltaire said, is on the side of the big battalions. Not any more, He ain't. Nor on the side of the richest or even - and this may surprise you - the most extravagantly well wired. Information technology is famously a great equalizer, a new hand that can tip the scales of power. And for those on the ramparts of the

world's sole superpower, the digital winds are blowing an icy chill through the post-Cold War's triumphant glow.

Consider this litany. From former National Security Agency director John McConnell: "We're more vulnerable than any other nation on earth." Or former CIA deputy director William Studeman: "Massive networking makes the US the world's most vulnerable target" ("and the most inviting," he might have added). Or former US Deputy Attorney General Jaime Gorelick: "We will have a cyber equivalent of Pearl Harbor at some point, and we do not want to wait for that wake-up call."

And the Pentagon brass? They commissioned their old RAND think-tank friends, who combed through the Day After results and concluded, "The more time one spent on this subject, the more one saw tough problems lacking concrete solutions and, in some cases, lacking even good ideas about where to start."

Not that nothing is being done. On the contrary, there's been a frenzy of activity, most of it little noticed by Washington at large. A presidential commission has been established; the FBI, the CIA, and the NSA have created their own specialist I-war teams; interagency bodies, complete with newly minted acronyms like IPTF (Infrastructure Protection Task Force) and CIWG (Critical Infrastructure Working Group), have been set up; defense advisory committees have been submitting reports thick and fast, calling for bigger budgets, smarter bombs, more surveillance, still more commissions to combat the cyber peril.

Yet, for all the bustle, there's no clear direction. For all the heat, there isn't a great deal of light. For all the talk about new threats, there's a reflexive grasp for old responses - what was good enough to beat the Soviet Union and Saddam Hussein will be good enough to beat a bunch of hackers. Smarter hardware, says the Pentagon. Bigger ears, says the NSA. Better files, says the FBI. And meanwhile The Day After's haunting refrain is playing over and over in the back of everyone's mind: What do we tell the White House?

A little digitally induced confusion might be par for the course in, say, the telecom industry or even on the global financial markets. But warfare is something else altogether. And while the old Washington wheels slowly turn, information technology is undermining most of the world's accumulated knowledge about armed conflict - since Sun Tzu, anyway.

What is an act of war? What is an appropriate response? Who's the first line of defense? What does "civilian" infrastructure mean when 90 percent of the US military's communications travel over public networks? Are we ready for a bonfire of civil liberties in the name of national security? Do we need an army? A navy? An air force? Does it matter whether we have them? And how do you encourage free and informed debate about an issue of unimpeachable importance without setting off panic?

Interesting questions all, unless you happen to be the men and women who get paid to keep the United States - or any other country - sleeping safe within its borders. In which case, those questions are a nightmare.

For a crisp, succinct summary of I-war - not to mention a taste of the threat's reality - you could do worse than glance at the Chinese army newspaper, *Jiefangjun Bao*. The following summarizes speeches delivered at last May's founding ceremony for Beijing's new Military Strategies Research Center:

"After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the information age. Information warfare is a war of decisions and control, a war of knowledge, and a war of intellect. The aim of information warfare will be gradually changed from 'preserving oneself and wiping out the enemy' to 'preserving oneself and controlling the opponent.' Information warfare includes electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, network warfare, and structural sabotage.

"Under today's technological conditions," the summary continues, "the 'all conquering stratagems' of Sun Tzu more than two millennia ago - 'vanquishing the enemy without fighting' and subduing the enemy by 'soft strike' or 'soft destruction' - could finally be truly realized."

Please note that there's no namby-pambying about defending the motherland. A Chinese take on the Critical Infrastructure Working Group this is not. The object is to vanquish, conquer, destroy - as deviously and pervasively as possible.

That's one of the factors that makes I-war discussions so fraught: Like the technology that makes it possible, the landscape is vast, hard to visualize, and infinitely flexible. I-war can be the kind of neat, conceptually contained electronic Pearl Harbor scenario that Washington strategists like - collapsing power grids, a stock market software bomb (Tom Clancy's been there already), an electromagnetic pulse that takes the phone system out. Or it could be something completely different: An unreachable, maybe even unknown, foe. Grinding you down. Messing with your collective mind. Driving you slowly, gently nuts. Turning around your high-powered, fully wired expeditionary force in Somalia with a single, 30-second videoclip of one of your boys being dragged behind a jeep. Weaponry by CNN.

The question is whether the creaky old Cold War decision-making juggernaut is up to it. "It's gone from think tank to commission to task force," says one Senate staffer, "and then the White House has put it back out for another commission. Nobody wants to get near it, because it's being presented in such humongous terms." And because jumping in requires wrestling with some of the most contentious issues around, from civil liberties and cryptography to the size of the Pentagon budget - not to mention heavy doses of what still remains, for most of area code 202, mind-bendingly impenetrable technology.

The whole Washington mind-set may be part of the problem. "The threat is distributed," says Georgetown University computer science professor and crypto wars veteran Dorothy Denning, "but the government's first response is, 'OK, who's going to be in charge?' It's the age-old hierarchical approach, and I'm not sure whether it will work this time." Denning is notorious on the electronic privacy scene as a crypto hardliner, but on I war, she sounds almost forlorn. "The problem is that the technology leaps ahead of the security, and that's going to be with us forever. What we need to do is come to grips with our vulnerability and do the best we can." Hardly a Churchillian call to fight them on the beaches, and not exactly the kind of rhetoric that might get the blood stirring on Capitol Hill.

Looking at I-war through the conventional military prism is scarcely more inspiring. No weapons to stockpile. No US$50 billion panacea programs. No Ho Chi Minh Trails to bomb. No missiles to monitor. No rear bases - possibly no immediately definable enemy at all. The I-war threat is, by definition, so overwhelmingly unstructured that any attempt at a top heavy response could actually be worse than doing nothing. Nor will expensive new toys help: as the NSA's and the FBI's crypto

warriors are already finding out, most of the technology involved is simply software - easy to duplicate, hard to restrict, and often frustratingly dual-use, civilian or military. It doesn't take a nice, fat sitting duck of a factory to manufacture software bombs; any PC anywhere will do.

The writing on the wall? John Arquilla, a professor at the Naval Postgraduate School in Monterey, California, and a leading Pentagon I-war thinker, puts it bluntly: "We have spent billions in the last few decades on large, expensive aircraft carriers, strategic bombers, and tanks. The information revolution suggests nothing less than that these assets have become much more vulnerable and much less necessary." (See "Netwar and Peace in the Global Village," page 52.)

The Pentagon's immediate response is among the hoariest in the military playbook: Cover your ass. Its brand-new Defense Science Board Task Force, chaired by two former DOD assistant secretaries, went out on a limb to recommend expanded I-war training (there's already a School of Information Warfare and Strategy, part of the National Defense University, outside Washington) and tightened security for the US military's information systems - the ever-expanding category now known as C4I (command, control, communications, computing, and intelligence). The report did include a provocative call for legal authority to allow "DOD, law enforcement, and intelligence agencies to conduct efficient, coordinated monitoring of attacks on the critical civilian information infrastructure." And for good measure, it recommended spending $240 million to establish a permanent Red Team - a putative hostile foe, sort of a Day After team in reverse - to begin routinely probing key US information systems for weak spots. Total price tag: $3 billion over five years, enough to pay for a couple of B-1 bombers.

Play Number Two: Pass the buck. Says John Petersen, president of The Arlington Institute and a regular Pentagon consultant, "Any time things start to smell like something other than killing people and breaking things, people in the military start pointing in other directions" - which in this case means the intelligence community and law enforcement.

Spooks and cops may well be better suited to the task, at least for holding up the defensive end of I-war. But *better* is only relative. I-war trashes time-honored distinctions between law enforcement and intelligence, between Americans and foreigners, between the kinds of surveillance permitted at home and what starts at the water's edge.

Undaunted, the FBI has created a Computer Investigation and Infrastructure Threat Assessment Center, expanding the bureau's three existing computer crime squads to 56 nationwide - one in every major field office. More tellingly, an executive order signed by President Clinton last July created an interagency outfit called the Infrastructure Protection Task Force. Chaired by the FBI and including representatives from the DOD and the NSA, the task force is charged with developing a "threat model" and "countermeasures." To these ends it is mightily empowered to demand "assistance, information, and advice" from "all executive departments and agencies." Says John Pike of the watchdog Federation of American Scientists, "The IPTF reeks of what everyone always worries about: the nebulous control authority. There are people who were looking for a hunting license, and they seem to have gotten it."

One proposal quietly making the rounds on Capitol Hill is to let the NSA engage in domestic monitoring, partly on the theory that digital technology makes distinctions between "domestic" and "foreign" artificial. Where's the water's edge in cyberspace?

That's just one looming I-war flashpoint. Another is an adjunct to the raging crypto debate: despite broad-based encryption's obvious merit as part of an I-war defense, the NSA and the FBI oppose it out of hand, on the grounds - not entirely unreasonable - that it makes *their* mission of listening in on potential enemies more problematic. The NSA, in particular, is looking on mournfully as encrypted communications spread around the world, obscuring its view even as the threat of I-war dramatically raises the stakes. In closed-door hearings where "black" budgets are debated, a powerful collision looms. And your local representatives may eventually be asked to ratify some tricky decisions - just as soon as they finish figuring out how to read their email.

If you're looking for someone to talk to about the vulnerability of computer networks, it would have to be Howard Frank, director of Darpa's Information Technology Office. Frank was on the team that 25 years ago invented the Internet - Doctor Frankenstein, if you will, now quietly trying to protect his creation from hostile new forces swarming around it.

Frank, an amiable, courteous man, patiently answers questions and puts things in perspective. The Internet, he says, was never designed to survive a nuclear war. Claims that it was designed to be invulnerable are urban myth, he's happy to tell you.

Frank is a Day After veteran; he even supervised one of the sessions. But at one point in our interview, he lets slip a remark so melodramatic that we can confidently expect it to be written into a Hollywood I-war blockbuster. We're chatting about last summer's big West Coast power outages, when suddenly he exclaims, "Each time I hear about one of these things, I say to myself, 'OK, it's started!' And when I find out it really didn't, I just think we've bought some additional time. But it *will* start."

So what do we do? "We've created a technology over a period of 20 or 30 years. It's going to take 10, 20 years to create an alternative technology that allows us a more sophisticated set of defenses."

That long? Who knows? It's like the drug war, or urban dwellers' perennial battles against roaches. It's not hard to grasp the problem, but solutions remain evasive, slippery, beyond reach.

Not that no one's looking. Darpa, for instance, is actively soliciting proposals for "research and new technology development related to the survivability of large-scale information systems whose continuous operation is critical to the defense and well-being of the nation." They're talking serious business here. They're talking *survivability*. And what they have in mind is not just any infrastructure "hardening"; this is cutting-edge stuff, grounded in the latest theories of ecological computing - digital versions of genetic variation and immune response. "There are naturally occurring models of survivable systems provided by biological organisms, populations, and societies," declares Darpa's request for proposals. "This research program uses these examples for metaphors and guidance about how to design survivable information systems."

Well, good luck to them. In the shorter term, more immediately practical ideas are also being pursued. The Defense Science Board estimates that to harden up US information networks will range from $3 billion for a so called Minimal Essential Information Infrastructure - a dedicated emergency system to keep necessary services running - to a pie-in-the sky $250 billion (roughly the Pentagon's annual budget) to globally secure everything to top-of-the-line DOD "Orange Book"

standards. But the latter figure is vague, to say the least: from a technical point of view, it is essentially impossible to distinguish between the global telecom net, the US national network, and a single-purpose military one. Worse, nearly all those cables and switches belong not to Uncle Sam, but to highly competitive, deeply cost-averse private companies still glowing with satisfaction after their escape from Washington's regulatory shackles. A White House staffer who's been working on the issue puts it this way: "It's one thing to say to the private sector, 'You have a responsibility to defend yourself against hackers.' Fine, everyone's in favor. But if you suddenly say the threat is a foreign government or a terrorist group, there's no way in hell they're going to want to pay for that. They look at us and say, 'Isn't that your job?'"

The most concerted attempt to sort out those issues is being made by the Commission on Critical Infrastructure Protection, established by Clinton's executive order last July. Former Deputy Attorney General Gorelick described it in a Senate hearing as "the equivalent of the Manhattan Project." Chaired by Robert "Tom"Marsh, a retired US Air Force general with long-standing military-industrial ties, the commission is charged with acting as a liaison between the government - all the usual-suspect agencies are involved - and the private-sector companies that own and operate "critical infrastructure," from TV broadcasting transmitters to long distance phone and data lines. Public hearings are being held around the country; the ultimate aim is a report evaluating the scope of the threat and recommending strategies to counter it.

There are plenty of bright ideas out in the freelance I-war market. In fact, there's a whole cottage industry, starting with Infowar.com, a sprawling commercial Web site run by longtime I-war enthusiast Winn Schwartau (see "Information Warrior," *Wired* 4.08, page 136). William Church, editor of the London-based *Journal of Infrastructural Warfare (www.iwar.org/)*, proposes I-war "Special Operations Squads" with "one goal, and only one goal: go out and patrol for the enemy" - on the networks. ("It is a very small flick of the switch to go offensive with these teams," Church notes helpfully.)

More out-of-the-box thinking comes from Robert Steele, a retired US Marine and former CIA intelligence officer who heads a consulting firm called Open Source Solutions Inc. Steele argues for what he calls "SmartNation," a sort of electronic Neighborhood Watch in which "each individual node - each individual citizen - is educated, responsible, alert, and able to join in a networked security chain."

Michael Wilson, a shadowy "OpFor" (that's "opposition forces") consultant and frequent contributor to online I-war debates, argues for universal strong cryptography. "While we're at it, who knows that there isn't something even better at the NSA?" Wilson asks. "Open the technology up - get out the strong crypto, security, authentication, et cetera. Ship the scientists out from Fort Meade to computer hardware and software developers. Think of it as investing the Cold War peace dividend, to help strengthen the society to weather the next wars."

The idea of confronting the threat of I-war by, in effect, opening up national security does have its appeal. Marc Rotenberg, director of the Washington-based Electronic Privacy Information Center, sees the I-war debate as a possible doorway to a full-scale reexamination of national security and the institutions devoted to guarding it. "Now's the time to bring more of the NSA's activities into the public light. If there are these looming threats, you don't want to keep the debate locked up in the White House basement or the back rooms of the Pentagon."

In the strange-bedfellows way of so many information revolution debates, that's not a problem for an I-war insider like John Arquilla. "Unless we grapple with the problem that information warfare is not simply a military problem," he says, "we won't be able to grapple with I-war at all."

Downsize the Pentagon? Fund cheap I-warriors instead, to fight in the electronic shadows? Arquilla again: "Clearly there is an institutional concern about making radical shifts away from a hardware-heavy military. Nevertheless, budgetary constraints will ultimately drive us in this direction." He won't be drawn on specifics, but the possibilities are obvious enough - halve the Pentagon budget, for instance, and put the savings toward a massive upgrade of the country's networks, using tax breaks and other incentives as a lure. "What will make it possible will be someone pointing out the savings that could be realized,"Arquilla says. "Institutional redesign is hot, politically, and this needs to be an issue in the next presidential cycle." Calling Al Gore.

The good news is that we have been down this path already: in government as in industry, downsizing and efficiency go with the territory. The bad news is that the magic of the marketplace isn't very reassuring protection against, say, a team of underemployed Bulgarian computer scientists working for Saddam Hussein.

But it is a fair bet that, sooner or later, we will find ourselves stumbling toward a genuine national debate - not, one hopes, in the wake of a real electronic Pearl Harbor. Certainly no elected official is likely to challenge the plausibility of the I-war threat, so long as the risk exists that events might spectacularly contradict him. The issues will be how to go about countering the danger, and how to do so without setting off a mêlée over hot-button issues like domestic spying, privacy rights, "hidden" enemies, and official regulation of privately owned networks.

That's not just a tactical problem: when the FBI, the NSA, the CIA, and the Pentagon get together to talk about national security, a lot of people start reaching for their copies of the Bill of Rights. And when the threat everyone's talking about is from faceless foreign hackers, terrorists, and bomb makers - why not throw in a few child pornographers - it is a fair bet that paranoid demagoguery will not be absent. It's happened before: look at the 1950s. The best will lack all conviction, the worst will be full of passionate intensity, and the political fabric will start to fray.

All of which, of course, could sound a lot like what our Chinese friends call "soft destruction." As William Church says, "The most damaging form of I-war is political war or psychological war." And pretty much anything can be part of it: power outages, network breakdowns, clever disinformation campaigns - anything "to get the populace to feel that the country is going to hell."

Those whom the I-war gods would destroy, they first make mad.

John Carlin is a Washington correspondent for The Independent newspaper of London.