Neil Munro

Infowar: AK-47s, Lies, and Videotape

Information warfare is not just about "hacker war." Infowar is far broader and requires a much deeper reform of national security than simply adding a few thousand well-paid sysadmins.

Throughout the continuing wars in Rwanda and what was once Zaire, TV journalists and aid workers were used and abused by the warring parties. In 1994, the Hutus constricted the Western media while their hateful radio propaganda spurred the killing of 800,000 Tutsi men, women, and children without significant interference from outside. Then, after the Tutsis seized Rwanda, the Tutsi blinded the Western media, allowing them to kill many of the Hutu soldiers and their families in a Zairean refuge, without interference from Western media, publics, or governments.

All this was accomplished from 1994 to 1997, with very simple weapons such as AK-47s, machetes, and radios. And it stands in sharp contrast to the 1995 Bosnia and 1999 Kosovo crises, where comparatively modest Serbian atrocities—roughly 2,000 dead from late 1998 to March 1999—were magnified by global TV, pushing NATO to fling its computerized weaponry against the Serbs in 1995 and again in 1999. "Seeing the results of the atrocities on the [TV] news never failed to anger [Clinton]… You could just see him getting outraged," said Tony Lake, Clinton's former national security adviser. To date, it is not clear how the Serbs and Kosovars manipulated TV images of massacres to cause or avoid U.S. involvement.

Of course, TV is only part of why the two crisises developed so differently. The people killed in far-off Africa were, well, Africans, who lacked a major domestic lobby willing in 1994 to publicize their plight or to overcome the White House's fear of any Somalia-type entanglement. Moreover, the corrupt Zairean government in 1997 had no friends to call for help, whereas Kosovo was just down the road from the U.S.-created, tri-ethnic statelet of Bosnia, whose possible collapse would have undermined one of the U.S.'s self-declared foreign policy successes.

But the techniques of infowar played a central role in the outcome of these crisises. Not the media's usual infowar stuff about hackers, but the essential infowar, manipulating the flow of information to make the enemy bend. Or as the Tutsi's chief general, Paul Kagame, said, "We used communications and information warfare better than anyone. We have

JONATHAN CARLSON

As soon as ships and airplanes were first developed, they were put to military and political use. So it is the same with each new information device.

found a new way of doing things."

No one should be surprised about this. As soon as reliable ships and airplanes were developed, they were put to military and political use. So it is the same with each new information device.

One notable example, as described by BBC anchor Nik Gowing, in his 77-page report, "Dispatches from Disaster Zones": In late 1996, Kagame's Tutsi force let hundreds of thousands of Hutu refugees quietly return from Zaire to Rwanda. The orderly return was not marked by disease or murder, as many had claimed would happen. This peaceful episode painted the humanitarian activists as alarmist "Chicken Littles" and calmed Western observers, even as the Tutsi forces readied battle plans for their stealthy attack on the Hutu fighters and families that remained in their Zairean bases.

Throughout the attack on Zaire, which began in early 1997, few media or humanitarian organizations could get near the fighting. Roadblocks, demands for bribes, denying TV reporters of enough interesting footage to justify their expensive travel costs, the occasional killing and bullying of journalists, and distrust between the media and aid workers, all combined to minimize TV coverage. This was intended by Kagame, because he feared the emotional impact of TV coverage would create a public push for intervention strong enough to overcome Western politicians' reluctance to intervene. Thus Kagame's Tutsi fighters—in close cooperation with Laurent Kabila's Zairean rebels—had a free hand in destroying the Zaire-based Hutu fighters by attacking the refugee camps and scattering their occupants in the surrounding brush. Many of the refugees died in the brush, others were shot down by their pursuers; others returned to Rwanda under the watchful eye of the Tutsis. Many fleeing Hutus were located by Tutsi attackers when aid workers talked via radio or dispatched food and medicine to particular locations. No death toll has ever been completed.

All of this shows that infowar is far more than mere hacker war. And not surprisingly, the U.S. government is struggling to keep up.

During the initial round of massacres in 1994, the Hutu government used the Milles des Collines radio station to incite hatred and name individuals that were to be killed. While this was under way, U.S. government officials rejected the idea of jamming the radio station, but were willing to pay for a pro-peace radio station once the corpses had been buried. The peace radio station is based in nearby Burundi.

To help prevent a recurrence of the Rwanda disaster, U.S. officials also drafted a new President Decision Directive (PDD) on International Public Diplomacy. This directive, still unsigned as of April 15, gives the State Department the task of harnessing all federal tools—including the Internet and the Pentagon's six Commando Solo TV-broadcasting aircraft—to counter future "hate radio" with pro-peace messages. These pro-peace messages, say officials, can be routinely broadcast from the U.S. Information Agency, Western media outlets, and from Hollywood which—despite or because of its emphasis on garish violence—exports U.S. values of capitalism, peace, and trade.

Even the Internet can serve national security by spreading U.S. values. "We can build on our progress and use these powerful new forces of technology to advance our oldest and most cherished values: to extend knowledge and prosperity to the most isolated inner cities at home, and the most rural villages around the world … to deepen the meaning of democracy and freedom in this Internet age," said Vice President Al Gore.

But this modest PDD has taken years to draft, and even now may be wrecked by bureaucratic infighting despite its potential value in the Kosovo crisis. For example, the State Department objected until the public-diplomacy job was taken from the National Security Council and given to the State Department. Politically minded agency press secretaries objected to the prospect of a bureaucrat in the State

Department telling them what their boss should say in public, and civil agencies—especially the State Department—are still loath to accept anything that smacks of the Pentagon's infowar vision. These disputes could not be resolved during the early days of the Kosovo war, so in mid-May the White House hired an outside p.r. specialist to present the best possible face of the war.

But the Pentagon's infowar vision is very influential, largely because the Pentagon is the intellectual leader in the area. For example, its vision incorporates U.S. hacker attacks, U.S. hacker defenses, smart weapons, satellites, intelligence, public affairs, and psychological operations. Infowar, recently dubbed "Information Operations" by the Pentagon, "involves actions taken to affect adversary information and information systems while defending one's own information and information-systems." But Pentagon officials know this vision is far broader that its legal or political authority. Which is why Pentagon officials worked with the Justice Department to have President Clinton sign off on PDD 63. This policy, signed in May 1998, directs the law-enforcement officers at the FBI—but not defense officials—to prod companies until they safeguard their various critical networks upon whose health the nation depends. Since then, the FBI has been cajoling the banking sector, the oil and gas companies, the electricity utilities, the phone companies, and others to bolster their anti-hacker defenses. The implied threat? Failing to build up anti-hacker defenses will leave any company vulnerable to a crippling

Government officials know the infowar vision is also much broader than the government, often demanding more from the private sector than it can grant.

lawsuit should its customers be financially hurt by a major computer-security breakdown.

For itself, the Pentagon has tentatively decided to give the U.S. Space Command, based in Colorado, the job of defending the military's critical networks, and perhaps, of launching hacker-attacks against foreign targets.

Of course, all military units have some role to play in infowar—flying stealthy bombers, presenting a good image to the media, hiding an Apache helicopter-base in the Albanian hills, for example. But Space Command's role as Pentagon hacker-in-chief raises the ante; it requires some form of top-level strategy and attack-approval process. The strategy must address numerous issues: What kinds of cyber-targets are worth destroying? What cyber-targets are more useful operating than dead? How much collateral damage should the U.S. accept in cyber-attacks? Should the president approve each cyber-attack, or let a deputy approve each attack once war starts?

Government officials know the infowar vision is also much broader than the government, often demanding more from the private sector than it can grant. For example, U.S. companies are eager to sell China advanced satellites and other information technology useful to Chinese entrepreneurs and soldiers, provide good jobs to workers and profits to shareholders, but might also hurt national security. A telling example is the $450 million deal under which Hughes built two cell-phone satellites for China. They could be used to for routine phone calls but they could also be used to eavesdrop on business calls through the region, or even to provide cell-phone service to Chinese soldiers. Under pressure from the Pentagon and intelligence agencies, this deal was nixed by the U.S. government early this year, despite support from the Department of Commerce. For the foreseeable future, there will likely be an endless stream of these disputes—on encryption, fast computers, fiber-optic communications gear, tiny jet-engines, specialized furnaces, spare parts— although there are some efforts in Congress and the Pentagon to revamp the nation's export-control laws.

At the moment, these infowar-related disputes are fought ad-hoc in Washington among agencies, companies, and associated interest groups. It would be better, says said John Arquilla, a professor at the Naval Postgraduate School, Monterey, Calif., if the government took the plunge and developed a broad national security strategy for the information age, akin to the Containment Strategy the U.S. relied upon during the Cold War. This broad strategy should link the hacker war aspect of infowar to the public information aspect, implement incentives that push agencies to share vital information, establish a "guarded openness" export policy that balances the benefits from trade deals against harms to the nation's security, create a central coordinating group to implement this strategy, and set procedures to shape and direct U.S.-hacker attacks.

But this is a very ambitious agenda for a government that can't approve the International Public Diplomacy policy without lengthy infighting. Perhaps the more likely outcome will be the slow emergence of a broad policy out of ad-hoc agency plans and alliances, in other words, creating an infowar strategy while pretending one doesn't exist.

Whether this strategy will be too fractured, too modest, too ambitious, too secretive, or simply misdirected, we won't know for many years. Still, that's no different from the Containment Strategy, which survived 50 years of partisan domestic disputes, periodic wars, and extensive technological change before its success was confirmed by the collapse of the Communist empire. C

Neil Munro (nmunro@njdc.com) covers the politics of the technology business for *National Journal.*