Target: Yugoslavia (A Look into the Future)

From the Archive: NATO’s 1999 war on Serbia showcased some of America’s then-cutting-edge strategies for waging electronic sabotage against an “enemy,” including hacking computers and controlling information, wrote Robert Parry in real time.

By Robert Parry (Originally published on May 4, 1999)

At center stage and behind the scenes, NATO’s war for Kosovo is pressing the edges of modern “information warfare.” Through the early phases of the conflict, NATO concentrated its attacks on command-and-control centers, power stations and even propaganda outlets. Those attacks included sophisticated electronic assaults on computers directing Serb air defenses and so-called “soft bombs” to short out electrical lines.

But there are new indications that President Bill Clinton might be opting for a far more expansive high-tech “info-war” assault to punish the Yugoslavian government, its leaders and the nation’s economy for atrocities in Kosovo.

In such an electronic offensive against Serbia, U.S. intelligence has the secret capability to go much further than sporadic battlefield computer hacking and causing black-outs. U.S. info-warriors have the capacity to plant viruses in civilian computer systems, alter bank records, and generally wreak havoc on Yugoslavia’s infrastructure, from disrupting electrical utilities to shutting down the phone system.

U.S. government hackers could target government bank accounts used for purchasing military supplies or the personal accounts of Yugoslav leaders. Funds could be deleted electronically to frustrate the prosecution of the war or to punish selected Yugoslav leaders for “ethnic cleansing” in Kosovo.

Intelligence sources say the U.S. forces in the Balkans were ill-prepared for this broader info-war when the NATO bombing started on March 24, 1999. One reason was the difficulty of gaining a NATO consensus for exotic tactics.

So initially, the info-war focused only on the battlefield. Time magazine caught a glimpse of the U.S. capability in its reporting on the Pentagon’s successes in “taking down the Serbian air defenses.” The Pentagon cited “attacks, jamming and corrupting data, which the allies have fed into Yugoslav computers through microwave transmissions.” [Time, April 26, 1999]
A Bag of Tricks

Later, expert teams were mobilized and tasked to the Yugoslav theater. Then, after NATO approved expanded operations, the U.S. military began pulling surprises out of its technological bag of tricks.

The first widely noted application of classified techno-warfare occurred on May 2, 1999. A “soft” bomb detonated over a Yugoslav electrical plant, spraying carbon filaments over the power lines and causing short-circuits that blacked out most of the country for seven hours.

“We have certain weapons we don’t talk about,” said Maj. Gen. Charles Wald. In line with info-war strategies, he noted that an electrical outage “confuses command and control, it disconnects and confuses computers.”

Government sources say that President Clinton now is poised to go further in using some of the Big Brother capabilities that are featured in Hollywood thrillers, such as “Enemy of the State,” though the techniques are rarely acknowledged officially.

The sources said Clinton has authorized secret intelligence operations against Yugoslavia, but those sources were unwilling to discuss any details about the high-tech strategies. Countries, such as Yugoslavia, with relatively primitive computers running their economy are considered especially vulnerable to info-war attacks, according to experts in these strategies.

Moral Issues

Some info-war advocates also argue that computer sabotage is a far more humane way to wage war than the current practice of dropping bombs and firing off missiles. These advocates note the obvious: that electronic attacks do not carry the immediate physical risk to civilians that explosives do.

But there are ethical concerns, too, about attacking a nation’s computer infrastructure and severely destabilizing its economy. Plus, there are fears that a computer virus or a similar tactic could backfire and infect computers far beyond Yugoslavia.

In a rare media report on the sensitive topic, The National Journal recently observed that “relatively modest questions [have been] raised here at home by the United States’ undoubted ability to wage offensive information warfare by hacking into foreign computers to pilfer secrets, move funds, corrupt data, and destroy software.

“When such activities are planned for a narrow, routine, peacetime spy
operation, they are dubbed ‘special intelligence operations’ and must be approved by top officials, sometimes even by the president. But what if a more massive U.S. hacker attack was designed to wreck the computers that control an enemy’s banking system, electrical-power grid, or telephone network?” [National Journal, March 27, 1999]

While skirting clear confirmation of a U.S. offensive info-war capability, American officials occasionally do discuss info-war developments in the third person, as if the United States were not a participant in this new arms race.

On Feb. 2, 1999, for instance, CIA Director George Tenet stated that “several countries have or are developing the capability to attack an adversary’s computer systems.” He added that “developing a computer attack capability can be quite inexpensive and easily conceal-able: it requires little infrastructure, and the technology required is dual-use.”

Left unsaid in Tenet’s statement was that the U.S. government, with the world’s most powerful computers and the most sophisticated software designs, has led the way both in offensive info-war strategies and defensive countermeasures.

Other times, when info-war gets mentioned in the American news media, it is in the context of a real or potential threat from an “enemy” seeking to damage the United States and its allies.

On March 31, 1999, one week into NATO’s air war, NATO’s spokesman Jamie Shea prompted “info-war” alert headlines in U.S. newspapers when he complained that “some hackers in Belgrade” had caused “line saturation” at the official NATO Web site.

But NATO computer experts acknowledged that this low-grade harassment was more “spamming” than hacking and that no sensitive computer systems had been entered. [Washington Post, April 1, 1999]

**Revolutionary Potential**

The U.S. military demonstrated the revolutionary potential of information warfare during the Persian Gulf War in 1990-91. With air attacks and technical means, U.S. forces destroyed Saddam Hussein’s command-and-control structure even before concentrating on his tanks and troops.

Scattered journalistic reports at the time noted U.S. success in planting viruses in Iraqi military computer systems. Since the Gulf War, however, Washington apparently has applied info-war techniques sparingly.

Sources say covert info-war attacks have been limited to such national security
concerns as disrupting the financial operations of some South American drug cartels.

In one case study of a CIA high-tech “dirty trick” from the mid-1990s, U.S. intelligence reportedly learned of a drug lord’s plans to bribe a South American government official. After the money was transferred, the spy agency accessed the bank records and remotely deleted the bribe.

Besides stopping the bribe, the money’s disappearance spread confusion within the cartel. The recriminations that followed — with the corrupt official and the drug lord complaining about the lost money — led eventually to the execution of a hapless bookkeeper, according to the story.

By the mid-1990s, the potential for info-war had become such a hot topic within the U.S. military that the Pentagon hired an outside consultant to summarize some of the important lessons in a chatty 13-page booklet called “Information Warfare for Dummies.”

The booklet was designed to clue in some of the Pentagon’s more unplugged officers “given our department’s unrelenting focus on the topic.” The booklet starts out by explaining the first objective for any lap-topped GI fighting a future Information War [IW]: “Destroy (or weaken) the bad guy’s system and protect your own.”

The manual separates the more traditional military methods from the new high-tech techniques. “Assault technologies for the Information Warrior can be divided into ‘hard kill,’ involving physical destruction, and ‘soft kill,’ where the goal is electronic or psychological disruption,” the primer states. “Their commonality lies in their emphatic focus on information — destroying it, corrupting it, and denying it.”

The primer notes that more traditional information warfare will target an enemy’s battlefield command-and-control structure to “decapitate” the fighters from their senior officers, thereby “causing panic and paralysis.” But the primer adds that “network penetrations” — or hacking — “represents a new and very high-tech form of warfighting.”

Indirectly, the booklet acknowledges secret U.S. capabilities in these areas. In an easy-to-read style, the manual describes these info-war tactics as “fairly ground-breaking stuff for our nation’s mud-sloggers. … Theft and the intentional manipulation of data are the product of devilish minds. … Pretty shady, those Army folks.”

Disruptive Strategies
The primer also gives some hints about the disruptive strategies in the U.S. arsenal. “Network penetrations” include “insertion of malicious code (viruses, worms, etc.), theft of information, manipulation of information, denial of service,” the primer says.

But the booklet also recognizes the taboo nature of the topic. “Due to the moral, ethical and legal questions raised by hacking, the military likes to keep a low profile on this issue,” the primer explains. “Specific DOD references to viral insertions are scarce” in public literature, the booklet observes.

The ethical questions include: “Is penetrating another nation’s computer system somehow ‘dirty’ and ‘wrong’ – something the U.S. military has no business doing? Are electronic attacks against a nation’s financial transaction computers too destabilizing and perhaps immoral?”

Despite the Pentagon’s nervousness about these tactics, the booklet notes that they do have advantages over other military operations. “The intrusions can be carried out remotely, transcending the boundaries of time and space,” the manual states. “They also offer the prospect of ‘plausible deniability’ or repudiation.”

The booklet indicates that U.S. intelligence has found it relatively easy to cover its tracks. “Due to the difficulty of tracing a network penetration to its source, it’s difficult for the adversary to prove that you are the one responsible for corrupting their system,” the primer says. “In fact, viral infections can be so subtle and insidious that the adversary may not even know that their systems have been attacked.”

The primer outlines other Buck-Rogers-type info-war weapons, such as electromagnetic pulse [EMP] bombs. “The high-energy pulse emitted by an EMP bomb can temporarily or permanently disable all electronics systems, including computers, for a radius of several kilometers,” the manual says.

“Put simply, EMP weaponry fries electronic circuitry. EMP weapons can be launched by airborne platforms or detonated inside information centers (banks, corporate headquarters, telephone exchanges, military command posts). The explosion needed to trigger the electromagnetic pulse apparently is minor compared to a conventional blast, theoretically resulting in fewer human casualties.”

The manual stresses, too, info-war’s potential for high-quality “psyops and deception” to confuse and demoralize a targeted population. “Future applications of psyops may include realistic computer simulations and ‘morphed’ imagery broadcasts of bogus news events,” the booklet explains.
Though deception has always been part of warfare, the booklet argues that “it is the sheer qualitative differences offered by today’s information technologies that makes IW potentially revolutionary.”

Some military theoreticians call the info-war capabilities “a Military-Technological Revolution,” a phrase reserved for major breakthroughs such as the discovery of gun powder or the development of strategic bombing.

But the manual observes some dangers. The info-war attacks, especially viral infections, could backfire and harm U.S. interests.

**Recruiting Hackers**

The manual wonders, too, whether the Army will have success in recruiting “hacker-types and ‘nerds’.” Then, there is “the $64 question: will the hackers ‘go bad’ and given the fighter-jock mentality of the U.S. military, will the ‘nerd track’ be a career killer?”

More recent internal papers indicate that in the past year, the Pentagon has begun concentrating on how to maintain its dominance in the info-war field.

Rand’s National Defense Research Institute drafted a report entitled “Strategic Information Warfare Rising” and suggested to the Pentagon several scenarios for managing and sharing “strategic information warfare” [SIW] capabilities with allies.

One scenario holds that the United States “overwhelmingly dominates the SIW warfare” with “the world’s best offensive SIW tools and techniques, capable of penetrating any other country’s SIW defenses.” The United States could then pick which allies would come under its defensive umbrella.

Another scenario foresees the United States leading five to 10 countries with advanced SIW capabilities, but with other nations lacking the technical skills to break into “the exclusivity of the club.”

Other scenarios stress defensive rather than offensive capacities. But an underlying theme of the report is the unquestioned dominance of the United States in these fields. [Intelligence Newsletter, Jan. 28, 1999]

Other insights into U.S. info-war capabilities can be found in papers of military intelligence specialists from other nations. In articles in China’s Liberation Army Daily, Cols. Wang Baocun and Li Fei expressed alarm about the West’s impressive lead in sophisticated information warfare.

In an apparent reference to the U.S. military and its allies, the authors wrote, “some countries are now considering the organization and establishment of
computer virus warfare platoons.” [Liberation Army Daily, June 13 & 20, 1995]

It is not clear whether such “platoons” formally exist in the U.S. Army — though obviously the specialty does. It also is too early to tell whether such information warriors will play a significant role in the war for Kosovo.

But, depending how aggressive President Clinton chooses to be, the Balkan war could turn into an important testing ground for these new offensive tactics — the conflict could become what the president might call a warfare bridge to the 21st Century.