GlobalResearch
Center for Research on Globalization

Evidence of a Second Bush Coup?

By Robert Parry
Global Research, November 07, 2004
Consortium News 7 November 2004

Region: USA
In-depth Report: Election Fraud in America

Theoretically at least, it is conceivable that sophisticated CIA-style computer hacking – known as "cyber-warfare" – could have let George W. Bush's campaign transform a three-percentage-point defeat, as measured by exit polls, into an official victory of about the same margin.

Whether such a scheme is feasible, however, is another matter, since it would require penetration of hundreds of local computer systems across the country, presumably from a single remote location. The known CIA successes in cyber-war have come from targeting a specific bank account or from shutting down an adversary's computer system, not from altering data simultaneously in a large number of computers.

To achieve that kind of result, cyber-war experts say, a preprogrammed "kernel of brain" would have to be inserted into election computers beforehand or teams of hackers would be needed to penetrate the lightly protected systems, targeting touch-screen systems without a paper backup for verifying the numbers. [More on "cyber-war" techniques below.]

Though there's still no proof of such a cyber-attack, suspicions are growing that the U.S. presidential election results were manipulated to some degree. Voting analyses of some precincts in Florida and Ohio have found surprisingly high percentages for Bush. Others have noted that the large turnout among young voters and the obvious enthusiasm of John Kerry's voters would have suggested a better showing for the Democrat.

Exit Polls

But the most perplexing fact is that exit polls into the evening of Nov. 2 showed Kerry rolling to a clear victory nationally and carrying most of the battleground states, including Florida and Ohio, whose totals would have ensured Kerry's victory in the Electoral College.

Significantly, polls also showed Republicans carrying the bulk of the tight Senate races. However, when the official results were tallied, the presidential exit polls proved wrong while the Senate polls proved right.

Explanations from the architects of the exit-poll sampling system also sound specious. Their report said Kerry voters were simply more willing than Bush voters to answer the exit pollsters' questions. But this "chattiness thesis" seems more like a post-facto excuse than a serious argument.

Another explanation from some pundits was that the exit polls were adjusted by late in the day to rectify pro-Kerry exaggerations from the earlier samples. But that is not what happened. As the New York Times reported, "The presumption of a Kerry victory built a head of steam late in the day, when the national survey showed the senator with a

statistically significant lead, one falling outside the survey's margin of error."

Washington Post managing editor Steve Coll wrote in an online chat on Nov. 3 that "the last wave of national exit polls we received ... showed Kerry winning the popular vote by 51 percent to 48 percent – if true, surely enough to carry the Electoral College." [NYT, Nov. 5, 2004]

Through the late afternoon, exit polls did show Kerry's lead in some swing states shrinking, For instance, his lead in Ohio slipped from four points to one point. In Florida, his lead dropped from three points to one point. However, his edge in the popular vote seems to have held fairly steady at about three percent.

During the day, even Bush's aides informed the president that he was losing the election by about three percentage points, according to a source with access to information inside the White House. But Bush's political adviser Karl Rove reportedly voiced confidence that the vote would turn around. By evening, Bush was displaying a cool confidence that he would prevail.

Irregularities

Since Election Day, some computer irregularities have surfaced in Ohio and elsewhere.

Ohio elections officials said an error with an electronic voting system in Franklin County gave Bush 3,893 extra votes in suburban Columbus, more than a 1,000 percent more than he actually got. Records indicated that only 638 voters cast ballots in the precinct and that Bush's total should have been recorded as 365.

The Associated Press reported that Franklin County is the only Ohio county to use Danaher Controls Inc.'s ELECTronic 1242, an older-style touch-screen voting system.

Much of the suspicion about Bush possibly manipulating the vote totals has centered on touch-screen electronic voting machines made by Ohio-based Diebold, which has more than 75,000 electronic voting stations operating across the United States.

Diebold's chief executive is Walden O'Dell, a major Bush fundraiser. In an invitation to one Bush fundraising event at his mansion in Columbus, O'Dell wrote that he was "committed to helping Ohio deliver its electoral votes for the president." He later expressed regret at his choice of language. [The Plain Dealer, Sept. 16, 2003, posted at Diebold's Web site .]

One Kerry insider told me that Democratic suspicions also were raised by Republican resistance to implementing any meaningful backup system for checking the results on Diebold and other electronic-voting machines. For its part, Diebold denies that its systems are vulnerable to computer hacking, calling such allegations "fantasy." [See Diebold's statement .]

Dirty Tricks

Another reason for suspicion about manipulation of the Nov. 2 vote is the Republican Party's long history of electoral dirty tricks, which I detail in my book, Secrecy & Privilege: Rise of the Bush Dynasty from Watergate to Iraq .

In 1968, Richard Nixon's campaign reportedly sabotaged Vietnam War peace talks to help ensure his victory. In 1972, burglars working for Nixon's reelection campaign broke into Democratic offices at Watergate.

In 1980, George H.W. Bush and other Republicans allegedly interfered with President Jimmy Carter's negotiations to free 52 hostages held in Iran. In 1992, Bush's administration was implicated in an illegal search of Bill Clinton's passport file. In 2000, George W. Bush sent a team of thugs to disrupt recounts in Florida and eventually got the U.S. Supreme Court to prevent a full counting of disputed ballots.

Now the question is whether Republicans have engaged in some high-tech dirty tricks to alter the outcome of a U.S. presidential election.

'Cyber-War'

The highly secretive practice of "cyber-warfare" has advanced far more than many Americans understand, with U.S. intelligence agencies pioneering methods for surreptitiously entering enemy computer systems.

Through the 1990s, the CIA and the U.S. military aggressively expanded "cyber-war" capabilities, bringing online powerful computer systems and recruiting some of the nation's best hackers, intelligence sources say. During the CIA's recruitment rush, some hackers were hired despite criminal records and questionable backgrounds. One got in trouble when he was found masturbating in front of his computer screen.

By the mid-1990s, cyber-war – also known as "information warfare" – was such a hot topic within the U.S. military that the Pentagon produced a breezy 13-page booklet called "Information Warfare for Dummies."

The primer said traditional information warfare would target an enemy's battlefield command-and-control structure to "decapitate" senior officers from their fighters, thereby "causing panic and paralysis." But the primer added that "network penetrations" — or hacking — "represents a new and very high-tech form of warfighting."

Indirectly, the booklet acknowledged secret U.S. capabilities in these areas. The manual described 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."

The primer also gave 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 said.

The booklet also recognized the sensitivity 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 explained.

Despite the Pentagon's nervousness, the booklet said the cyber-war tactics do have advantages over other military operations. "The intrusions can be carried out remotely, transcending the boundaries of time and space," the manual said. "They also offer the prospect of 'plausible deniability' or repudiation."

The booklet indicated 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 said. “In fact, viral infections can be so subtle and insidious that the adversary may not even know that their systems have been attacked.”

Drug Scam

U.S. intelligence sources described one case study of a CIA high-tech “dirty trick” that worked in the mid-1990s. After learning of a drug lord’s plans to bribe a South American government official, the spy agency waited for the money to be transferred and then accessed the bank records to remotely delete 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.

During the war over Kosovo in 1999, U.S. government hackers tried to expand on these strategies, targeting Serbian computer systems and government bank accounts. By most accounts, the cyber-war attacks on Serbian targets achieved only limited success.

While avoiding clear confirmation of a U.S. offensive cyber-war capability, American officials occasionally have discussed the topic in the third person, as if the United States were not a participant in this new arms race.

On Feb. 2, 1999, for instance, then-CIA director George Tenet said “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 concealable.”

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 “cyber-war” strategies and defensive countermeasures.

With questions lingering about discrepancies between the Nov. 2 exit polls and Bush’s final tallies, some Democrats are wondering whether the intelligence community’s cyber-war capabilities may have come home to roost.

Robert Parry, who broke many of the Iran-Contra stories in the 1980s for the Associated Press and Newsweek, has written a new book, Secrecy & Privilege: Rise of the Bush Dynasty from Watergate to Iraq. It can be ordered at secrecyandprivilege.com . It’s also available at Amazon.com .

Articles by: Robert Parry