Seattle mess muddied up the message

by Billy O'Keefe
Campus Correspondent
Columbia College
December 06, 1999

There was a whole lotta chanting going on last Wednesday, Dec. 1, as I made the second of three trips from one of my classes to the student center. On the sidewalk, positioned in front of a large pane of glass looking into center, some students were holding big signs that sported slogans in large, demanding print.

I tried to get a good look at what the signs said, but the group was huddled in a semicircle of sorts, and the messages were obstructed. The members of the group — there were probably five people involved, although I can't say for certain — were also boisterously chanting a rhyme, the words of which I could barely understand, save for what I think was the phrase "open admissions."

All I can say for sure was that it was loud — loud enough to stop students in the doorway, loud enough to turn heads on the other side of the student center's glass, and loud enough to drown out any sort of curiosity those passing by might have had. If you wanted to know what was going on, you couldn't ask. They were too busy putting on a show to even hear you.

Don't know what's going on? Sorry, you're in the dark and you're not getting out. And if that's the case, you just chuckled and carried on your way. That's what I did on two separate occasions, and that's what a drove of students in front of and behind me did. Believe me, I checked. I'm not just making assumptions here.

Nearly 2,000 miles away in Seattle, the same bucket o' madness had spilled its guts a day earlier, only for a much larger cause and at a degree far more extreme. Fires were blazing, windows were shattered, and the tear gas in the air gave oxygen a run for its money. People screamed this, people shrieked that, and activists and ordinary folks were dragged away kicking and screaming by authorities. Damn the man. The protests continued the next day, and while the violence had subsided for the most part, the bedlam had not lost steam at press time.

So hey, here's a question: do you even know what happened? Do you have ANY idea what cause or causes these people were fighting? Don't be ashamed if you don't. Even if you're one of those dubious folks who can't even name the vice president of this country, you're a long way from alone this time. Here's the skinny (and a skinny skinny at that): the World Trade Organization was in Seattle last week for a series of meetings about, well, world trade. Critics have chastised the WTO for insensitive practices against workers and the environment, citing the respective abuse and abundance of poor working conditions and unsafe, genetically-modified (g.m.) crops that pop up in the foods we eat every day. They also believe that the WTO is far more privy to the wishes of large corporations and the almighty dollar than those of workers and consumers. In both respects, I agree.

But this is where it gets ugly. As is allowed, a nonviolent display of civil disobedience was planned by commoners and activist groups like the Direct Action Network whose name contains such misused words as "Direct," "Action" and "Network."

PHOTO: AMBER LEWIS

Three anarchists break from attacking "global capitalism."

Thousands of people showed up. They yelled, they chanted, they rhymed like a bunch of white Biz Markies. Then some people — a small number, to be fair — started smashing the front windows of outlets, such as the Gap and Starbucks, and tagging the ruins with yet more slogans. Among them: "Destroy the Gap" and "No sweat shops."

So is it about food, clothes, workers, the environment, or all of these things? To be honest with you, I have no idea. I was hoping someone could put down their brick and tell me. Too bad I'm not ready for the crash course these folks are trying to teach an entire country. Few people are. And now a lot of well-meaning people who were quietly bringing the issue to the public's consciousness are now going to run into a wall of confusion, anger and indifference. That's what happens when you break things to make a point. But that doesn't matter to some of these people, who would rather make a headline than any meaningful impression on anyone. So we have no choice but to dive into this mess headfirst, only to be confused by it all and stop caring in a few (circle one) weeks/months/years.

And make no mistake about it: people will stop caring, and that's only if they give a donkey's bum in the first place. Who's to say anyone will? Whatever this cause shapes up to be, it will be seen first as a violent, ironic embarrassment in which people tried to save the planet by setting it ablaze. The day after the riot, I overheard a girl likening the melee to the Civil Rights movement in the 1960's. That would be worth a good laugh if she were alone in that belief, but I know she's not. I'm sure many of the people who were high on tear gas last week felt the same way, like they were a part of something special.

Not likely. Not even close. When men and women like Martin Luther King, Jr. and Rosa Parks fought for their freedoms, they did it with eloquence — King by educating the common man with a mix of poetic and common sense, Parks by simply living the life she felt she'd earned. They didn't spend hours of their lives writing slogans, dressing up in costumes and looting tech vests. But they did take a once-scornful public and force it to realize just how wrong it had been all those years.

That didn't happen last week, either on my campus or in Seattle. Those demonstrations were met with anger, head-shaking, shrugs and laughter, on behalf of those who fought not just against the cause, but for it too. Enlightenment? Not on the list, sorry. Progress? Only if you like illusions. Change? Yeah, right.

Military girds for upsurge by hackers at the Y2K rollover

by Steve Goldstein
Knight-Ridder Newspapers
December 01, 1999

ARLINGTON, Va. — In a large windowless room of a nondescript office building a few miles from the Pentagon, the war of the future is being waged.

The field of battle is several dozen flat-screen computer monitors that show Department of Defense communications. Six screens display selected computer traffic, though one during a recent visit was tuned to the Weather Channel. If fears of a concerted cyber attack on the U.S. military are realized — what Deputy Defense Secretary John Hamre has called an "electronic Pearl Harbor" — this room, the Global Network Operations and Security Center, is where the battle will be won. Or lost.

Between 80 and 100 unauthorized "intrusions" of Pentagon computers are reported each day; about 10 require investigation. Most attacks come from "ankle biters" — hackers who just want to annoy — but some are aimed higher up, at the nerve system of the nation's defenses.

Alarmed by a dramatic increase in cyber attacks, the Pentagon is reorganizing its computer network defense. A September report by the watchdog General Accounting Office concluded that there were "serious weaknesses" in the Department of Defense's information security.

Moreover, the rapidly approaching Y2K rollover has military officials wondering if they will be able to distinguish between a network intrusion and the millennium computer glitch. Capt. Bob West, deputy commander of the Joint Task Force on Computer Network Defense, said there was real potential for a "crippling" attack at any time because of "substantial" vulnerability, especially in the network that handles non-secret communications — the NIPRNET (Non-classified Internet Protocol Router Network).

According to the Defense Information Systems Agency, the number of reported network intrusions has increased dramatically, to more than 18,500 this year compared with 5,844 in 1998. The Pentagon reported only 225 unauthorized network intrusions in all of 1994.

"The NIPRNET is really vulnerable; it has over two million hosts," West said in an interview. Information that can be accessed and misused includes troop locations, orders for spare parts, transportation logistics, names of military spouses, even credit-card and telephone numbers.

"It's a sensitive but unclassified network," said Gen. Thomas B. Goslin Jr., director of operations for U.S. Space Command, which recently assumed control of computer network defense. "A lot of information could tell you about where we might be going" in an operation.

The Pentagon also maintains a classified network, the SIPRNET (Secret Internet Protocol Router Network), but officials are reluctant to shift a lot of currently unclassified information to secret cover. "Once you put things on a secure network, you put some constraints on yourself," Goslin explained. Goslin declined to answer whether the SIPRNET had been breached.

> *"We're learning just like the rest of the world that the promise of the Internet is that it gives us so much capability, but also so much vulnerability in security."*
>
> -Gen. Thomas B. Goslin Jr., director of operations for U.S. Space Command

"There are people who have tried to get into that particular network; I don't want to talk about it," Goslin said.

The Pentagon is a tempting target, West said. "A hacker who says he's gotten into military systems has a badge he wears proudly," he said.

West and others attributed the surge in reported attacks to the rapid growth of the Internet, and advancing skills of computer users. And better detection systems have caught intrusions that probably would not have been reported before.

But the GAO report said that "serious weaknesses in information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose and destroy sensitive DOD data."

West acknowledged that information technology was a double-edged weapon. "We're learning just like the rest of the world that the promise of the Internet is that it gives us so much capability, but also so much vulnerability in security," he said.

The Pentagon is trying to upgrade the software for intrusion detection systems, train military personnel as security experts, and reexamine the traffic allowed on nonclassified networks. The millennium rollover will provide a test. Although DOD systems have been made Y2K-compliant, military officials worry that they are susceptible to an attack.

"It's certainly a golden opportunity," said West, cautioning that he had not seen intelligence warning of particular attacks.

Apart from concern that hackers consider New Year's a prime time for mischief, there is some worry that intruders have planted codes disguised as Y2K protection but set to go off Jan. 1, like a time bomb.

"We have some indication that there will be more sophisticated-type people trying to gain access under the guise of a Y2K problem," Goslin said.

For the Pentagon, computer network defense is an effort that now involves hundreds of people and billions of dollars annually, West said. The Joint Task Force, originally established in December 1998, has been put under the authority of U.S. Space Command at Peterson Air Force Base in Colorado. The command also will oversee the computer network defense components operated by the Army, Air Force, Navy and the Marines, including their CERTS — computer emergency response teams. In wartime, the task force will be dispatched to set up top-secret computer networks for field commanders. Next October, U.S. Space Command will begin developing ways to attack the enemy's computer-dependent weapons and systems.

Some of this "non-kinetic" warfare occurred during the bombing campaign against Serb forces in Kosovo. The emphasis now, however, is defense. Gen. Robert Shea, Marine computer defense commander, described the effort as a "long, long march."

"Before we get to the end of the march," he added, "there's going to be some ambushes." The first ambush was self-inflicted. A 1997 war-game exercise known as Eligible Receiver showed that sophisticated hackers (in this case from the National Security Agency) could cause power outages and 911 emergency phone system overloads in a number of cities. They also reportedly gained "supervisory-level" access to dozens of military networks, disrupting e-mail and phone traffic.

A real attack occurred from January through March, described by officials as a "sustained, well-resourced intrusion." The matter is under investigation by the FBI, amid reports that Russia might have been involved. No one is commenting, even off the record. Attacking a DOD Web site is the usual modus for the "ankle-biters." But West said officials did not regard defacing a Web site as a big deal because there was no "operational impact."

"It's when the hackers get into the so-called (dot).mil environment that real trouble can occur. These attacks most often happen when the United States is engaged somewhere militarily. NATO's air campaign in Kosovo brought a rash of computer intrusions.

An intrusion-detection system produced jointly by the government and commercial ventures has proved useful only for monitoring intrusions after hackers have broken in — not for alerting officials to suspicious entries as they happen. "They let you know after the barn door has been opened," Shea said.

In fact, many attacks may at first look innocent. For example: a staff person is going through some files, which seems fine until someone discovers that the staffer is actually on leave. The task force members look for anything on the network that is not normal, or is occurring outside a regular cycle of traffic.

"More often than not we see something that looks funny and it's not such a big deal," said West. "The real sophisticated ones don't want to be seen." When an intrusion is successfully traced, it typically is handed off to the FBI's national infrastructure protection agency.

"The military is not going to show up on someone's doorstep," said Maj. Michael Birmingham, a spokesman for U.S. Space Command. A computer hacker who attacked the White House Web site this year pleaded guilty to a felony in November, and was sentenced to 15 months in federal prison and a $36,000 fine.

But attribution is mostly a needle-haystack exercise. West said foreign-based hackers often entered systems through Canadian or American university sites, making it difficult to trace the origin of the attack. And mostly, the hackers don't have a set destination. "They don't go where they want to go," West said. "They go where they can."

The Pentagon is now building redundant communications networks, so that hackers can't see how the military is responding to an attack. And they are trying to increase the recognition speed of intrusions. Military officials do not want to have to immediately retreat and regroup when cyberwar breaks out.

"Today we are primarily reactive," West said. "We monitor the network. We use intelligence reports. We want to become more proactive and be able to predict when malicious activity might occur."

Texas couple find $300,000 in brown paper bag

Knight Ridder Newspapers
December 07, 1999

DUCANVILLE, Texas — Serendipity smiled on a Duncanville couple over the weekend, but they apparently chose safety instead. Police said a woman and her husband stumbled upon a brown paper bag Saturday afternoon in the middle of a Red Bird street. Without looking inside, the woman said, she presumed it contained schoolbooks left behind by an absent-minded youth.

But inside the sack was nearly $300,000 in cash, a 9 mm chrome handgun and 18 rounds of ammunition.

"The gun would lead the citizen to believe that this is obviously from some kind of criminal offense," said police Deputy Chief Danny Garcia. "Having kept that money, it may have turned into the worst decision anybody can make."

In an interview Monday, the woman described the Hollywood-like scenario, saying "I started hyperventilating" after examining the bag's contents. The couple flagged down a Dallas officer, who himself gasped at the amount of money inside. He immediately called a supervisor to the scene, a police report states.

The woman stood across from a Christmas tree and a bevy of red stockings as she described feeling more fearful than proud. She didn't want her identity revealed and sought no publicity for her actions. Although citizens routinely report finding sums of money in the hundreds and even thousands, department officials couldn't cite an instance in which a Dallas resident found so much money at one time. Chief Garcia, who last month presented an award to two men who turned in $2,000 that they had found in an Oak Lawn apartment complex, termed this case "amazing."

Police are now working to determine the origins of the money. Detectives will check robbery and missing property reports for any possible connections, as well as examining the money itself for any signs of narcotics. Investigators will also wait to see if anyone calls to claim the money. Although they're certain that amount of money will attract more than a few phone calls, the claimant will have to know details about the money and have a credible story about how he or she lost it.

It's no leap of logic to presume that the loot could be related to drugs, because the department's narcotics division routinely executes search warrants that yield "extremely large amounts of money," Chief Garcia said.

If police can't link the money to anyone within 60 days, state law states that the investigation becomes a game of finders-keepers. The woman and her husband could officially apply to secure all of the nearly $300,000. The woman indicated that her family might place a claim on the money. "But that has some responsibility that goes with it," Chief Garcia said, referring to the possible danger of claiming the money. (Dallas Morning News staff writer Connie Piloto contributed to this report.)

Okla. shooter used dad's gun

TMS Campus
December 07, 1999

FORT GIBSON, Okla. (TMS) — The 13-year-old boy who opened fire on his middle school classmates used his father's 9mm semiautomatic handgun, officials said at a Tuesday morning news conference. The gun was purchased at a Wal-Mart.

Meanwhile, President Clinton, in Washington, D.C., said investigators from the FBI and Bureau of Alcohol, Tobacco and Firearms were on the scene in Fort Gibson. "Our prayers are with each of the children and their families," Clinton told reporters.

On Monday, the seventh grader fired the gun at least 15 times on the campus of Fort Gibson Middle School, wounding four students before he was subdued by a school teacher.

Police Chief Richard Slader said the student had more ammunition available. The gun was registered to the youth's father, although it was not known when it was purchased, Slader said. The boy's name is not being released, but the news reports say students at the school identified the shooter as Seth Trickey.

The day after the shooting, classes resumed. Many students who typically ride a bus to school were brought by their parents. Local police were on hand, telling students to enter to through the back doors of the school.

Officials have said the boy did not have any previous record of wrongdoing. He's been described as a good student, active in his church and popular. Prosecutors cannot charge the teen as an adult unless one of his victims dies. Of his victims, a 12-year-old girl, suffered the worst injury — a shot to the cheek. She was listed in fair condition on Tuesday. In addition, a 13-year-old was treated for a wound to his forearm and another 13-year-old underwent surgery for a leg wound. Brad Schindel, 12, was shot in both arms. Fort Gibson is 50 miles southeast of Tulsa.