LORAL
Data Systems

SECURITY
N·E·W·S·L·E·T·T·E·R

Volume 1 | A quarterly awareness briefing for defense contractor employees | Number 2

KGB Training Hackers as Computer Spies

A specter is haunting the U.S. — the specter of Soviet computer hackers who are now being trained to break into Western data bases.

Earlier this year, the arrest of three West German mercenary computer hackers on suspicion of supplying sensitive computer information to the KGB has raised concerns among security experts about the growing problem of computer espionage.

KGB interest in penetrating computer systems isn't new. For years, this Soviet intelligence agency has been on the prowl seeking new computer designs and, where possible, purchasing advanced computers or, if necessary,

stealing them. But Dr. Stephen M. Meyer, an associate professor at the Center for International Studies at the Massachusetts Institute of Technology who specializes in Soviet military affairs, says it's probably the GRU, Soviet military intelligence, that's more involved in training hackers to penetrate databases in the West. "One must assume that the GRU is developing the same kind of capability in some of their people that our people at NSA have to break into computer networks," he added.

Dr. Loren R. Graham, a specialist in Soviet science and technology policy at MIT, told the *Employee Security Connection* that he doesn't have any hard evidence that the Soviets have their own trained hackers, "but everybody I talk to assumes that they're doing the same thing that we're doing to them. Only we've been at it much longer and we're better at it."

Until recently Soviet intelligence was forced by circumstances to use the services of a third country *khaker*, a new Russian word for "hacker." But now the Soviet intelligence community is going one step further by training its own hackers as computer spies.

It's going to take years, according to Dr. Graham. "The Soviets have created special schools where they're training young people to be thoroughly at home with computers," he explained. "I've visited this kind of a school. It's unlike our spontaneous hacker culture created by free spirits who become so obsessed with computers that most of their academic careers fall by the wayside. Our own institutions didn't purposely decide to create a hacker culture.

Continued on page 7.

In This Issue. . .

'Espionage' is Out, 'Intelligence' is In. 2

A Kinder, Gentler KGB. 3

Drug Facts at a Glance. 4

Telemarketing Fraud. . . Thieves Dialing for Dollars 5

KGB Intensifies Spy Recruitment Effort. 6

DIS Shifts Inspection Focus. 8

"Security awareness is job security. . . it doesn't end when you leave the office. Think before you speak."

'Espionage' is Out, 'Intelligence' is In

You've watched the scene in many a sitcom: an injured party in a bar asks for a lawyer, and 25 members of the legal community rush the victim, business cards in hand. But what if you went into your after-work watering hole and called for a corporate spy? You might not have them rush you with their business cards flashing, but you can bet they're there.

Corporate espionage, business intelligence of late, is thriving, and your company is a target. Guaranteed! But the trenchcoats are gathering dust in the closets, freshly pressed suits, crisply laundered shirts, power ties and wingtips sales are up.

There's a subtle shift taking place in corporate espionage—it isn't called corporate spying anymore. It's been upgraded. Now, the sleuths and purveyors of corporate-sensitive information call their game competitive intelligence or business intelligence. The end-result, objectives and goals remain the same, only the name and the fashion plate have changed.

Competitive or business intelligence is a formal, systematic approach to collecting and analyzing data about competitors—about product, corporate, and marketing and sales strategies. What makes your company tick? Why are sales up or down? How much money is budgeted for R&D? How many employees do you have? What are their salaries? Their backgrounds?

Wait a minute, isn't this kind of thing illegal? Not at all. In fact, it has been estimated that as much as 95% of competitive intelligence gathered and analyzed in this country is accomplished legally and ethically. Competitive intelligence is gleaned from many sources, with much of the information readily available for anyone willing to take the time to ask and search for it.

Annual reports, and other financial reports such as 10-Ks and 10-Qs can be obtained from any company whose stock is traded in the public market. Press releases flood the mail and fax machines. Conversations are overheard everyday at lunch or over coffee everyday. The press covers anything that moves

It isn't called corporate spying anymore

But critical information is also obtained directly from employees, in face-to-face encounters and over the telephone. Competitive intelligence analysts use a variety of methods to gain access to company employees. Many pose as reporters, stock or investment analysts, market researchers, insurance analysts or brokers, and as association members.

Like a counterpart in the CIA, the business intelligence analyst is seeking trends and patterns in business. Japan's major companies are fielding armies of business intelligence collectors and analysts.

Mitsubishi, one of Japan's corporate conglomerates, has two floors in New York City's Pan Am building devoted to the collection and analysis of business and industrial information that is telefaxed back to the home office in Japan for further analysis.

In a softening economy, competitive intelligence activities are bound to escalate, so extra care should be taken to avoid sharing sensitive company data. And here are a few tips for preventing the disclosure of sensitive information:

- The company's public affairs or public relations office is the appropriate contact for outside callers seeking corporate information.

- If you do talk to people outside the company, be certain you know who you're talking to. If you get a telephone call from an investment analyst, market researcher or reporter, get a telephone number and call back after checking with directory assistance. If the phone numbers don't match, you could be a target for "information acquisition."

- Critical information is frequently delivered electronically via fax machines. So avoid placing fax machines in open uncontrolled areas where the output can be observed by others. Unless you've done a thorough electronic sweep recently, it should be assumed that any information passed by fax, telephone, electronic mail or telex can be intercepted.

Competitive intelligence has become so commonplace and routine that organizations must constantly be on the defensive against losing precious information. Most major companies freely admit today that they formally gather and analyze intelligence. Just a few years ago, virtually no one even admitted to engaging in industrial espionage.

Terror Close to Home

While Americans have long viewed terrorism as a threat overseas, the war on drugs may bring the threat closer to home, according to a series of witnesses who testified before Congress recently. Drug lords have illustrated their ruthlessness and unhesitating use of weapons and other terrorists acts when their organizations are threatened. "If they (drug leaders) mount a campaign of blood running in the streets, I can't assure you that we would be in a position to pre-empt it," said Oliver B. Revell, Chief of Investigations for the FBI.

"They have dealt in blood since their inception," Revell added. He expects the first wave of violence to be against American targets, both personnel and U.S. facilities, in Columbia, home of the powerful drug cartels. Revell and others testified before the Senate Governmental Affairs Committee. "It's easier for them to operate there," Revell said, "but that does not mean we are not vulnerable here in the United States." The Columbian cartels have established powerful, extensive distribution networks in the U.S. and have carried out assassinations in this country, primarily drug traffickers who have crossed these organizations.

A Kinder, Gentler KGB

A new feature film that premiered in Moscow recently, starring none other than the KGB, is part of the Soviet Union's charm offensive that shows the secret police as your plain folks friends next door, your average Joe (but not as in Joseph Stalin).

Viewed on opening night by the foreign press corps, harsh critics of the infamous intelligence and secret police organization, reporters were given the rare opportunity to interrogate the chief of the KGB.

The film, *The KGB Today*, is a propaganda piece intended to convince domestic and foreign audiences that the KGB is nothing more these days than an easy-going law enforcement agency. The western press responded to parts of the film with disbelieving laughter when Novosti news agency tried to present the KGB as "good neighbors."

At the forefront of the public relations blitz is Vladimir Kryuchkov, chief of the KGB, who explained to an Italian Communist Party newspaper, "Violence, inhumanity and violation of human rights have always been alien to the work of our secret services." Kryuchkov was appointed to his post in October, 1988.

Fifty-five minutes in length, the film, produced by the Soviet press agency, is being shown throughout the Soviet Union to help counter the unsavory reputation of the KGB.

Novosti, which heartily endorsed the KGB in the film, is believed to have ties to the KGB. A recurring theme in the *The KGB Today* is that all nations carry out intelligence activities, and the KGB is no worse than its Western rivals. In fact, according to the movie, the KGB spies with a greater sense of morality than does its competitors.

The film glosses over the NKVD, the predecessor of the KGB in the Stalin era, portraying that organization as a victim of the purges at the time, not as a perpetrator. Also, the film doesn't mention the violence associated with the KGB in its handling of Soviet dissidents in the 1960s, '70s and early '80s.

But according to KGB Col. Igor Prelin, responsible for the agency's public relations, "when dealing with dissidents, everything was done according to the laws we had then."

German Hackers on KGB Payroll

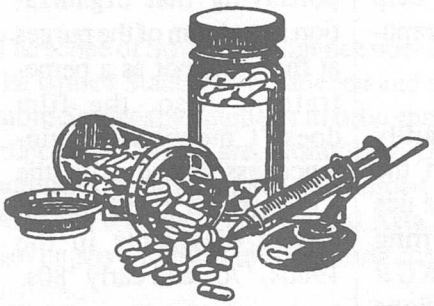
Three computer hackers thought to have given the Soviet Union information from industrial and military computers worldwide have been indicted on espionage charges by the West German government. Secrets from 12 western nations, including the U.S., were said to have been given to the Soviets by the three computer hackers.

The breakup of the spy ring is considered to be a major blow to the Soviets, according to the West German government. Kurt Rebmann, chief federal prosecutor in the case, said it was the first time his office has prosecuted hackers for violations of national security.

The range of information provided to the Soviets is currently unknown, but the espionage activities had been in operation since at least September 1986. The hackers were first detected by a U.S. computer specialist. The Soviets paid approximately $49,000 for the information.

Computers in the U.S., West Germany, Britain, France, Switzerland, the Netherlands, Canada, Japan, Hong Kong, Norway, Austria, and Italy were broken into by the three, who are identified only as Peter C., Dirk B., and Markus H. They were originally arrested in March of this year.

SECURITYbriefs



Drug Facts at a Glance

Here's a quick look at the drug problem facing America, based on material from the American Council for Drug Education, the National Household Survey on Drug Abuse, and the U.S. Government.

How Many

❑ Some 72 million Americans, 37 percent of the population age 12 or older, have used illegal drugs at least once.

❑ About 21 million Americans have tried cocaine; 3 million still use it occasionally and 1 million report being heavy users.

Who

❑ About 75 percent of illegal drug users are white.

❑ Women constitute 41 percent of drug users, including 5 million women of childbearing ages.

❑ Eleven percent of the babies born in 1988 were exposed to illegal drugs during the mother's pregnancy.

The Cost

❑ Cocaine-induced deaths totaled 1,696 last year, up from 604 in 1984.

❑ Hospital emergency rooms treated 46,020 cocaine users last year, up from 8,831 in 1984.

❑ Drug-related absenteeism and medical expenses cost businesses about 3 percent of their payroll.

Tax Credit for Security Devices

If Rep. Denny Smith (R-Oreg.) has his way, Americans may soon be eligible for a 25 percent tax credit on the purchase and installation of locks, alarms, security lighting, protective window bars and other security devices for their homes.

The Oregon Republican has sponsored legislation in response to the increase in home burglaries across the nation. The FBI reports that more than 2 million burglaries occurred in 1988—that translates into one burglary every 15 seconds.

The proposed tax credit would jumpt to 100 percent for people 65 and over—the most frequent victims of burglary. Smith says he proposed the credit to stem the steady growth of residential crime.

Child Safety Checklist

Is your child safe when he or she is at home and you're at work? The National Parent-Teacher Association suggests that you make sure your child knows the following things.

✔ Never go into your house or apartment if the door is ajar or a window broken.

✔ To lock the door when he or she comes home and to keep the doors and windows locked.

✔ To check in with you by telephone or report to a neighbor at a regularly scheduled time.

✔ To avoid walking or playing alone on the way home from school.

✔ His or her full name, address and telephone number—including area code.

✔ *Your* full name, the exact name of the place where you work and its telephone number.

✔ How to use both push-button and dial phones to reach the operator or report an emergency.

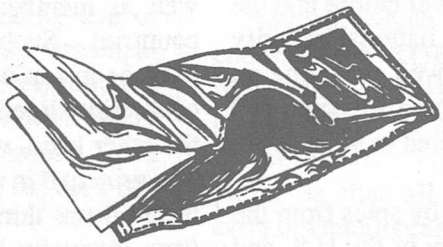
✔ How to carry a key so it's secure but out of sight.

✔ How to answer the telephone without letting callers know that he or she is home alone.

✔ How to get out of the home safely and quickly in case of fire.

Help! My Wallet's Gone!

You've been victimized by a pickpocket in a crowd of holiday shoppers. Or, distracted amid the frenzy of heading home for the festivities, you've walked off the plane without your purse. Whatever the reason, your wallet is gone—and with it, your credit cards, driver's license, and bank cash card along with any semblance of holiday cheer. What can you do to minimize the damage? Follow these tips provided by *U.S. News & World Report.*



Deal With Cards First

By law, you escape any liability for unauthorized charges to your credit cards as long as you report them lost or stolen before anyone else uses them. That means that you have to act fast. According to the Federal Trade Commission, a credit-card thief is most likely to use your card within 48 hours of taking it. If the thief acts before you do, you're responsible for the first $50 of fraudulent charges per card—which can add up quickly if you've lost a bank credit card, an American Express card, a gas card and a department store card or two. You should have a file of your account numbers, expiration dates and telephone numbers to call in the event of card loss or theft.

Don't Carry A PIN

The loss or theft of an automated-teller-machine card can be a lot more dangerous, so resist the temptation to carry in your wallet—no matter how well you think you've disguised it—the personal identification number, or PIN, that accesses your account. As with a credit card, you're off the hook if you notify your bank before the ATM card is used. Call within two business days after your card is missing and the most you stand to lose is $50. Otherwise, you risk $500.

And if your bank still has not heard from you 60 days after your next statement is mailed out, your potential loss is limited only by the size of your account. To activate all these legal safeguards you have to follow up your phone calls with written notification. Include your full name, account number, the date you discovered your card missing and the date you reported it gone.

Telemarketing Fraud . . .

Thieves Dialing for Dollars

The smooth voice on the other end of the phone offered Janice something she really needed: a chance to get away on an autumn vacation at a bargain price. All she had to do was give the caller her Master Card number. She gave her account number to the caller, then got her suitcases ready. The bill came but the trip didn't.

Janice was taken by what's known as telemarketing fraud, one of many ploys used by sophisticated thieves who prey on the multibillion dollar credit-card industry. The industry says all users are victims because the cost of fraud is passed on via higher credit card interest rates for everyone.

For the first half of 1989, the Secret Service, which has jurisdiction for crimes involving credit cards—said it made 760 credit card-related arrests and estimates industrywide losses from those cases at $89.7 million.

Some experts say that besides Christmas, the summer-fall vacation season is the busiest time of year for credit card thieves, who find that naive travelers make the easiest targets.

KGB Intensifies Spy Recruitment Effort

by Stanislav Levchenko

The scope of Soviet intelligence operations directed against the United States has broadened and intensified. There are more Soviet spy satellites in orbit than ever before and the majority of them are monitoring U.S. national security activities in this country and abroad as well as spying on America's allies in Europe and Asia. There are some 160 Soviet spy satellites in space now compared to 90 in 1980.

On the ground, KGB agents, assisted by spies from the Soviet Union's East bloc allies, are busy in the U.S. and Western Europe, Asia and elsewhere. Soviet President Mikhail Gorbachev has agreed to large cuts in nuclear forces, but with NATO's conventional armies in place it takes more traditional shoeleather spying to keep abreast of troop movements, new weaponry and tactics. This HUMINT (human intelligence collection) requires the kind of spying in which the KGB has become proficient over the years. The 1980s have proved just how successful the KGB has been in its spying activities against the U.S. And these were the years when the U.S. was supposed to be on a higher alert status against the activities of hostile intelligence agents!

Americans now are more easily recruitable by the KGB

But now there's a new and easier relationship between the U.S. and the U.S.S.R. The Soviet Union is undergoing change. It's for the better, as most Americans view the relaxation of tensions between Washington and Moscow. People in the White House are talking to people in the Kremlin. Americans are no longer nervous about Russians. Today, these visitors dress like Americans and even speak like them. Formerly uptight Americans are relaxing these days, now that the danger of a nuclear or a conventional war seems to have passed.

But relaxed Americans are more easily recruitable by the KGB. I'm reminded of a secret cable I received in Tokyo from the head of the KGB's First Chief Directorate shortly after the signing of the Helsinki human rights agreement in 1975 when *détente* was flowering and there was a thaw between East and West — like there is now. The message said that the West will be more trusting and less vigilant, "so now is the best time to recruit Americans." That message was sent by Vladimir Kryuchkov; he now heads the KGB.

Recent news reports also have provided enough examples of the KGB recruiting U.S. military personnel as well as members of the armed forces of other NATO countries. Such recruitment is difficult in Washington, D.C. or in London, Paris or Bonn, or even Japan, where counterintelligence operations are much more active. On the other hand, nothing is impossible in the spy business. The principal in the Walker spy case regularly made undetected drops during auto trips that were only 40 minutes from downtown Washington. He got away with it for years.

Why the increase in Soviet spying against the U.S.? The U.S. today is still *glavny vrag*, the "main enemy" of the state. Moreover, there are very pragmatic and practical considerations for Soviet spying directed against the U.S.. The Soviet economy is a mess. Only the West and the U.S. can provide the money, and the industrial, scientific and technical talent that the Soviet Union needs to avoid a serious economic disaster.

It's expected that industrial espionage directed against U.S. high-tech firms will pay off in higher productivity by Soviet workers who will operate new factory equipment and machinery which the Soviet economy desperately needs if it is to grow. These are times of tight budgets in the Soviet Union. Espionage, according to knowledgeable intelligence officials, can be a very cost-effective defense. "Spying becomes the great equalizer," according to one U.S. intelligence official.

Nor is the KGB changing it's stripes because of the easing of tensions between the U.S. and its allies. It may seem that way to many Americans and others in the western democracies who want to believe in these so-called "winds of change." Actually, the KGB is becoming more sophisticated in its use of public relations and there's more sophistication in its intelligence operations.

A new KGB? Not from my experience and that of millions of others. If Gorbachev's *détente, perestroika* and *glasnost* policies should fail, the United States—my country—will face new dangers from Soviet hardliners and more aggressive KGB operations in the U.S.

Stanislav Levchenko, a former KGB agent who quit the espionage business in Japan in 1979 is now a U.S. citizen and an author and lecturer.

. . . *Continued from page 1*

"But once the Soviets awakened to the potency of the hacker culture in the United States and other western nations, their leaders decided that they had to have the tools and the trained people. They have gone all out to create hackers but the Soviets are not yet completely successful. They have a long way to go."

These special schools that the Soviets created for their own *khakers*, according to Dr. Graham, permit certain privileges that don't exist in regular schools. He noted one drawback, however, that even in this period of *glasnost* is difficult to overcome: the police state mentality. The PCs used by students are locked up after use. All floppy disks have to be signed out and signed in.

In the final analysis, controls over the human spirit don't quite work. Soviet authorities are going to have to tolerate the rebellious streak that is found in all emerging computer cultures.

One 16-year old *khaker* at Moscow High School 57, a special mathematics school which has a number of foreign-made PCs, is proud of his hacker talent. He displays a button on his lapel that reads: "Don't tell me how to live!" It's this kind of person that Soviet intelligence is looking for, and the KGB's secret police know many ways to pressure a citizen to work on behalf of their nation's intelligence service.

The floppy disk has been under KGB suspicion for many years because it can be easily and surreptitiously transported and its contents copied and easily distributed, somewhat similar to the laboriously hand-copied *samizdat* writings that for years had been smuggled out of the country with inside information that the Soviet authorities did not want reported in the West. Today, some dissidents use rudimentary desktop publishing equipment to tackle controversial political topics.

One indicator of the interest of Soviet students in an American hacker's experience was the visit last fall of John Draper. He delivered a standing-room-only lecture on PCs at Moscow University. He told the students and professors about networking, electronic mail, desktop publishing, "and everything that the Soviets aren't supposed to do, and they couldn't get enough of it." Draper had run afoul of the law in the U.S. and had served time for his telephone exploits as a hacker.

"The KGB and the GRU are not known for going out and paying money for information that is not worth something," explained John Crowley, a former specialist at NSA's National Computer Security Center and National Security Assessment Center. Crowley, now a computer security executive with Information Security International, Silver Spring, Md., told the *Employee Security Connection* that unclassified information was stored in recently penetrated data banks that included personal information such as home addresses, phone numbers of people employed in Top Secret research.

Electronic mail in data banks also would provide valuable leads for Soviet intelligence in spotting and assessing potential spies. "If you're the KGB, you're only looking for that one person who can obtain access to classified areas or to sprawling contractor facilities," Crowley continued.

Finally, the Soviet intelligence services require such detailed information that some years will be needed to train their own *khaker* recruits how to break into computers and burglarize them. "Therefore, they will have to use third parties for this kind of intelligence gathering," adds Crowley. Among the data bases these hackers reportedly penetrated were the unclassified DOD Optimus data base, and computer systems throughout the U.S., Japan, Britain, France, Italy, Switzerland and West Germany.

Hackers are always attempting to penetrate global computer networks such as DOD's Defense Data Network in an effort to access computer systems. Although computer systems storing classified information are believed to be well protected, the compilation of unclassified but sensitive information in non-classified systems does pose a danger to security.

Computer security experts assume that the Soviet intelligence service is working hard at collecting passwords in an effort to ease break-ins to Western computers. Many passwords are not difficult to break, notes Harold Highland, Editor of the Journal, Computers & Security.

If there is one thing that Soviet intelligence has learned, it's that probing networks by using powerful computers can occasionally uncover software flaws that can be exploited to crack often simple security measures. Once inside a target computer, information can be copied and the location of new computers to break into can be discovered.

"It all boils down to heavy-duty electronic burglary of sensitive information, and I'm very upset that people are not watching the bank vaults," notes Dr. Clifford Stoll, an astronomer with the Smithsonian Astrophysical Observatory in Cambridge, Mass. Last year he discovered that those West German hackers working for the KGB had penetrated some U.S. databases and reported this security breach to counterintelligence authorities. ❑

DIS Shifts Inspection Focus

In what he called the "highest priority," Defense Investigative Service (DIS) Director John Donnelly recently announced that his agency—which is responsible for inspecting cleared defense contractor security programs—will practice a cooperative rather than adversarial approach to industry. DIS agency inspectors have been directed to emphasize "advice and assistance" rather than "gotcha" inspections.

In addition, more pre-inspection research will be conducted by DIS so that Government inspectors will be better prepared when they arrive on-site.

For example, DIS inspectors will go directly to the User Agency customer to learn more about the contract and also ask these customers to comment on the effectiveness and security posture of the company undergoing inspection.

A flexible approach to DIS inspections is also in the works. In light of budget cutbacks DIS is re-thinking how to best deploy its limited resources. As a result, contractors with a good security program in place may be rewarded with less frequent inspections.

First, the overall security posture of a contractor will be analyzed in determining how often inspections should be performed. Second, past inspection results will be a determinant along with the level of classified information possessed and the type of defense work in which the contractor is engaged. Third, increased use of sampling techniques may reduce the time that it takes to conduct inspections.

Since January, DIS has conducted some 19,937 security inspections of contractor facilities and have identified 1,300 major deficiencies. "We found some bootlegged documents," Donnelly admitted, "along with some lost documents not reported and some falsified classified destruction reports. But on balance, these were rare exceptions."

What does all this mean for employees? DIS plans to spend more time interviewing employees to determine how well they understand and carry out their security responsibilities. DIS believes that the contractor's most effective barometer of security is its employees.

But while contractors complain about the time and effort it takes to satisfy Government inspectors and auditors, they all grudgingly agree the inspections are necessary.

To make the process easier, what is needed is a closer, more cooperative relationship between the contractor and the inspector. And that is exactly what DIS Director Donnelly says he intends to do.

Terms You Should Know

Classification Management — That function of the Security Organization that is the internal point of contact on all matters relating to the proper assignment of security classification(s) to national security information.

Facility Security Officer (FSO) — A cleared contractor representative who is a U.S. citizen and is assigned responsibility for directing the Company's defense industrial security program.

Letter of Consent (LOC) — Defense Industrial Security Clearance Office (DISCO) form 560 used to notify a contractor that a personnel security clearance or a Limited Access Authorization has been granted to an employee.

Protected Area — An area housing one or more automated information systems, including communications equipment, remote computer facilities, terminals or peripheral devices, and continuously protected by physical security safeguards and access controls.

The *Employee Security Connection* (ISSN 0894-2080) is published quarterly by the National Security Institute, 161 Worcester Road, Framingham, Massachusetts 01701. Telephone (508) 872-8001 for information concerning company subscriptions.