Recent Key Developme ts Regarding NSA

National Security Telec mmunications and Information Systems Security Committee (NSTISSC)

The National Security Te ecommunications and Information Systems Security Committee (NSTISSC) v as established by President Bush under National Security Directive 42 (N D 42) entitled, "National Policy for the Security of National Security Telecc mmunications and Information Systems," dated July 5, 1990. The Chair of th NSTISSC is Art Money, the Assistant Secretary of Defense for Command, C ontrol, Communications, and Intelligence (ASDC3I). The NSTISS C sets national policy, and promulgates direction, operational procedures, nd guidance for the security of national security systems through the NS ISSC Issuance System.

[redacted] report that NSA is trying to put teeth back into NSD 42. The irective originally granted NSA broad authority over "national security systen s." These were originally defined as those systems falling into the military a d intelligence realm, i.e., systems handling classified information an l other unclassified sensitive military information falling under the Warner Amendment. However, NSA has recently tried to convince the new Bush dministration to grant it security oversight authority for non-national security systems in which integrity and availability are paramount. The NSA is particularly trying to gain control over security of the Federal Aviation Admin stration's National Airspace System and the National Weather System. This p wer move has met with stiff opposition from the OMB, Department of S ate, and Department of the Treasury.

National Security Age cy (NSA)

The National Security A gency (NSA) continues to expand its influence in government-wide cyber security programs. In fact, it has ignored the Computer Security Act y providing technical assistance directly to civilian government agencies, t ereby extending the national security umbrella to non-national security-relatec and unclassified computer systems. It has provided security assessments to he Departments of Interior and Commerce and the Federal Emergency Ma agement Agency (FEMA).

Public Key Infrastruc ure (PKI)

A report released by the General Accounting Office (GAO) urges the federal government to ensure the security of e-government through the use of public key infrastructure (PKI) technologies.

The report states that most PKI products are not interoperable and this problem needs to be addressed before e-government services can be offered widely, as government agencies will need to have a common PKI system.

The report also says that the expense of introducing PKIs may scare off many government agencies operating within tight financial constraints.

NSA and NIST have jointly developed the Internet Protocol Security (IPSEC) standard. The IPSEC provides integrity and confidentiality protection for Internet Protocol datagrams. IPSEC also integrates with NSA's Internet Security Association and Key Management Protocol (ISAKMP). IPSEC is the basis for RSA Security's Secure Wide Area Network (SWAN) initiative to provide secure virtual private networking in firewall applications. However, the involvement of NSA in Internet security technical standards makes the actual security provided by them somewhat questionable.

Government Access to Keys (GAK)

There is a strong belief that the NSA, supported by the FBI, will try to convince the new Bush administration to push for a government access to key escrow-like system. Attempts by the Clinton administration to force industry to adopt key escrow systems like CLIPPER (for voice communications), CAPSTONE (for data communications), and TESSERA/FORTEZZA (PCMCIA card) met with failure. Even after NSA declassified the two algorithms used in the FORTEZZA PCMCIA card – the 1024-bit Key Exchange Algorithm and the 80-bit SKIPJACK algorithm – to promote commercial development of FORTEZZA-based security systems, the program was not embraced by the private sector.

Nevertheless, NSA continues to attempt to dominate the commercial encryption industry. [redacted], commenting on recent revelations that Pretty Good Privacy (PGP) has now been back-doored by NSA (partly resulting in its inventor Phil Zimmermann's decision to leave Network Associates, Inc.), NSA was once again reasserting its unofficial strong encryption use doctrine of "NOBUS," which means "No One But Us." In January 2000, [redacted] confirmed that Network Associates had close links with the NSA. Pennsylvania Congressman Curt Weldon also admitted that the heads of IBM and Microsoft had cut a deal with NSA and the Pentagon to give the U.S. government "access to their systems." Specifically, Weldon was referring to software encryption exported by the two companies. Cylink, a major exporter

of encryption hardware a id software devices, is headed by William Crowell, the former Deputy Direc or of NSA.

The FBI has sought auth rity to place "recovery devices" on computers without the user's know dge to gain access to pre-encrypted computer data and files. This was soug in the failed Cyberspace Electronic Security Act (CESA) of 1999 and is e pected to be sought by the FBI in future legislation.

One company with close ties to NSA is the former Information Resource Engineering (IRE) of Ba timore, Maryland. Staffed by a number of ex-NSA engineers, IRE changed ts name to SafeNet. In 1995, it acquired Gretag A.G. of Switzerland, the manufacturer of the Gretacoder encryption device. The Gretacoder was thought by some encryption experts to have been "red threaded" by NSA – a process in which a back door was placed in the units to permit U.S. intelligence o decrypt encoded messages.

Firewalls

In 1999, NSA establish d its Laboratory for Telecommunications Sciences (LTS) to provide a coll borative R&D environment with industry and academia. That same ye r, LTS licensed Marconi Communications of Warrendale, Pa., to sell NSA's prototype high-speed firewall under the Domestic Technology Transfer Program. The firewall is commercially called the SA-400 Firewall Li e Card. The firewall allows only authorized Internet Protocol (IP) and asyn hronous transfer mode (ATM) traffic into a protected network. NSA plans to share other security technology with the private sector.

Steganography

Steganography is not e cryption, per se, but is included under the topic because it, like encrypt on, hides information from eavesdroppers. Steganography, often r ferred to as "stego," is the art of hiding writing in other text of images. It is also known as "covered writing."

The U.S. Department f Defense, the U.S. Air Force's Rome (New York) Laboratory, and the N A are funding research at Syracuse University to develop programs to d tect the use of steganography programs in e-mail and other files. The NSA a d the military are concerned that an increasing number of images on the Inter et are being discovered to contain hidden text and could be used by forei n intelligence agents and terrorists to secretly transmit messages much in the ame way that clandestine radio operators once openly broadcast sets of code numbers over the air waves. These include image, audio, and video files n web sites that may be altered by hackers to secretly embed "stegoed" mes ges. Through the use of "blind steganography" programs and standar traffic analysis, the NSA and other intelligence agencies can detect th presence of steganography with a view to distorting

the message or replacing t with a bogus version. The steganography detection software can also decode images and other files. According to the Syracuse University researchers, Internet use of Steganos, one of the most popular steganography programs, has skyrocketed.

Education and Certification

The NSA is also involved heavily in cyber-security education and training. Fourteen universities have been designated by NSA as Centers of Excellence in Information Assurance under the Centers of Excellence Program. NSA granted the designations following its review of university applications against published criteria based on training standards established by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). As with any program funded by NSA, national security concerns are primary. Therefore, the funding of these programs is directed to recruiting potential future employees for NSA and foreign student participation in these education and certification programs is unofficially discouraged. NSA's academic recruiting pipelines include the NSA-run college and high school courses under the Gifted and Talented Program (GTP) and the High School Work Study Program (HSWSP). Computer science students are eligible for scholarships and a one-year work-study program at the NSA. The 2001 budget contains funding to develop a "Cybercorp" program to address the shortage of information security personnel within the government.

It should be noted that of the fourteen NSA Centers of Excellence, the Naval Postgraduate School and National Defense University are Defense Department institutions while Carnegie Mellon has had a long-term relationship with the Defense Department in its hosting of the Computer Emergency Response Team (CERT), an activity largely funded from the defense and intelligence budgets. Idaho State has had a long relationship with the NSA's information security program, preparing an information security Common Body of Knowledge (CBK) for training and certification purposes. Stanford, Purdue, George Mason, and James Madison also have close connections to the Defense Department and intelligence community. The Research Directorate of the NSA also maintains close links with the University of Maryland where it oversees a High Performance Computing Center.

Encryption Exports

The United States revised its cryptographic export control policies effective January 14, 2000 [redacted]. The January 2000 change resulted in many requests for mass market encryption exports receiving positive rather than negative replies from the Commerce Department's Bureau of Export Administration. Key length was no longer a

determining factor in gra ting an export license. However, the January policy kept in place cumbersom rules and procedures regarding one-time technical reviews by NSA and a se gmentation of permissible end-users into an unworkable quagmire. T e NSA technical review entailed would-be exporters submitting their source c de to the NSA and agreeing to accept any changes to the software prior to l eing granted an export license. The European Union responded by the U.S. m ve by allowing encryption exports within the EU and selected other count ies on an export license-free basis. This once again put U.S. mass market en cryption exporters at a disadvantage. In October 2000, the U.S. governm nt also allowed export-license free mass market cryptographic exports tc the EU and eight additional countries.

CALEA Implementati n Section (CIS)

The Communication Assistance to Law Enforcement Act (CALEA), passed in 1994, con nues to require telecommunications providers to make their switches and networks "wiretap-friendly" to federal law enforcement agenci s. The office charged with ensuring telecommunications industry compliance is the CALEA Implementation Section (CIS), an of ice in Chantilly, Virginia staffed by FBI personnel and telecommunicat ons contractor specialists working for the firm Booz, Allen and Hamilton (BAH). The program manager for BAH is Mike McConnell, a forme Director of the NSA. Many of the BAH personnel working at the CIS re former and retired NSA communications intercept experts.

The efforts of the C S are particularly worrisome for foreign telecommunication providers in the United States. The FBI has become the final decision-m king authority in deciding whether or not to approve foreign acquisition f U.S. telecommunications and Internet Service Providers. It was h avily involved in British Telecom's failed bid to buy MCI Communicati ns Corp. in 1996 – and may have actually killed the deal. It got involve in the joint venture between Verizon Communications a d Britain's Vodafone, as well as Deutsche Telekom AG's bid for Voice Stream Wireless Corp. of Bellevue, Washington. The FBI was wary of th German government's large stake in Deutsche Telekom. The FBI also held up Nippon Telegraph & Telephone's offer to acquire U.S. Intern t Service Provider Verio until NTT agreed to strict national security sa eguards.

According to Fede al Communications Commissioner (FCC) Harold Furchtgott-Roth, C ALEA is not popular with the FCC, the lawful and traditional governn ent regulatory authority over the telecommunications service industry. T e FBI insists on attaching conditions to foreign telecommunication deals with U.S. telecommunications providers. This results in the FCC delaying its approval until the FBI and companies agree

on the FBI's national security controls. These controls originally included barring all non-U.S. citizens from handling the companies' billing and call information. Faced with violating U.S. equal opportunity employment laws, the FBI dropped that idea. However, companies are required to maintain all equipment for domestic traffic in the U.S., so the FBI can have wiretapping access. All record-keeping facilities must also be based in the U.S. Companies like Vodafone and Verio must also employ only "trustworthy personnel" to monitor the network and handle wiretap requests. Vodafone and Verio also must ensure that no wiretap information is transmitted to any foreign government, and in the case of Verio, only specially cleared Verio personnel can have access to wiretap information.

When TMI Communications Inc., a subsidiary of BCE, Inc. of Canada wanted to sell satellite-phone service to U.S. customers, the FBI interjected itself into the FCC approval process. TMI was forced to install a call-switching station in New England through which it would route all its U.S. traffic for FBI wiretappers. TMI phones were also required to be equipped with geo-positioning technology to permit the FBI to pinpoint a suspect user's location.

Working with the CALEA is the Telecommunications Contracts and Audit Unit (TCAU). This office processes industry requests for reimbursement for retrofitting surveillance into digital networks. It is assumed by many experts that the final bill for surveillance upgrades will range between $5 and $7 billion over a ten-year period.

Internationalizing CALEA

According to senior U.S. telecommunications industry officials, the FBI has sought for the last few years to internationalize the U.S. Communications Assistance to Law Enforcement Act (CALEA). Among other requirements, the CALEA forces U.S. telecommunications providers to make their systems "wiretap friendly" for U.S. law enforcement. It has been expanded to require cellular companies to provide location data on cell phone customers to federal investigators. In addition, providers must provide law enforcement with access to the content of conference calls when only one of the participants is under surveillance. Monitoring would be permitted after the targeted individual dropped off the conference call. Other participants in the conference call would also be identified to law enforcement.

Specifically, the FBI would like to see the International Telecommunications Union (ITU) to adopt a series of international technical standards that would mirror the CALEA's wiretapping requirements. The FBI has been quietly lobbying its partner law

enforcement agencies including the Australian Federal Police and Royal Canadian Mounted Police, to support a series of ITU technical standards for communications surveillance.

Engineering Research Facility (ERF)

The Engineering Research Facility, located in Quantico, Virginia, is the main FBI activity developing tools and techniques to monitor the Internet. It is composed of the Electronic Surveillance Technology Section (ESTS), which itself is divided into the Network Access Development Unit (NADU) and the Data Intercept Technology Unit (DITU). The ESTS developed the CARNIVORE e-mail sniffing and capture program, since renamed Data Collection System 1000 (DCS 1000). The FBI's CARNIVORE system is supported by Booz, Allen & Hamilton, the same contractor that supports the CALEA Implementation Section (CIS). CARNIVORE runs on a personal computer under the Windows operating system. It is a packet sniffer -- a device connected to an ISP for the purpose of monitoring electronic traffic.

Carnivore first aroused public suspicion when the ISP EarthLink refused to let Carnivore on its network citing concern that the FBI would have the ability to monitor all of the network traffic, including e-mail and other electronic information. EarthLink has mounted a huge public relations campaign touting its commitment to privacy and anonymity to its subscribers.

CARNIVORE has access to a much wider range of information than it has with current wiretaping operations -- it can view e-mail, web surfing, web searches, web mail, instant messaging, file downloads, etc., and it intercepts information about everyone on the network even though a court order targets only one person for surveillance.

The Partnership for Critical Infrastructure Security, an association comprising Citigroup, the U.S. Chamber of Commerce, Microsoft, BellSouth, Lucent, SBC Communications, Union Pacific, and Cisco Systems, stated that in the future the federal government should develop cost-benefit tests to determine whether a tool like Carnivore is invasive/valuable. The group said this requires a "nuanced and 'political' approach to the issue, and the optimal way to achieve these benefits is by adopting a consultative approach before such tools are developed and implemented."

The FBI is also creating data warehouses, enabling it to store information from communications intercepts in large databases. One such database is code named CASA DE WEB, which stores audio files, intercept transcripts, translated intercepts, and reports. Another program code-

named DIGITAL ST)RM permits FBI agents to remotely access stored wiretaps via Internet- ike connections. Both programs facilitate text and voice key word spott ng and voice print identification. The FBI's fiscal year 2001 budget rec uest states that "advanced digital collection systems [will] increase the nu nber of [wiretaps] by as much as 300 percent over the next ten years."

National Infrastru ure Protection Center (NIPC)

The National Infrast ucture Protection Center (NIPC) was created within the FBI in 1998 wit a target budget of $64 million and a proposed staff of around 125. The NI C is authorized to use Department of Defense and Intelligence Comm ity assets in monitoring "hacking" activity on the Internet. The NIPC coordinates the INFRAGARD program: an information sharing initiative between the government, private companies, and academic insti tions. The CIA, NSA, and Defense Department supply personnel to the NIPC. The FBI is seeking greater Internet monitoring powers nder the Foreign Intelligence Surveillance Act, a law that enables the bu eau to work closely with the NSA.

According to one s nior government official, 200 FBI field agents provide the "eyes and ears" for the NIPC in specific regions of the United States. The FBI field offic s are bolstered by NSA personnel assigned to provide "technical assistan e." The largest FBI field offices are located in New York, Washington Los Angeles, San Francisco, Miami, Chicago, Houston, New Or ans, Baltimore, and Atlanta. The FBI has established INFRAGARD ch pters within the jurisdiction of each FBI Field Office. Unlike the NSA d tailees at the NIPC, the NSA technical field personnel are assigned direc y from NSA Headquarters and do not fall within the FBI's managemen structure. The NSA personnel are involved in the wiretapping of co puter networks and monitoring Internet Service Provider activity nder specific U.S. Criminal Statutes dealing with foreign counter-in elligence, i e., those authorized by the Foreign Intelligence Surv llance Court. However, NSA personnel also assist in the examination o computer media seized as a result of lower-level court-ordered search w rrants.

National Securi Agency (NSA)

The NSA consid rs itself the lead agency in both defensive and offensive information warf re. The agency coordinated the efforts of the Joint Intelligence Com nunity and Department of Defense Information Operations Tech ology Center (IOTC) at Fort Meade, Maryland. That component parti ipated heavily in INFOWAR games and exercises like ELIGIBLE REC EIVER, EVIDENT SURPRISE, SOLAR SUNRISE, and

MOONLIGHT MAZE, the latter a major operation said to involve combating Russian hackers.

The NSA will play a major role in ensuring that civilian government agencies and key corporations have eliminated most significant known vulnerabilities by May 2003. This is represents a significant expansion of NSA's domestic role in the United States. Historically, the NSA's role has been confined to foreign intelligence activities. However, the government would like the change this approach. It argues that both jurisdictions and national origins are meaningless in cyberspace and that these two pillars upon which current intelligence gathering activities are based are now "irrelevant."

The National Security Incident Response Center (NSIRC), which is located at the NSA, is designed to be a "focal point" for incidents impacting U.S. national security information systems. NSA's importance to Internet monitoring is derived from the fact that it is the "only organization positioned to link intrusion data to signals intelligence." The NSIRC houses four functional areas – 1) the information Protect Cell (an operation within the National Security Operations Center (NSOC)); 2) the Reporting and Analysis of Network Exploitation Division (provides all-source analysis of network incident activity); 3) the Network Intrusion Analysis Capability (provides information on hacker techniques); and 4) the Threat Assessment Division (provides a global wide-ranging perspective of threats to U.S. telecommunications and information systems).

Through projects like SOFT LANDING, SOFT SOURCING, BREAKTHROUGH, AND GROUNDBREAKER, the NSA is placing a number of its retirement-age personnel in major high-technology firms. These companies, which include Computer Sciences Corp. (CSC), Data Procurement Corp., SAIC, TRW, Lockheed martin, Questech, Kathpal Technologies, Allied Signal and Compro, are actively soliciting contracts to participate in critical infrastructure protection in key economic sectors. The NSA's GROUNDBREAKER information-technology outsourcing project has wooed companies like AT&T Corp., CSC, IBM Corp., General Dynamics Corp. and OAO Corp., which have formed three teams to compete for a contract set to be valued at as much as $5 billion over 10 years. The winning contractor team will assume control of 1700 outsourced NSA employees, most of whom are senior personnel.

The NSA is asking Congress for billions in new funding to create what it calls TRAILBLAZER -- a computer system designed to better process and gain useful intelligence from the vast quantities of information the NSA collects around the world. The agency says TRAILBLAZER is one of its major modernization efforts to the Signals Intelligence (SIGINT)

programs. The agenc is working on studies to research and create the system concepts and architectures for the TRAILBLAZER initiative.

Central Intelligenc Agency (CIA)

The CIA's Office of Advanced Information Technology is developing a number of data-mini g enhancements to enhance the communications intelligence collectio efforts of the NSA. It has developed a program called OASIS, which automatically converts audio signals into readable and searchable text. OASIS can distinguish between different male and female voices. OASI will soon have the capability to monitor Arabic and Chinese conversatio s. Another system code-named FLUENT, allows an intelligence analyst t search stored foreign language documents using English. Such capab ities are said to exist with regard to the ECHELON "dictionary" progra s. The NSA contracted with Sand Technology Systems of Montrea to help it provide links between various databases it has developed over number of years. Specifically, NSA bought Sand's Nucleus software to help it data mine its numerous databases.

Department of Tre sury

The Financial Crime Enforcement Network (FINCEN), located in Vienna, Virginia, tra ks banking and other financial movements and transactions around he world in association with similar operations in the United Kingdom, G rmany, France, Canada, Australia, Italy, Belgium, the Caribbean and other countries. Officially under the aegis of the U.S. Department of Trea ury, FINCEN's computers are linked to the NSA, FBI, CIA, and other agencies.

National Security Telecommunications Advisory Council (NSTAC)

Information Shari g and Analysis Centers (ISACs)

The Bush administra ion continues to support the Information Sharing and Analysis Centers (IS ACs) established by the previous administration to facilitate the exchan e of network vulnerability and threat information between the govern ent and the key sectors of the critical infrastructure. These centers curre tly exist for the banking and telecommunications sectors.

Financial Services nformation Sharing and Analysis Center (FS/ISAC)

A financial services ector ISAC has been established with the strong support of Citigrou under the aegis of the Department of Treasury. By agreeing to share in rnal information with the government, banks may be

compromising their fiduciary responsibilities with their customers. The FS/ISAC and the Pentagon's Joint Task Force/Computer Network Defense activity have announced an information sharing agreement.

The speed at which several banks agreed to set up a financial Information Sharing and Analysis Center (ISAC) as the first one of its type is emblematic of the problem. [redacted], the NSA approached the banking organization with a proposal to set up its ISAC complete with NSA-developed technical monitoring capabilities. [redacted]

The FS/ISAC is operated by Global Integrity Corp., a subsidiary of the large intelligence contractor Science Applications International Corporation (SAIC)

J.P. Morgan supports the FS/ISAC in the research and development area. This is an example where J. P. Morgan succumbed to NSA overtures through an outsourcing contract. In 1997, J. P. Morgan outsourced its IT operations, including the information security function, to Computer Sciences Corporation's (CSC's) Pinnacle Alliance. CSC began assigning former NSA personnel to its J. P. Morgan contract.

Information Technology – Information Sharing and Analysis Center (IT-ISAC)

An ISAC for the information technology sector has been established with collaborative efforts being led by the Information Technology Association of America (ITAA), the President's National Security Telecommunications Advisory Committee (NSTAC) – an industry consortium of telecommunications providers – and the FBI through its INFRAGARD program. The IT-ISAC offers a 24-by-7 network, notifying members of threats and vulnerabilities. Howard Schmidt, chief security officer at Microsoft is the head of the Virginia-based Information Technology ISAC. Schmidt reportedly enjoys close links with NSA officials.

The major supporters of the IT sector ISAC include communications service providers AT&T, Bell South, Sprint, Teledesic, Verizon, and WorldCom; hardware and software providers Cisco Systems, Computer Associates, Hughes Electronics, Hewlett-Packard, IBM, Intel, Microsoft, Motorola, Network Solutions, Inc., Nortel Networks, Oracle, Symantec, Unisys, and UUNET Technologies. Other key participants are those companies that stand to gain the most from the initiative – federal contractors. These include Booz Allen & Hamilton, Computer Sciences Corporation (CSC), EDS, Litton TASC, Lockheed Martin, Northrop

Grumman Logicon, Raytheon, Rockwell, SAIC, SRA, and Titan Systems, TRW.

It should be noted that the original PCCIP Report recommended that the National Security Council (NSC) establish standards for sharing critical infrastructure information with foreign corporations and their U.S. subsidiaries. The composition of the ISACs to date indicates that the U.S. national security community has declined to invite foreign corporate to participate in ISAC activities – a further demonstration that critical infrastructure protection has more to do with national security and intelligence than in providing enhanced security for critical computer systems and networks. It should also be noted that many of the companies listed above have had long-standing contracts with the U.S. intelligence community and military.

In fact, the IT-ISAC which is a not-for-profit corporation run under the umbrella of ITAA, is only open to U.S.- based IT companies. The hand of the U.S. intelligence community in the IT-ISAC is evidenced by the fact that the U.S-only stipulation is waived for two Canadian companies – Nortel and Entrust – which have a long-standing relationship with the NSA and its Canadian counterpart, the Communications Security Establishment (CSE).

[redacted] report that the FBI levied the pre-condition of holding a US government Secret security clearance for sharing FBI threat data with the private sector. Security clearances are not, as a general rule, granted to foreign nationals – a further impediment to foreign corporations becoming involved in the critical infrastructure regime.

A. Information or Cyber-Warfare

It is expected that the Bush administration will continue to champion the development of information warfare/cyber-defense programs. In his acceptance speech, Secretary of Defense nominee Donald Rumsfeld, cited the beefing up information warfare capabilities as a key element in his plan to overhaul the Pentagon. Information warfare policy officials have long argued that current U.S. law stymies the ability of the Pentagon and NSA to coordinate cyber warfare activities since the act bars NSA from direct involvement with the security of either civilian government agency or commercial computer systems and networks. [redacted] believe that a number of information warfare supporters from the old Bush administration will return to key posts in the new Bush administration. This is particularly true of the new Deputy Defense Secretary, Paul Wolfowitz, and Assistant Secretary of Defense for

Command, Control, Communications, and Intelligence (C3I), Art Money. Before he sworn in on March 2, 2001, Wolfowitz told the Senate Armed Services Committee, "Terrorists may try to increase their reach by using conventional devices with increased destructiveness, weapons of mass destruction or cyber weapons against the United States. We must do everything in our power to stop them." Art Money [redacted] "My vision is to make Information Superiority happen." National Security Adviser Condoleezaa Rice told an information security forum on March 21, 2001 that the nation must "be prepared for scenarios where we have to restore and reconstitute critical operations quickly once they've been disrupted," adding that government agencies "need to work hand in hand with the private sector."

The FBI's program of mutually sharing computer security and infrastructure threat and vulnerability information between it and the private sector is rife with danger for foreign participation in the defensive infrastructure protection aspects. [redacted] confided that, although the FBI claims there is a separation between the defensive infrastructure protection elements in the government and those involved with classified offensive information warfare planning, no such separation actually exists. The Pentagon and NSA are said to have full access to shared corporate secrets in order to exploit potential information system weaknesses in a possible future cyberwar.

1. **Defensive Operations**

<u>National Security Agency (NSA)</u>

Through the NSIRC the NSA provides "Cyber CRITIC" messages to alert the Defense Department JTF-CND, Defense Information Systems Agency (DISA), the General Services Administration's (GSA) Federal Computer Incident Response Capability (FedCIRC), OMB, and NIPC with cyber attack warning information. The NSIRC is located within the National Security Operations Center (NSOC), which sends critical intelligence (CRITIC) messages from national signals intelligence and other national intelligence and warning systems. In many ways, the NSIRC has taken on the function of the proposed Federal Intrusion Detection Network (FIDNET), an early warning system to be operated by the General Services Administration (GSA). However, the now only oversees the Managed Security Services (MSS), a smaller scale replacement for FIDNET. MSS is nothing more than an intra-federal government ISAC.

2. **Offensive Operations**

Department of Defense

In October 1999, the U.S. Defense Department consolidated its defensive and offensive information warfare activities within the U.S. Space Command in Colorado Springs, Colorado. The subordinate activity responsible for these operations is the Joint Task Force for Computer Network Defense (JTF-CND). According to Robert West, the deputy commander of the JTF-CND, the Pentagon's computer security personnel are spending a great deal of time and resources monitoring hackers' chat rooms to spot the trading of technical information on hacking techniques. However, this also involves the monitoring of anti-globalization groups like "Electrohippies" that set up "black lists" of companies involved in environmental or social degradation. For example, the monitoring by the Pentagon of hacker groups opposed to Nike and The Gap for exploiting children in the Third World, indicates that the military is not only potentially violating constitutional provisions against illegal surveillance of U.S. citizens but also may be conducting low-level computer economic espionage on behalf of U.S. companies.

The Defense Information Systems Agency operates the DOD CERT (Computer Emergency Response Team) and the Global Network Operations and Security Center (GNSOC), two entities that monitor military data networks for suspicious activity.

Private Contractors

iDefense, an information warfare/computer security consulting firm headquartered in Fairfax, Virginia with satellite offices in London and Tokyo, has been awarded a sole-source contract to provide the US State Department with on-line cyber-intelligence. The Chairman of the Board of iDefense is James Adams, formerly the Washington correspondent for the Sunday Times of London and briefly the CEO of United Press International. After having recently attained US citizenship, he now serves on the National Security Agency's (NSA) Advisory Board and the Department of Defense's Joint Service Advisory Group.

Veridian of Arlington, Va., has developed an Automatic Security Incident Measurement sensor to monitor suspicious or malicious traffic crossing Air Force networks. When such activity is detected, the system sends real-time alerts to the Air Force Computer Emergency Response Team (AFCERT).

Other firms are involved in Internet monitoring on behalf of the Defense Information Systems Agency (DISA). They include SRA

International of Fairfax, Va., CACI, Inc., of Arlington, Va., Electronic Warfare Associates (EWA), Inc., of Herndon, Va., and Logicon-Northrop Grumman also of Herndon, Va.

The Navy uses an intrusion detection system called SHADOW (Secondary Heuristic Analysis for Defensive On-line Warfare).

International Legal Issues

In late 1999, a team of Judge Advocate General (JAG) lawyers at the Defense Department cautioned against the use of computer hacking and disinformation in offensive information campaigns. In a document titled "An Assessment of International Legal Issues in Information Operations," the Pentagon's Office of General Counsel opined that it was dangerous for the military to contemplate launching information warfare attacks on banks, stock exchanges, and universities. The lawyers warned of the possibility of a ripple effect on civilian populations and unintended consequences for neutral or allied nations. As for disinformation campaigns contemplated by some within the Pentagon and intelligence community, the Pentagon report was straightforward: "It might be possible to use computer morphing techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed. If false, this also would be a war crime."

According to sources close to transatlantic negotiations on the Council of Europe's Cyber-crime Convention, the Pentagon and National Security Council want to retain language in the convention that would implicitly exempt U.S. military and intelligence personnel from potential criminal prosecution for engaging in cross-border computer hacking. The key wording in the convention draft is that computer hacking, generally, would be prohibited "without right." The U.S. cyber-warfare community believes that the "without right" caveat implies that U.S. personnel would have legal authority to penetrate foreign computer systems in a cyber-war scenario.

Therefore, U.S. government negotiators have ensured that military operations are not covered by the convention. For example, sources point out that in its present form, the convention would legally accommodate the hacking by U.S. personnel of targets like the Serbian air defense network.