

## CHAPTER 3

### INTRODUCTION

In its 1998 report entitled “Technology Collection Trends in the US Defense Industry,” the Defense Security Agency (DSS) reported that the number of suspected industrial intelligence-gathering attempts against the US defense industry tripled since 1995. It also said that 37 nations were engaged in industrial espionage to gain information about US Department of Defense technology. In its 2001 report, the number of countries had grown to 63.

While the DSS study focused on foreign collection of classified or sensitive information on US weapons systems, emerging technologies with military applications, and related technical methods, intelligence collection against US economic, commercial, and proprietary information continues vigorously. This collection effort allows foreign nations and corporations to obtain shortcuts to industrial development and to improve their competitiveness against US corporations in the global marketplace.

At the same time, some foreign scientists and businessmen working with US firms or research institutes try to circumvent US laws to steal or illegally transfer embargoed American technology. There were several notable cases involving theft of American proprietary information. The first involved several Taiwanese nationals charged with allegedly trying to steal the secret formula for an anticancer drug made by the Bristol-Myers Squibb Company. Another was an Avery Dennison employee who supplied a Taiwanese firm some of his company’s most closely held secrets. In a third case, two Japanese stole genetic materials from Lerner Research Institute and made it available to an institute in Japan.

Spying by other nations within the United States also came to the surface during this period. The most notable of which was Cuba when it suffered setbacks with the arrest of seven members of its Wasp Spy network in Florida, its spy within the US Defense Intelligence Agency, and another in the US Customs Service. Five Americans were also arrested for selling or trying to sell US classified information to foreign intelligence services or nations.

Collection by the National Security Agency (NSA) came under the foreign microscope when the European Parliament alleged that NSA operates an international SIGINT collection effort—identified as ECHELON—that intercepts communications worldwide to provide economic intelligence to US corporations. On 5 July 2000, the European Parliament voted to launch a further investigation of ECHELON; the resultant draft report on ECHELON was made public on 18 May 2001. Maintaining that NSA operates in accordance with existing statutes and executive orders, senior US officials strongly disputed claims that intelligence agencies assist US corporations competing with foreign firms. They acknowledged, however, that intelligence agencies collect information regarding the use of bribery and other illegal efforts by foreign firms in competition with US corporations.

---

## **Kai-Lo Hsu, Chester S. Ho, and Jessica Chou**

Kai-Lo Hsu, Chester S. Ho, and Jessica Chou, all Taiwanese nationals, were charged with allegedly trying to steal the secret formula for Taxol, an anticancer drug made by the Bristol-Myers Squibb Company.<sup>1</sup> In October 1997, a Federal judge ordered prosecutors to turn over to the defendants and their lawyers the very documents the defendants are accused of trying to steal. The judge ruled that they needed the information to prepare their defense and that their right to a fair trial overrides the rights of a company to protect its trade secrets. Prosecutors appealed the ruling.

In a closely watched economic espionage case, the Third US Circuit Court of Appeals in Philadelphia ruled on 27 August 1998 that Federal prosecutors did not have to turn over trade secrets to defendants. The ruling reversed the lower court's decision.

The three-judge appeals panel said the defendants do not need to see the purported trade secrets because they can be guilty of conspiracy and attempted theft of trade secrets "even if the documents contained no confidential information at all." The appeals panel also said that the district judge's analysis was mistaken, since it was based on the belief that the defendants were charged with the actual theft of trade secrets. In fact, since they were charged with only an attempted theft, the defendants were not entitled to the documents because they were not an essential element of the prosecution's case.

The appellate court ordered the district judge to ensure that the trade secrets were edited out of the documents before they were turned over to the defendants.

On 31 March 1999, Kai-Lo Hsu, the technical director of the Yuen Foong Paper Co., Ltd., in Taipei, pleaded guilty to one count of conspiracy to acquire a trade secret. Under the plea, Hsu was to cooperate with Federal authorities who were investigating the extent of the conspiracy. In exchange for his cooperation, 10 other criminal charges against him were dropped, and a sentence below the 10-month prison term that was

recommended under sentencing guidelines will be encouraged. Hsu was released on \$1 million bail, awaiting sentencing.

Hsu was one of three people charged two years ago in an FBI sting operation. Also of the three, Jessica Chou, Yuen Foong Paper's business manager, is considered a fugitive by US authorities and is believed to be in Taiwan. The other defendant, Chester S. Ho—an MIT-trained biochemistry professor at two Taiwanese universities—was released last January after Federal prosecutors dismissed the charges against him.

According to the sentencing transcript produced in the US District Court for the Eastern District of Pennsylvania, Hsu was sentenced to two years' probation and fined \$10,000 on 13 July 1999 for conspiring to buy information regarding Taxol. The drug had earned the company almost \$1 billion in revenue.

The US Government took the position that, due to Hsu's cooperation, he was entitled to a departure under the sentencing guidelines. However, due to the seriousness of the offense, the prosecution argued that some period of incarceration was warranted in order to send a signal to those who are inclined to violate the Economic Espionage Act. Noting that technology has made the United States what it is today, the US Government also argued that it was important to prevent this kind of theft so that companies like Bristol-Myers Squibb will remain willing to take the risks and invest millions of dollars in developing technology that might or might not work. Despite this urging, the court sentenced Hsu to time served (14 days), two years of supervised release, and a \$10,000 fine.

A separate civil settlement was negotiated between Hsu's company, the Yuen Foong Paper Co., Ltd., in Taipei, and the US Government in the amount of \$300,000.

---

### **Endnote**

<sup>1</sup> See *Counterintelligence Reader*, Volume III, pp. 414-415, for previous information on their arrest.

## **Theresa Squillacote, Kurt Stand, and James Clark: The Espionage Careers of Three Americans**

Three people were arrested on 4 October 1997 and charged with spying for the former German Democratic Republic (GDR) and Russia in an espionage operation that began in 1972: the three coconspirators were Theresa Squillacote; her husband, Kurt Stand; and their friend James Clark. The three were described in court papers as Communist Party sympathizers who had met at the University of Wisconsin in Milwaukee during their student days in the 1970s.

Theresa Marie Squillacote, 39, was a senior staff attorney in the office of the Deputy Under Secretary of Defense for Acquisition Reform until January 1997. According to court papers, Squillacote got her job at the Pentagon after the German reunification in 1990 to gain access to government secrets. She had also sought a job at the White House Office of Management and Budget, which she had hoped to use as a springboard to a position at the National Security Council. Before her Pentagon assignment as a senior staff attorney, Squillacote had worked for the House Armed Services Committee.

Kurt Alan Stand, 42, was a regional representative of the International Union of Food, Agricultural, Hotel, Restaurant, Catering, Tobacco and Allied Workers Association. He was accused of starting his spy activities in 1973 when he was recruited by the GDR (East Germany) to develop spies in Washington. He recruited Squillacote around the time he married her in 1980.

James Michael Clark, 49, a private investigator from Falls Church, Virginia, once worked for a defense contractor at the Rocky Mountain Arsenal in Boulder, Colorado, where he had access to classified information on chemical warfare. Clark was accused of providing East Germany with US State Department documents concerning the Soviet leadership, Soviet nuclear doctrine, and military problems in the Soviet Bloc countries.

On 17 February 1998, Squillacote, Stand, and Clark were indicted by a federal grand jury on charges of conspiring to spy for the former GDR, the former Soviet Union, the Russian Federation, and South Africa. All three were held without bond until their trial on 20 July 1998. According to press reports, the US Justice Department reviewed the allegations to determine if special circumstances existed that warranted seeking the death penalty.

Kurt Stand's parents fled Germany for the United States during Hitler's regime. After the war, his family maintained contact with friends in eastern Germany, which became the German Democratic Republic in 1949. When Stand was approximately 18 years old, his father introduced him to Lothar Ziemer, an officer in charge of Section 3 of the Main Administration for Intelligence's (HVA) Department XI. HVA was the foreign intelligence arm of the Ministry of State Security (MfS),<sup>1</sup> East Germany's intelligence service. The primary mission of Department XI was the operational reconnaissance of North America. Its purpose was to acquire data of significance to the GDR that could not be acquired by legal means.

On an HVA codename agent data sheet, "Junior" is listed with file number "VX2207/73" and is listed as a source with direct access. The origin of the case is listed as "Agent in the West," and Junior is listed as having been recruited in 1972 in the GDR on an "ideological" basis by an MfS officer. Junior is listed as a married American male born in 1954 who lives in New York and is a trade union employee. Junior's target is listed as "Central trade union organization, USA, and direct contact at upper levels." He is deemed to be "reliable," and his means of communication are listed as one-way shortwave radio, accommodation addresses in the GRD and the West, cipher system, microdot, meetings in the West with his principal agent from the GDR, and international travel documents.

The HVA archival record for this file lists the case as having been opened on 1 October 1973 by Lothar Ziemer. An examination of a true name card in the file lists the name "Kurt Stand," born 5 November 1954 in New York. The date and place

---

of birth match those of Kurt Stand. Also in the file was another true name card in the name of “Alan David Jackson” with a date of birth identical to that of Stand. This was an alias on a British passport given to Stand for use in meeting with his GDR handler. The “Jackson” true name card had a stamp with the word “DOKUMENT” on it, which suggests that it was used on a document provided to an HVA agent.

In the early 1970s, Stand began working as an HVA agent responsible primarily for recruiting other agents. In 1976, Stand invited James Michael Clark, a college friend, to travel with him to Germany. Stand introduced Clark to an HVA operative, who introduced him to Ziemer. Ziemer invited Clark to join his organization, which he described as performing intelligence work on behalf of East Germany and other socialist countries, as well as for “liberation movements” in Asia, Latin America, and Africa. Clark agreed to join.

According to an HVA codename data sheet, “Jack” is listed with the file number “XV/43/77” and is listed as a source with direct access. The origin of the case is listed as “Agent in the West,” and Jack is listed as having been recruited in 1976 on an “ideological basis” by an MfS officer. Jack’s target is listed as “Ministry of Defense for a NATO country”. He is deemed “reliable,” and his means of communication are listed as one-way shortwave radio, accommodation addresses in the GDR and the West, a cipher system, code, microdot, contact with agent handler, and international travel documents and/or passport.

The HVA archival record for file number XV/43/77 lists the case as having been opened on 17 January 1977 by Lothar Ziemer, an HVA officer. A true name card listed under the same file number identified James Michael Clark, born 1 April 1948 in Lowell, Massachusetts. This is the correct date and place of birth of Clark.

A second true name card under the same file number lists a “Christopher Michael Glanz,” who was born 1 April 1949. This is believed to be an alias on a British passport that the HVA provided to Clark

for use in meeting with his HVA handlers. The Glanz true name, like the card on “Jackson” under Stand’s file, bears the same stamp with the word “DOKUMENT,” which suggests that it was the alias name used on a document provided to Clark.

Sometime between 1979 and 1981, Stand brought his wife, Theresa Squillacote, into the fold, and she too became what Ziemer described as an “informal collaborator.” At some point, Squillacote’s relationship with Ziemer became more than professional, and they had an affair that lasted until 1996.

Another HVA file, “XV/2207/73,” lists the codename “Resi,” who is described as a “Developmental agent,” recruited in 1981 in the GDR on an “ideological basis.” Resi is a married American female, born in 1957, who lives in Washington, DC, whose occupation is listed as “official lawyer.” Her target is described as “US Federal government.” She is deemed to be “trustworthy,” and her means of communication is listed as “met in West by principal agent from GDR.”

A true name card in the same file lists “Teresa Squillacote” with a birth date of 10 November 1957 in Chicago, Illinois. This is the same date and place of birth of Squillacote, who also was a lawyer with the National Labor Relations Board in Washington. Like Stand and Clark, there is another true name card with the name “Mary Teresa Miller,” with a date of birth identical to that of Squillacote. Like her two codefendants, the name was an alias on a British passport used by Squillacote to meet with her GDR handlers.

The HVA devoted substantial resources to the training of Squillacote, Stand, and Clark. They received training on detecting and avoiding surveillance, receiving and decoding messages sent by shortwave radio from Cuba, mailing and receiving packages through the use of accommodation addresses, using codewords and phrases, using a miniature camera to photograph documents, and removing classified markings from documents. HVA records indicate that the three conspirators together were paid more

---

than \$40,000 between 1985 and 1989, primarily as reimbursement for travel to many countries, including East Germany and Mexico, to meet with their handlers.

The HVA placed great value on these three agents and took numerous steps to protect their security. In their contacts with the three defendants, the HVA made extensive use of codenames and codewords to communicate tasking and operational instructions. For example, in the Operation “Junior” communications, the address frequently used by Squillacote and Stand to communicate with HVA headquarters was “Tante Klara,” and the intelligence service was referred to as the “family.” At various times, HVA intelligence officers received packages or mailings from them, had telephonic contact with them, and met them outside the United States.

In the Operation “Jack” communications, numerous religious references were used, including referring to Clark as a “brother,” referring to an accommodation address as “Sister Margarete,” and making various coded references to “mass,” “pilgrimage,” “Holy Father,” “Holy Church,” “Holy Relics,” the “Voice of God,” the “Sign of God,” and “missionary work.”

HVA intelligence officers used typical espionage tradecraft to protect the security of their operations. This included, for example, the use of routine shopping excursions as a cover for covert telephone calls and to detect FBI surveillance, limitations on the length of telephone calls, and the use of public telephones to make contact.

As part of his “operational plan” devised with Ziemer, Clark moved to Washington, DC, and obtained a master’s degree in Russian. For a time, Clark worked for a private company in a position that required him to obtain a security clearance. He later obtained a position with the US Army in its environmental law division, which also required a security clearance. Clark had friends who worked for the State Department, and through them he obtained numerous classified documents that he turned over to the HVA.

Squillacote and Stand also moved to Washington, DC, and she went to law school at the HVA’s suggestion. Squillacote first followed in her father’s footsteps by becoming an attorney for the National Labor Relations Board (NLRB). When she realized that she had taken a career path that was not “in the best direction,” she began trying to “move her professional work more in line with the commitments that she had made.” To that end, Squillacote used her father’s connections to obtain an unprecedented temporary detail from the NLRB to the House Armed Services Committee.

In 1991, Squillacote obtained a permanent job as an attorney in the Department of Defense, eventually becoming the Director of Legislative Affairs in the Office of the Under Secretary of Defense (Acquisition Reform), a position that required a security clearance and provided access to valuable information. During her tenure with the Federal Government, Squillacote applied for numerous government jobs, including positions with the CIA; NSA; US Army, Navy, and Air Force; and the Departments of State, Commerce, Energy, and Treasury. Apparently, it was not until she began working for the Department of Defense that Squillacote gained access to the kind of information sought by her handlers.

By the time Squillacote had secured her DoD position, however, the GDR had collapsed. After the fall of the Berlin Wall, Ziemer began working with the Committee for State Security (KGB), the Soviet Union’s intelligence agency. Ziemer maintained his relationships with Squillacote, Stand, and Clark during this time, and they, too, became involved with the KGB.

Squillacote, Stand, and Clark each traveled overseas to meet with Ziemer during the period after the collapse of the GDR. Ziemer instructed all three to purchase Casio digital diaries with interchangeable memory cards. The three Americans, Ziemer, and their KGB contacts communicated with each other by exchanging memory cards.

---

In April 1992, Ziemer and another former HVA official were arrested and ultimately convicted for their postunification intelligence activities with the KGB. Squillacote, Stand, and Clark became understandably concerned about their personal safety after Ziemer's arrest. They knew that "Western services" were looking for two men and one woman operating out of Washington, DC, and that the Western services were aware of the codenames they had used. They believed, however, that Ziemer and other former HVA officials would not compromise their identities. When Ziemer was released from prison in September 1992, Squillacote, Stand, and Clark reestablished a system of communication with him, one purpose of which was to keep everyone informed about any threats to their safety.

From the beginning of their involvement with the HVA, Squillacote, Stand, and Clark operated independently of each other and generally were unaware of the others' activities. After Ziemer's arrest in 1992, however, the three began talking in detail about their activities and precautions needed to maintain their security. They began discussing the possibility of future intelligence work, perhaps for Vietnam or Cuba. Squillacote also talked to Clark about her interest in South Africa's Communist Party.

In 1994, Squillacote, as part of her search for "another connection," went to Amsterdam to speak to David Truong, whom she had met in college. Truong, who had been convicted of espionage on behalf of North Vietnam, was intrigued, but took no further action.<sup>2</sup>

In 1995, Squillacote went to great lengths to obtain a post office box under the name of "Lisa Martin." In June 1995, Squillacote, as Lisa Martin, sent a letter to Ronnie Kasrils, the Deputy Defense Minister of South Africa. Kasrils was a Communist Party official and had received training in East Germany, the Soviet Union, and Cuba. The letter, which took Squillacote months to write, was primarily devoted to Squillacote's explanation for the collapse of socialism that began with the fall of the Berlin Wall and her views on how the

Communist movement should proceed in the future. The letter was an attempt by Squillacote to make a connection with Kasrils, whom Squillacote hoped would "read between the lines."

Stand and Clark were aware of Squillacote's letter, but Clark apparently doubted its effectiveness. In February 1996, Squillacote received a Christmas card from Kasrils addressed to L. Martin. In the card, Kasrils thanked "Lisa" for "the best letter" he had received in 1995. Stand and Squillacote were thrilled they had received the note, and they began to think that perhaps a connection could be made.

In September 1996, Squillacote found another letter from Kasrils in her Lisa Martin post office box. The letter stated that, "you may have the interest and vision to assist in our struggle," and invited Squillacote to a meeting in New York City with a representative of "our special components."

Squillacote and Stand, however, were unaware that, for many years, they had been the subjects of an intense FBI investigation. As part of its investigation, the FBI in January 1996 obtained authorization to conduct clandestine electronic surveillance, which included the monitoring of all conversations in their home, as well as calls made to and from their home and Squillacote's office. Through its investigation, the FBI had learned of Squillacote's letter to Kasrils and their response to the February 1996 note from Kasrils. The Kasrils letter of September 1996 was, in fact, written by the FBI as part of a false flag operation intended to uncover information about the previous espionage activities of Squillacote, Stand, and Clark.

When designing the false flag operation, the FBI's Behavioral Analysis Program (BAP) Team prepared a report "to examine the personality of Squillacote and based on this examination, to provide suggestions that could be used in furthering the objective of this investigation—to obtain evidence regarding the subject's espionage activity." The BAP report was based on information the FBI had learned during its extensive investigation and surveillance of the couple.

---

The BAP report traced Squillacote's family background, including the suicide of her older sister and her mother's history of depression. The report stated that Squillacote was suffering from depression and listed the antidepressant medications she was taking. The primary focus of the BAP report, however, was Squillacote's emotional makeup and how to tailor the approach to her emotional characteristics.

The report described Squillacote as having "a cluster of personality characteristics often loosely referred to as 'emotional and dramatic.'" It recommended taking advantage of Squillacote's "emotional vulnerability" during her period of grieving over the then-recent end of her affair with Ziemer. It further recommended using an undercover agent "who possesses the same qualities of dedication and professionalism as her last contact," and "structuring the undercover agent's pitch" to mirror her relationship with Ziemer. The BAP report also made very specific recommendations about how the false flag operation should be designed:

*The following scenario has been developed upon an analysis of the subject's personality, and includes suggestions designed to exploit her narcissistic and histrionic characteristics. It is believed that [Squillacote] will be susceptible to an approach through her mail drop based on her recent rejection by her long-term German handler, and her thrill at receiving a Christmas card from the South African official.*

The report suggested the use of a letter from "the object of [Squillacote's] adulation in South Africa." It recommended that the letter instruct Squillacote to travel a circuitous route to the location of the first meeting to "add a sense of excitement and intrigue to the scenario." The report recommended the use of a mature male undercover agent, who should "capitalize on [Squillacote's] fantasies and intrigue" by making a "friendly overture," and "act [ing] professional and somewhat aloof yet responsive to her moods. The initial meet should be brief and leave [Squillacote] beguiled and craving more attention."

The false flag letter received by Squillacote in September 1996 served its intended purpose. Unaware of any FBI involvement, Squillacote and Stand were thrilled about the letter, and Squillacote began enthusiastically making plans for a trip to New York City to meet the South African emissary.

In October 1996, Squillacote met with an undercover FBI agent posing as a South African intelligence officer. She had face-to-face meetings with the agent a total of four times, including one meeting where she brought Stand and her two children. Several letters were also exchanged, including a letter that Squillacote wrote at the request of the undercover agent describing her previous activities with Ziemer. In these meetings and letters, Squillacote expressed her enthusiasm for her new South African connection and her hope for a productive collaboration.

Throughout her association with the undercover agent, Squillacote discussed the possibility of bringing Ziemer and other former East German contacts into the operation. In December 1996, she contacted Ziemer to see if he was interested in the operation. According to Squillacote, Ziemer's response was "[y]es, yes, yes, yes, yes!"

At the second meeting with the undercover agent on 5 January 1997, Squillacote presented the agent with four classified documents she had obtained from the Department of Defense. Although the agent had never requested any documents or classified information from Squillacote, she explained that one day when she and her secretary were alone in her office, she decided to "score what [she] could score." In fact, she had obtained one of the documents even before her first meeting with the undercover agent. The documents Squillacote gave to the undercover agent were:

- *Defense Planning Guidance for Fiscal Year 1997 through 2001*, a numbered document, classified Secret, with restricted dissemination.
- *Defense Planning Guidance Scenario Appendix for 1998 through 2003*, a numbered document classified at the Secret level, which forbade reproduction or further dissemination without authorization.

- 
- *Defense Planning Guidance, Fiscal Years 1996 through 2001, Final For Comment Draft*, which was classified Secret, with restricted dissemination.
  - An untitled CIA intelligence report classified Secret, with restricted dissemination.

Three of the documents Squillacote gave to the undercover agent were copies; the *Defense Planning Guidance Scenario Appendix* was an original that Squillacote said would not be missed. These documents formed the basis of the charges against Squillacote and Stand.

Shortly after this meeting, Squillacote quit her job with the Department of Defense; a political maneuver she hoped would put her in position for a more prestigious job.<sup>3</sup> Nonetheless, Squillacote continued meeting and corresponding with the undercover agent for several more months until she and Stand were arrested in October 1997.

A search of their home uncovered a wealth of incriminating evidence, including a miniature camera, a Casio digital diary and memory cards, and an extra copy of two of the documents given to the undercover agent. Clark eventually pleaded guilty to a single charge of conspiring to commit espionage, and he testified for the government at the trial of Squillacote and Stand.

At trial, the government introduced certain HVA records, including true name cards showing the names and addresses of Squillacote, Stand, and Clark, as well as documents listing some of their code names and the names of the operations to which they were assigned. The HVA records listed Squillacote as “a developmental agent whose target was the US Government” and described Squillacote as trustworthy.

The records described Stand as reliable and listed him as a source with direct access, with a target of “U.S. union/organization, direct/upper level, IBFG union, U.S.A.” Clark was listed as a “source with direct access,” whose activities were targeted against the “Defense Ministry NATO Country FRG USA.” The records also described Clark as reliable. Other than the four documents passed to the undercover agent, the

government presented no evidence establishing that Squillacote or Stand had previously supplied classified documents or information to Ziemer or anyone else.

Clark pleaded guilty on 3 June 1998 to conspiracy to commit espionage, admitting that he passed classified documents to the former GDR and sought to spy for Moscow as well. On 5 December 1998, Clark was sentenced to 12 years and seven months in prison. Clark had admitted earlier in a plea bargain with prosecutors that he conspired with his two leftist college friends to spy on the United States.

Squillacote and her husband, Stand, were convicted on 23 October 1998, of conspiring to commit espionage, attempting espionage, and illegally obtaining national defense documents. Accused of spying for the former GDR, the former Soviet Union, and South Africa, the couple was described as “Communists on an expense account” who took lavish trips abroad, courtesy of the East German Government, at a time when they had applied for food stamps and for help paying their electric bills. The two also sought jobs in and around the government and stole and smuggled classified documents. Prosecutors never established in court how much the couple was paid for their activities.

On 22 January 1999, Squillacote and Stand were sentenced to lengthy prison terms. A federal judge handed Squillacote a sentence of 21 years and 10 months in prison. Stand received 17 years and six months in prison. The couple had faced a maximum sentence of life in prison for spying. Federal prosecutors argued that the couple should have received longer prison terms, more than 27 years for Squillacote and more than 21 years for Stand, for betraying their country. But the couple’s attorneys sought leniency. The amount of prison time that the judge gave the couple was the minimum required under federal sentencing guidelines.

Squillacote and Stand appealed, raising numerous issues that arose during the course of the prosecution. They filed several pretrial motions to suppress various portions of the government’s evidence. The District Court denied each of the motions, and they challenged those rulings on appeal.

---

One of their motions, prior to their trial, sought to suppress the evidence of the Foreign Intelligence Surveillance Act (FISA)<sup>4</sup> surveillance. They attacked the validity of the surveillance<sup>5</sup> on several grounds, all of which were rejected by the District Court. On appeal, however, they pressed only one FISA-related issue. They asserted that the surveillance was improper because there was no probable cause to believe that Squillacote or Stand were agents of a foreign power. The court disagreed, stating that under FISA, an agent of a foreign power is any person who “knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States.” The court added that a person who knowingly aids and abets another engaging in such clandestine intelligence activities, or one who knowingly conspires with another to engage in the clandestine intelligence activities is also considered an agent of a foreign power.

Squillacote and Stand also sought to suppress the evidence obtained during the search of their home, including the miniature camera, the digital diary and memory cards, a doll with a roll of miniature film hidden inside, and copies of two of the documents Squillacote passed to the undercover agent. They contended that the search was conducted in flagrant disregard of the express terms of the warrant and that the District Court, therefore, erred in denying their suppression motion.

The warrant authorizing the search of their home stated that the government was to search the residence on or before 13 October 1997 (not to exceed ten days)—including serving the warrant and making the search in the daytime between 6:00 A.M. and 10:00 P.M. The search extended over six days, with two FBI agents remaining at the house each night. It was the presence of the FBI agents in the home after 10:00 p.m. that formed the basis of their suppression arguments.

The couple first argued that, by remaining inside their home overnight for five consecutive nights, the FBI searched the home at night, thus flagrantly disregarding the warrant’s time restriction. The

court was not persuaded by this argument. Preliminarily, the court rejected the main premise of their challenge to the search: that the presence of the agents in the house, in and of itself, constitutes a search that should be considered separate and distinct from the authorized search of the residence.

The court concluded that the government did not exceed the scope of the warrant, and even if the government did exceed the scope of the warrant, blanket suppression of all evidence seized would not be required. When denying their motion to suppress, the District Court found that the government complied with the warrant by conducting the search “during the hours that were set out in the warrant.” This conclusion was supported by the affidavit of Special Agent Gregory Leylegian, an FBI agent who took part in the search. Leylegian’s affidavit stated that the FBI “conducted no searching of the premises after 10:00 p.m. each day” and that “the FBI maintained two agents on the premises each night to preserve the integrity of the search process, to expedite the completion of the search, and to maintain security of the premises to prevent the removal or destruction of evidence.”

During the FISA-authorized surveillance, the government intercepted several telephone calls between Squillacote and her psychotherapists. Only the first two of these conversations, however, were listened to or transcribed by the government.<sup>6</sup> Once the supervising FBI agent learned of the conversations, she instructed the agent responsible for transcribing and indexing the conversations not to listen to, index, or transcribe any other conversations between Squillacote and her therapists.

The couple moved to suppress any evidence derived from the privileged communications and requested a hearing to require the government to prove that the evidence it would present at trial was derived from sources independent of the privileged communications. The District Court refused to hold the hearing, concluding that such a hearing was required only when a constitutionally based privilege was at issue.

---

On appeal, the couple contended that the FBI employee who listened to and transcribed the conversations between Squillacote and her therapists was involved in the preparation of Squillacote's BAP report and that privileged information was, therefore, used to formulate the false flag operation that led to their arrest. The couple contended that any evidence derived from the privileged information should have been suppressed and that they were entitled to a hearing to vindicate the principles set forth by the Supreme Court in *Kastigar v. United States*, 406 U.S. 441 (1972).

The court, however, concluded that the *Kastigar* case simply was not applicable to this case. In *Kastigar*, the issue was whether a witness who asserts his Fifth Amendment privilege against self-incrimination may be compelled to testify "by granting immunity from the use of compelled testimony and evidence derived therefrom ('use and derivative use' immunity), or whether it is necessary to grant immunity from prosecution for offenses to which compelled testimony relates ('transactional' immunity)."

Because this case did not involve the use of compelled testimony, the District Court refused the appellants' request for a *Kastigar*-type hearing. In addition, because the privilege at issue here was not a constitutional one, the District Court refused to suppress any evidence arguably derived from the government's interception of the two conversations with Squillacote's therapists.

Perhaps some of the most damaging evidence introduced against Squillacote and Stand at trial were the HVA documents—the true name cards listing their names and their codenames and the agent data sheets showing the nature of their assignments for the HVA. The couple moved to prevent the introduction of these documents, but the District Court denied the motion. On appeal, they contended that the documents were improperly admitted, arguing that they were not properly authenticated and that, even if authenticated, the documents were inadmissible hearsay. The Federal Rules of Civil Procedure provide that official records of a foreign country

are considered properly authenticated if the records are attested by a person authorized to make the attestation, and accompanied by a final certification as to the genuineness of the signature and official position (i) of the attesting person, or (ii) of any foreign official whose certificate of genuineness of signature and official position relates to the attestation or is a chain of certificates of genuineness of signature and official position relating to the attestation.

In this case, the government presented a certification from Dirk Dorrenberg, the director of the counterespionage and protective security department of the *Bundesamt für Verfassungsschutz*, the counterintelligence service for the unified Federal Republic of Germany (FRG). In his certification, Dorrenberg stated that the FRG is the legal successor to the GDR and that he had the "authority to make this certification by virtue of [his] official position and area of expertise."

Dorrenberg stated that he had compared the HVA documents introduced by the government to "actual duplicates" of the original records, and he certified that the government's copies were "true and correct copies" of "genuine and authentic records" of the HVA. Dorrenberg also certified that the signature of Lothar Ziemer appearing on some of the records was "genuine and authentic."

The government also presented a final certification from Manfred Bless, an FRG representative "assigned and accredited to the United States as a Counselor, Political Section, of the Embassy of the Federal Republic of Germany, in Washington, D.C." In this final certification, Bless certified that Dorrenberg held the position claimed in the Dorrenberg certification and that Dorrenberg was authorized to make the certification. These certifications comply in all respects with the requirements of Rule 44(a)(2) and Rule 902(3). Therefore, whether the documents are considered official documents or official records, the District Court concluded that the government adequately authenticated the HVA documents.

---

The couple, however, contended that the certification process of Rule 902(3) is intended to confirm the signature or attestation contained in the offered document. According to them, if the document being offered into evidence does not contain a signature, then a self-serving declaration of authenticity is meaningless. Thus, they contended that many of the HVA documents were not subject to self-authentication under the rules because the documents themselves were not signed or did not contain an attestation.

The court ruled that this argument is without merit. Nothing in Rule 44(a)(2) or in Rule 902(3) requires that the documents themselves be signed or contain an attestation within the body of the document. The rules are written in the alternative—foreign documents may be authenticated by a certification from the official executing the document or by an official attesting to the document. Thus, so long as a proper official attests that the proffered document is true and genuine, it simply does not matter whether the document itself is signed or contains its own attestation.

As noted above, Rule 44(a)(2) also requires a final certification regarding the signature and position “(i) of the attesting person, or (ii) of any foreign official whose certificate of genuineness of signature and official position relates to the attestation or is in a chain of certificates of genuineness of signature and official position relating to the attestation.” Seizing on these requirements, the couple contended that neither the Dorrenberg certification nor the Bless certification establish that “Dorrenberg is an official ‘whose certificate of genuineness of signature and official position relates to the execution or attestation’ or that his certificate is in a ‘chain of certificates of genuineness of signature and official position relating to the execution or attestation.’ ”

The court ruled that this second argument was likewise without merit, as it was premised upon a fundamental misapprehension of the requirements for the authentication of foreign documents. An examination of Rule 44(a)(2) and Rule 902(3) reveals two requirements for the authentication

of a foreign document. First, there must be some indication that the document is what it purports to be. Thus, a proper official in his official capacity must execute the proffered document, or a proper official must attest to the genuineness of the document in his official capacity.

In this case, the government satisfied the first requirement of establishing that the HVA records were what they purported to be by presenting Dorrenberg’s certification that the government’s records were true and accurate copies of genuine HVA records. The government then established that the official vouching for the document was who he purported to be in the first manner described above—by presenting a final certification from another official establishing that it was Dorrenberg’s signature on the proffered certification and that Dorrenberg was authorized to attest to the authenticity of the HVA documents.

Because the government established the genuineness of the signature and position of the person attesting to the documents, the portions of the rules dealing with officials that related to the execution or attestation in the chain of certifications were not applicable. Finally, contrary to the couple’s suggestions, the rules do not require the official attesting to the genuineness of foreign documents or records to have possession or custody of the proffered documents, to be an expert in handwriting analysis, or to have been associated with the foreign government at the time the documents were created.

The couple also challenged the District Court’s ruling that the HVA documents were admissible as statements of a coconspirator under Rule 801(d)(2)(E) of the Federal Rules of Evidence. The Appeals Court reviewed the District Court’s admission of evidence under Rule 801(d)(2)(E) for an abuse of discretion. In the Appeals Court’s view, the District Court properly admitted the HVA records as statements by a coconspirator.

First, the indictment specifically charged the couple with conspiring with, among others, “agents and officers of the GDR,” and the

---

government presented ample evidence supporting that allegation, including the government's overwhelming evidence of their relationship with Lothar Ziemer, whose signature appears on many of the disputed HVA documents. Second, although some of the documents are undated, many bear dates within the text that are clearly within the course of the conspiracy as defined by the government's evidence. Many of the undated HVA documents show the same registration number as the dated documents and the documents bearing Ziemer's signature, thus establishing a connection between all of the HVA documents. Accordingly, the government's evidence demonstrated that the statements were made during the course of the conspiracy. Third, there can be no real dispute that, by compiling the information contained in the disputed documents—the couple's real and code names, their addresses, the object of their assignments, and how they could be contacted—the GDR was acting in furtherance of the conspiracy.

Although the identity of the declarant of the unsigned documents may not be known, the only conclusion that can be drawn from the information included in the documents—information that was corroborated in many respects by Clark's testimony and by Squillacote's own statements to the undercover agent—is that the documents were created by or at the direction of East German agents who had knowledge of and were involved in the conspiracy with them. While there may be cases where the inability to identify the declarant of an alleged coconspirator's statement could render the statement inadmissible, this is not one of those cases. The HVA documents were sufficiently connected to each other and to the conspiracy established by the government's evidence to make them reliable and admissible under Rule 801(d)(2)(E), notwithstanding the government's inability to identify the declarants. The Appeals Court, therefore, concluded that the HVA records were properly authenticated and were properly admitted as statements of coconspirators.

Finally, the couple raised numerous issues in connection with the District Court's instructions to the jury. Their challenges involved the District

Court's instructions on their entrapment defense, the court's failure to include an instruction on multiple conspiracies, and its explanation to the jury of "information relating to the national defense."

Squillacote and Stand contended that the government's first contact with Squillacote—the phony Kasrils letter—was an "approach," not an "encounter," because encounter can mean only a face-to-face meeting. Thus, they argued that, by instructing the jury to consider predisposition that existed before the first encounter with the government, the jury may have concluded that Squillacote became predisposed to commit the crimes only after receiving the Kasrils letter, but still rejected the entrapment defense because the disposition arose before Squillacote met the undercover agent for the first time. The Appeals Court believed that the District Court's instruction sufficiently directed the jury's focus to the proper time frame for determining the existence of Squillacote's predisposition, particularly since there was no dispute that the government's first contact was the Kasrils letter.

Squillacote clearly was in the position to commit the crimes with which she was charged. After years of trying, Squillacote finally had a job that provided her with access to classified information and documents. She had received excellent training in the arts of espionage, and she had a long relationship with a "spy-master" who was trying to find another connection interested in the services that she and her coconspirators could provide. In addition, as evidenced by her approach to David Truong—the convicted spy—and her letter to her South African hero, Squillacote herself was actively searching for another customer for her skills. Thus, Squillacote was in the position to become an active spy even without the help of the undercover agent. If the evidence in this case did not establish Squillacote's readiness, then the Appeals Court could not imagine what would be sufficient to do so.

The couple's theory of the case was that the FBI, through its BAP report profiling Squillacote, masterfully catalogued Squillacote's every emotional and psychological vulnerability. The

---

FBI then used this information to devise an undercover operation exploiting these weaknesses to ensure that Squillacote would fall for the undercover agent's pitch. The couple claimed that the agent induced Squillacote into going along with his scheme by making subtle psychological appeals to which he knew Squillacote would be uniquely vulnerable. Consistent with this theory of entrapment, the couple's lawyer requested the following instruction on entrapment:

*Entrapment occurs . . . [w]here the Government goes beyond providing an opportunity for a crime but instead induces its commission by taking advantage of the defendant through such persuasion as appealing to the defendant's political beliefs or to some other alternative, non-criminal type of motive, or by playing on defendant's personal sympathies and life experiences, or by exploiting the unique vulnerabilities of the defendant. The law of entrapment forbids the conviction of [a] person where the Government has played on the weaknesses of an innocent party and beguiled her into committing crimes which she otherwise would not have attempted had the Government not induced her.*

The District Court refused to give this instruction. Instead, the court instructed the jury as follows:

*A person is entrapped when that person has no previous disposition or willingness or intent to commit the crime charged and is induced by law enforcement officers to commit the offense. In determining the question of entrapment, you should consider all of the evidence received in this case concerning the intentions and disposition of the defendant before encountering the law enforcement officer, as well as the nature and the degree of the inducement provided by the law enforcement officer.*

In the Appeals Court's view, the evidence of Squillacote's predisposition can only be described as overwhelming. The government's evidence established that Squillacote's involvement with the HVA went back almost twenty years. Through her

East German contacts, Squillacote learned how to determine if she was being followed and how to evade those who might be following her, how to receive and decipher sophisticated coded messages, how to use the miniature document camera, and how best to remove any "classified" markings on documents. After the fall of East Germany, when Squillacote finally had a job that gave her access to sensitive information, Squillacote herself sought out opportunities to use these skills. She contacted David Truong, a convicted spy, in the hopes of establishing a new "connection," and she sent her fan letter to Kasrils, the South African official, hoping that he would "read between the lines." That Squillacote actively sought employment as a spy is powerful evidence that she was disposed to committing espionage well before the government first contacted her.

Squillacote's response to the government's phony Kasrils letter was also strong evidence of her predisposition. It was perhaps an understatement to say that Squillacote was ecstatic when the Kasrils letter arrived in the mail. When she received the letter, Squillacote called her brother to tell him about the letter. While laughing and crying, Squillacote said, "Michael, I did it. I did it Mike. All those years. All those years and I did it. I did it."

To her husband, Squillacote described the letter as "really, really, really, amazing." In fact, Squillacote was so excited when she received the phony letter that she even told her children about the impending meeting. In another telephone conversation with her brother, Squillacote explained how proud she was that Kasrils had "read between the lines" of her letter. Squillacote's predisposition to commit espionage is also evidenced by her statements to the undercover agent during their first meeting.

In that meeting, the agent identified himself as being with the South African Intelligence Service, and he explained that, "there are still operations being conducted without the full knowledge of everybody in the state, for reasons, I guess, you can well understand." Squillacote responded that "[t]his is an area that's not unfamiliar to me."

---

Squillacote then elaborated that she had been associated with similar activities “in another kind of capacity” for many years, “so, you should understand that this is not a tabula rasa for me. I’m coming with a history.” Squillacote described her covert activities as her “raison d’être.” When the undercover agent told Squillacote that he had “done some things that this government would consider to be illegal,” Squillacote responded, “[b]een there,” and she explained that she had “violated Federal eighteen, lots and lots.”<sup>7</sup>

To the Appeals Court, these statements clearly showed that Squillacote was more than willing, without any encouragement from the government, to commit espionage. Perhaps the most compelling evidence of Squillacote’s predisposition is related to the documents she passed to the undercover agent at their second meeting.

The government’s evidence established that Squillacote obtained one of the documents sometime before her first meeting with the undercover agent, even though the phony Kasrils letter did not request, or even suggest, that Squillacote bring any classified materials to the meeting. Extra copies of two of the documents were found in Squillacote’s home when the government executed its search warrant. Thus, even before she first met the undercover agent, Squillacote had already violated 18 U.S.C.A. § 793(b) by taking or copying classified national defense information. Clearer evidence of predisposition is difficult to imagine.

The government’s evidence established that Squillacote, Stand, and Clark were involved in a single conspiracy to compromise information related to this country’s national defense. Stand, who was recruited by Ziemer, recruited both Clark and Squillacote. Ziemer was the primary handler for Stand, Squillacote, and Clark, and the three received largely the same training and used the same methods of communicating with their East German contacts. After the collapse of the GDR, the three continued their relationships with Ziemer, which expanded to include the KGB. With the knowledge of the other conspirators, Squillacote also sought to develop new contacts with others who might be interested in what the group had to offer.

Stand was aware of Squillacote’s letter to Kasrils, as well as her meetings with the undercover agent. In fact, Stand helped Squillacote remove the classified markings from the documents she provided to the agent. Clark was likewise aware of the letter she wrote to Kasrils, and Squillacote sought to involve Stand, Clark, and Ziemer in the operation after the undercover agent contacted her.

In the Appeals Court’s view, this evidence was more than sufficient to support the finding of a single conspiracy. That Squillacote, Stand, and Clark were not always aware of the others’ activities is part of the standard operating procedure for those engaged in espionage and would not prevent the jury from determining that a single conspiracy existed.

Although it is possible that Squillacote’s South African foray could be viewed as separate from the original conspiracy, it was certainly closely related to the conspiracy charged in the indictment, a conspiracy in which the evidence overwhelmingly established the involvement of Squillacote and Stand. Therefore, because the evidence did not establish that the couple was involved “only in ‘separate conspiracies unrelated to the overall conspiracy charged in the indictment,’” the District Court properly refused to instruct the jury on multiple conspiracies.

The couple made much of Clark’s testimony on cross-examination that he did not have an agreement with them to commit espionage, that he lost contact with them for several years in the late 1970s and early 1980s, and that he was not involved in the South African effort. Given that Clark pleaded guilty to the charge that he conspired with Squillacote and Stand to commit espionage, it seems unlikely that the jury would have found this testimony particularly persuasive. In any event, to accept this argument would have required the Appeals Court to consider only Clark’s testimony and to ignore the other evidence tending to show the existence of a single conspiracy or multiple—but still related—conspiracies, which, of course, the Appeals Court did not do at this stage of the proceedings.

---

After carefully reviewing the record and considering the arguments of the parties, the Appeals Court found no reversible error in the proceedings. Accordingly, the convictions of Squillacote and Stand were affirmed.

In April 2001, the Supreme Court declined to hear an appeal by Squillacote and Stand, which challenged the government's ability to obtain wiretaps and search warrants under FISA on the basis of secret evidence. Attorneys for Squillacote and Stand argued that prosecutors should have been forced to show them the evidence underlying a FISA wiretap that remained on a telephone at the couple's home for 550 days.

## Endnotes

<sup>1</sup> *Ministerium fur Staatssicherheit*.

<sup>2</sup> David Truong, also known as Truong Dinh Hung, and Ronald Louis Humphrey were sentenced on 7 July 1978 to 15 years each in prison for espionage. Humphrey, a US Information Agency officer, met Truong while trying to get his mistress and her children out of Vietnam in the mid-1970s. Truong, who portrayed himself as an anti-Communist, had many official contacts in the US Government, including contact with William Colby at the CIA. The FBI arrested the two men on 31 January 1978 and charged them with seven counts of espionage on behalf of North Vietnam. Humphrey took classified State Department documents and passed them to Truong who handed them over to a courier for delivery to North Vietnamese officials.

<sup>3</sup> However, Squillacote explained to the undercover agent that her involvement in the political maneuvering and her decision to quit were primarily motivated by her "joint efforts" with the undercover agent. Squillacote believed that her former Department of Defense boss might be named Deputy Secretary of Defense and that she would be able to follow her former employer back into the Department. Squillacote described this scenario as "the big time," noting that if it worked out, there would be a "straight f---ing line," presumably to the Secretary of Defense. This scenario never came to pass.

<sup>4</sup> FISA was enacted "to put to rest a troubling constitutional issue" regarding the President's "inherent power to conduct warrantless electronic surveillance in order to gather foreign intelligence in the interests of national security," a question that had not been definitively answered by the Supreme Court. FISA thus created a secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this nation's commitment to privacy and individual rights.

<sup>5</sup> The government conducted 550 consecutive days of clandestine surveillance of them, surveillance that was authorized under the Foreign Intelligence Surveillance Act of 1978.

<sup>6</sup> Actually, one of these conversations was between Stand and one of Squillacote's therapists. Because Squillacote gave the therapist permission to talk to Stand, the court assumed for purposes of their motion that the conversation was privileged, and, in the interest of convenience, the court referred to both conversations as having taken place between Squillacote and her therapists.

<sup>7</sup> Given the context, it is apparent that this statement is a reference to Title 18 of the United States Code, which is entitled "Crimes and Criminal Procedure."

## French SIGINT Targeting

The French magazine *Le Point* reported in June 1998<sup>1</sup> that France systematically listens in on the telephone conversations and cable traffic of many businesses based in the United States and other nations. The article also reports that the French Government uses a network of listening stations to eavesdrop and pass on commercial secrets to French businesses competing in the global economy.

The article goes on to state that the French secret service, DGSE, has established listening posts in the Dordogne (southern France) and also in its overseas territories, including French Guiana and New Caledonia. The article attributes to an unnamed “senior official within this branch of the French secret service” the claim, “This is the game of the secret war,” adding that US listening posts do the same. The magazine report says that Germans who bought into the French Helios 1A spy satellite system are being given access to political and economic secrets as part of a Franco-German agreement to compete with a commercial information agreement between the United States and Britain.

According to multiple sources, on 5 July 1999, TotalFina—the Franco-Belgium oil company—initiated a \$43 billion hostile takeover bid to buy the French oil company Elf Aquitaine. Elf formally rejected the takeover bid and on 19 July offered a counterbid of \$51 billion. After two months of acrimony, the takeover battle ended when both companies announced they had agreed to a friendly merger. The TotalFina–Elf merger would result in the world’s fourth-largest oil company, ahead of Chevron and Texaco, but still well behind Exxon-Mobil, Royal Dutch Shell, and BP-Amoco-Arco.

The struggle of these two world-class companies is characteristic of the hostile takeover era that has dawned in Europe. According to Mr. Terry Desmarest, President and Chief Executive of TotalFina, the grab for Elf was “to assure continued solid growth and to take our place as an oil major of the first rank, at a time when the industry is restructuring on a global basis.”

But wait; could there be more to this story than meets the eye? Did TotalFina beat Elf to the punch? Perhaps it did, but according to Paris *Le Monde*, which cited London’s *Financial News*, TotalFina’s bid followed an indiscretion on the part of two of Elf’s advisory bankers discussing preparations for a raid on TotalFina that prompted Desmarest to carry out his surprise attack. The indiscretion took the form of a conversation between the two French bankers on a flight between London and Paris. Unfortunately for Elf, the conversation was overheard by a TotalFina financier traveling on the same flight who chose to disregard the old adage that a gentleman does not eavesdrop on other people’s conversations.

The French article goes on to discuss the gravity of the situation, noting that, according to one source, “travelling constantly, business bankers, who spend days and nights preparing a takeover bid, sometimes commit indiscretions due to tiredness. Shouting on a mobile phone in a business class waiting room, reading presentation documents during a flight, or boasting to a colleague are all high risk actions.” The article further notes, “the new boys are easily recognizable in the plane. They get out their files as thick as a telephone book, whereas the veterans have a nap or read a bestseller.”

According to the *Sunday Times*<sup>2</sup> (London), French intelligence is intercepting British businessmen’s calls after investing millions of francs in satellite technology for its listening stations. Since the French Government upgraded its signals intelligence capabilities last year, secret service elements are now using it to tap into commercial secrets. At least eight centers scattered across France are being “aimed” at British defense firms, petroleum companies, and other commercial targets.

Eavesdroppers can “pluck” digital mobile phone signals from the air by targeting individual numbers or sweeping sets of numbers. Targets have included executives at British Aerospace (BAe), British Petroleum, and British Airways, according to French sources.

---

Senior executives have been told not to discuss sensitive issues on mobile phones, and BAe staff have been told to be “especially careful” during campaigns for new business, such as the current battle to supply Eurofighter missiles.

An executive within one British defense firm said, “Top people use the same mobile telephones as anyone else, without any sort of high-tech security equipment. There is an understanding that we need to be careful. People never say anything that they would not want heard elsewhere —especially at sensitive times and during projects when other people may have an interest in listening.”

A source in Paris with links to French intelligence said: “It is not fair to say that France is constantly listening to British or German companies, but there may be times when certain areas might be targeted.”

This report comes on the heels of another *Sunday Times* article in late 1999, which reported that BAe executives were burglarized at a Toulouse hotel by French secret service agents involved in industrial espionage. The raid is believed to have been carried out by a *Direction et Surveillance du Territoire* (DST) unit called *Protection du Patrimoine Economique*, which is said to conduct specialized break-in operations targeting foreign companies.

The agents allegedly searched briefcases and stole documents from BAe officials while they were meeting with officials from the French aviation company, Airbus Industrie. The French officials, who apologized and returned photocopies of the company documents, notified the British. The incident involved at least four BAe staff members who were discussing aviation contacts and BAe’s future relationship with Airbus.

## Endnotes

<sup>1</sup> See *Le Point*, 6 June 1998, pp. 61-64.

<sup>2</sup> See *Sunday Times*, 23 January 2000.

## Updates on Two Espionage Cases

*(Editor's Note: Information on the espionage cases of Douglas F. Groat and Robert Kim appear in Volume III of the CI Reader on pages 408 and 341, respectively. Since then the following activities have occurred in their cases.)*

### Douglas F. Groat

On 25 September 1998, former CIA covert operative Douglas F. Groat was sentenced to five years in prison after having pleaded guilty in July to one count of extortion. He had attempted to extort \$1 million from the Agency in exchange for his silence about overseas operations. As part of the plea agreement, Federal prosecutors dropped four counts of espionage.

According to the indictment, Groat not only disclosed damaging intelligence information to foreign countries, but also tried to extort more than \$500,000 from the CIA under the threat he would tell certain governments of highly classified CIA operations. Prosecutors refused to identify the two countries Groat allegedly aided.



The CIA employed Groat from 1980 to 1996, where he worked in the Science and Technology Directorate. In the spring of 1993, he was placed on administrative leave for “personnel” issues and was fired three years later. Intelligence officials, and Groat’s own relatives, have described him as a

disgruntled employee who was under suspension for botching an overseas operation involving a break-in at a foreign embassy.

The plea agreement eased prosecutors’ concerns that a trial on all the charges might have forced them to disclose sensitive information in open court. On the other hand, the initial charges could have carried the death penalty. Groat agreed to help the government sort out whether his activities during or after his tenure at the Agency breached national security, and he agreed to submit any books, articles, or interviews to federal officials for security review.

### Robert Kim

On 4 October 1999, the US Supreme Court rejected, without comment or dissent, an appeal by Robert Kim, 59, who is serving a nine-year sentence for spying on behalf of South Korea. Kim, a former US Navy computer technician who was arrested in 1996, argued that his civil rights had been violated and that his status as a naturalized US citizen, rather than a US citizen by birth, added to the severity of his sentence. He admitted shortly after his arrest that he had collected military documents to pass on to a captain in the South Korean Navy. The US Justice Department had asked the Supreme Court to reject Kim’s appeal.



A South Korean Foreign Affairs and Trade Ministry spokesman said that his government would not get involved in the case, noting that “the government

---

is not in a position to officially get involved in a US Court's ruling on Kim's espionage conviction, which went thorough US legal procedures."

The "Committee To Rescue Robert Kim," which was originally established in March 1997 but remained dormant until 1998, held an emergency meeting at Seoul's Koreana Hotel on 31 October 1998 to start a campaign to rescue Kim. The committee, composed of some 100 people, decided to set out on a full-scale campaign because of their disappointment in former President Kim Yong-sam who visited the United States in 1998 and said "the ROK Government would not interfere in the matter because Robert Kim is an American." Headed by Ryu Chae-kol, vice president of the National Congress for New Politics (NCNP), Yi T'ae-pyon, a member of the United Liberal Democrats (ULD) and lawyer Yi Se-chung, the committee planned to urge President Kim Tae-chung to make diplomatic efforts to have Kim released. They also decided to send a written petition with the joint signatures of members of the National Assembly to the US Government. In addition, the committee planned to stimulate public interest using personal computers and to launch a signature campaign together with social and human rights groups.

Yi said the committee would stage a rally calling for the release of Robert Kim in front of the US Embassy on 20 November 1998, during President Clinton's visit to the Republic of Korea (ROK). The rally will show the united stance of the South Korean people, albeit somewhat belatedly.

The committee planned to make various efforts to support Kim's family in their daily lives. Since June 2000, Yi Ung-chin, president of the Sonu marriage consultant office and member of the committee, sent 1 million won monthly to Kim's elderly mother (77) and his wife (53). Since her husband was put in prison, Robert Kim's wife has been working as a janitor in churches.

According to South Korean media reporting, Kim is proud of what he did and showed his patriotism

in prison. With regard to his espionage charges, Kim stated, "I am not a spy from the ROK, and likewise I am not a hero. While dealing with much intelligence, I decided to dedicate my life to improving the weakness of my country, a minority, because I knew what intelligence our country needed politically and technologically."<sup>1</sup>

In an appeal at the National Assembly on 14 November 1998, Representative Kim Sung-gon, brother of Robert Kim and a member of the National Congress for New Politics, urged the government to push for US acceptance of the re-sentencing demand when Kim talks with Clinton. Representative Kim, as an opposition leader, wrote a petition to the US Government calling for his brother's release. But as President of the National Assembly, he opposed an Assembly resolution on the issue, saying that the decision of the U.S. court must be respected.

He said, legally, his brother is guilty, but the sentence imposed was too severe because his brother was not exactly "spying." Kim is seeking his brother's release from a humanitarian standpoint. "What he engaged in was just delivery of classified documents, not spying," said Representative Kim. "He didn't get any money from our government and he's not employed by our government." Kim feels that the passage of secret information between countries with friendly relations with a wide gap in information acquisition capabilities is only natural. "The imbalance between the United States and South Korea in terms of intelligence will cause these kinds of things (leaking of secrets) to happen," said Representative Kim.

According to Kim, South Korea is virtually dependent on the United States for vital information on national security and North Korea. He argued that his brother's passage of "routine" documents was a great help to Korea, but no great loss for the United States. He added that his brother, while being a US citizen, is still a Korean at heart. It seems he was compelled by patriotism to hand the material over to the Colonel Baek Dong-il, the embassy attaché he met through his supervisor.

---

Representative Kim believes in his brother's innocence but did not have any illusions about his brother's situation. "The chance is not very high (that he will be released), but still I believe that if he's innocent, God will help him," he said.<sup>2</sup>

---

### Endnotes

<sup>1</sup> *Seoul Chungang Ilbo*, 2 November 1998.

<sup>2</sup> *Korean Herald*, 21 November 1998.

---

## Cuban Spies in Miami

In 1995, after obtaining FISA (Foreign Intelligence Surveillance Act) Court approval, the FBI obtained warrants to surreptitiously search apartments and monitor telephone communications by a group of Cubans who were Cuban intelligence operatives. The group, through its principal agents or illegal officers, communicated directly with the Cuban Government about its activities and received specific missions and taskings from the Cuban Government. The instructions were subsequently relayed to the other members of the spy ring as appropriate.

During the searches, the FBI uncovered and read the contents of the communications from and to the Cuban Government. This information was concealed in hidden files on computer floppy diskettes kept in the residences of three of the principal agents.

At Cuban Government direction, the Cuban spy ring collected and reported information on domestic, political, and humanitarian activity of anti-Castro organizations in the Miami-Dade county area; the operation of US military installations; and other US Government functions, including law enforcement activity. The spy ring also carried out tasks in the United States as directed by the Cuban Government, which included attempted penetration of US military installations, duplicitous participation in and manipulation of anti-Castro organizations, and attempted manipulation of US political institutions and government entities through disinformation and pretended cooperation. The spy ring received financial support from the Cuban Government to carry out its tasks.

An analysis of the communications used by the spy ring revealed that they spoke and addressed each other and their agents as representing the Cuban Government. They referenced decision-making "by the High Command," referred to individuals as "comrade," and used names and abbreviations associated with Cuban Government organizations. Communications between the

---

members also referenced the “Intelligence Information Department”; “C.P.” for *centro principal* or headquarters; “MINIT” for Ministry of Interior—which administers the Cuban Directorate of Intelligence or DI; and “DAAFAR,” a known abbreviation for the Cuban Air Force Command. They also used jargon and abbreviations such as “S.E.E.” (*Servicios Especiales Enemigos*) that refers to the FBI or CIA.

The spy ring members paid great attention to maintaining secrecy as to their identity and mission and took elaborate steps to evade detection. They called themselves “*La Red Avispa*”—The Wasp Network. They used code names, including “Giro,” “Castor,” “Lorient,” “Vicky,” “Franklyn,” “Allan,” “Manolo,” “Judith,” “Mario,” and “Julia.” They spy ring also used false identities, including assuming the name, date of birth, and social security number of a deceased person. The ring is viewed as the largest Cuban espionage operation uncovered in the United States in a decade.

On the basis of its investigation and surveillance, the FBI had identified three individuals as the spy ringleaders by 1998. The first was Gerardo Hernandez who had oversight for infiltrating his subagents into US anti-Castro groups in the Miami area. The second leader was Ramon Labanino whose primary task was to penetrate and report on US military installations and activity in the South Florida area, including the Southern Command and the Boca Chica Naval Air Base in Key West. The third leader was Fernando Gonzalez, who took over Labanino’s responsibilities, including meeting with subagents when Labanino was tasked with Cuban Government missions outside the Miami area.

Hernandez and Labanino received reports from, and provided payments to, their respective subagents and tasked their subagents based on instructions they received from Cuba. Ricardo Villareal and Remijio Luna also exercised managerial or supervisory functions over subagents at times, but both men left the United States for other operational assignments.

## Geraldo Hernandez

Geraldo Hernandez, who was known as Manuel Viramontes in Florida, used the code names “Giro” and “Giraldo.” He resided at 18100 Atlantic Boulevard, Apartment 305, North Miami Beach. He was arrested there in the early morning hours of 12 September 1998. He had been in the United States since 1992. The FBI bugged his apartment, picking up numerous conversations by Hernandez regarding his Cuban intelligence activities. The press identified him as a captain in Cuban intelligence.<sup>1</sup>

An FBI search of the apartment revealed a shortwave radio, computers, numerous 3.5 floppy diskettes, recording devices, and photographic equipment. Hidden on the floppy diskettes were literally thousands of pages of lengthy, detailed narrative reports between Hernandez and the Cuban Government, as well as between Hernandez and the various subagents in his network—“Castor,” “Franklyn,” “Lorient,” “Judith,” and “Manolo.”

Hernandez’s managerial and supervisory role within the spy ring is reflected in the computer records. They show that he communicated by telephone and met frequently with the other senior agents of the ring, including Labanino, Villareal, and Luna in various combinations and that countersurveillance measures were taken to avoid detection. When using the telephone, Hernandez used coded language and a false Puerto Rican accent.

He had a budget and routinely submitted a financial report detailing expenses for the “operation base” and “management of (the) agent network,” as well as cash payments to various subagents to Cuba. In one communication from Cuba, Hernandez was advised that “(b)ecause of the economic state of our country, headquarters has been obligated to reduce the budget of all the comrades there.”

Hernandez received detailed instructions from Cuba directing him to task individual subagents within the “theater of operations” with specific missions. He ensured that the missions or taskings were accomplished and reported the results to

---

Cuba. He also frequently offered his analysis and interpretation of events and information in his communications to Cuba.

Among the many communication topics between Hernandez and Cuba or his subagents were:

- The infiltration of the US Southern Command headquarters in Miami—according to Cuba, “one of the new prioritized objectives that we have in the Miami area.”
- The activities of Cuban exile groups in Miami and tactics to disrupt those groups by, among other things, “creat(ing) animosity” between specified groups and attempting to discredit certain individual leaders.
- The activities at the Boca Rica Naval Air Station as well as reports on an apparent military topic identified by Cuba that “continues to be of great importance to our comrades at DAAFAR.”
- The manipulation of the media, political institutions, and public opinion, including using anonymous or misidentified telephone calls and letters to media and political figures.
- Specific security precautions to be undertaken to avoid detection.

Other communications reference false identities used by Hernandez—he stole the identity of a dead man—as well as an “arrest alibi” and an escape plan to flee the United States. He had four escape routes—two via Mexico and one each in Canada and Nicaragua. He also had three different covers prepared, which included personal histories, details of schools and jobs, and names of relatives. He was explicitly directed that, under no circumstances, was he ever to “admit to being part of, or linked to, Cuban intelligence or any other Cuban government organization.”

A frequent topic of the messages within the files is the methods by which the spy ring communicates with each other and particularly their use of computers and floppy diskettes to deliver messages to each other.

Hernandez kept diskettes that appear specifically to have been delivered by, to, or exchanged with “Lorient,” “Castor,” “Franklyn,” “Oso,” and “Horacio.” Precise communications procedures and instructions as to how the computers and diskettes were to be used was often the subject of messages between the ring members. In one such communication, Hernandez references “codes to decrypt operational base diskettes.” He also directly communicated to other senior agents—“Horacio” and “Rami”—about specific problems he was having with his computer.

Among the documents discovered was a sabotage operation—codenamed Operation Picada—which targeted buildings and aircraft in Florida.

### **Ramon Labanino**

Ramon Labanino, who was known as Luis Medino, resided at 1776 Polk Street, Apartment 3G, Hollywood, Florida, and was arrested there in the early morning hours of 12 September 1998. He used the code name Allan. A press article identified him as a major in Cuban intelligence and said he was featured in an FBI videotape exchanging folders in a Wendy’s restroom with a Cuban UN diplomat.<sup>2</sup> Before his assignment to Miami in 1996, he operated in the Tampa, Florida, area from as early as 1992, reporting information to Cuba regarding operations at McDill Air Force Base.

Electronic surveillance of his apartment reflected numerous conversations up to September 1998 on activities on behalf of the Cuban Government. A search of the apartment revealed a computer, numerous floppy diskettes containing concealed messages dating back to 1992, a shortwave radio, and recording equipment.

Labanino was transferred specifically to lead the effort to infiltrate the US Southern Command. In communications received from Cuba in late 1996, he was advised: “Headquarters decided that the Southern Command, which will soon be stationed in Miami, should be assigned to a group of comrades under the direction of Allan. The Comrades are Mario and Julia, Gabriel and Lorient.”

---

The computer records seized from Labanino's apartment exposed codes, encryption procedures, and messages regarding the quality of radio message traffic received from "C.P." In his communications, Labanino referred to himself as an "illegal officer." The communications also contained at least one reference to his "comrades from C.P." He also discussed how he obtained a false driver's license in the name of "Luis Medina," his assumed identity.

Labanino had meetings with other principal agents, including "Giro," "Horacio," and "Rami," and used codewords when speaking with them. In addition, computer records showed that Labanino received reports from his subagents about the Southern Command and the Boca Chica Naval Air Station.

Prior to his arrest on 12 September 1998, he had planned to flee the United States on 17 September because his brief case had been stolen while he was in Los Angeles the previous week. The briefcase contained various espionage paraphernalia as well as school diplomas, a birth certificate, \$5,000 in cash, and a video shot in Cuba.<sup>3</sup>

### **Antonio Guerrero**

Antonio Guerrero, a.k.a. "Lorient," resided at 30161 Poinciana Road, Big Pine Key, Florida, where he was arrested in the early morning hours of 12 September 1998. His girlfriend, with whom he resided, owns the house. He was a civilian employee of the US Navy, Public Works, Boca Chica Naval Air Station, Key West. According to the news media, Guerrero grew up in Cuba and studied engineering in the Soviet Union. He worked menial jobs at Boca Chica Naval Air Station for more than five years.<sup>4</sup>

In the past, Guerrero reported to Hernandez who was tasked by Cuba "if . . . necessary, to go to Key West every two weeks to pick up information (Lorient has) obtained . . ." Surveillance of Guerrero identified him meeting and exchanging bags with Hernandez. Later, Labanino assumed handling of Guerrero. Guerrero reported his activities and received taskings from both Hernandez and Labanino via the exchange of floppy diskettes.

Guerrero was specifically tasked to report any "unusual exercises, maneuvers, and other activity related to combat readiness" at the air station. Guerrero did, in fact, report detailed information regarding the daily activities at the air station, including—through the use of beeper codes—the type of aircraft being deployed there; precise physical descriptions of the interior and exterior of a structure at the air station, which he suspected of being prepared for top secret activity, such as supposed "electronic warfare" aircraft believed to be deployed "to activities of exploration and tactics against our country"; and the addresses of certain military officers assigned to the base.

In a communication to Hernandez from Cuba, Guerrero was directed to "continue with the gathering of military information and at the same time . . . search for new relations and tightening of the ones he already possess [*sic*], with the aim of achieving broader penetration and gathering of information at the base."

### **Alejandro Alonso**

Alejandro Alonso, a.k.a. "Franklyn," resided at 19761 SW 79<sup>th</sup> Place, Miami and was arrested there in the early morning hours of 12 September 1998. Hernandez handled Alonso.

In the computer records obtained from Hernandez's apartment were expense reports relating to "Franklyn," his telephone and beeper numbers, as well as operational plans and meeting sites involving Alonso. On one occasion when Alonso failed to answer a page by Hernandez in a timely manner, he was admonished and told that he needed to maintain "a full combat readiness status . . ."

Records reflect repeated directions from the Cuban Government that Alonso participate in and report information on the Miami-based Cuban exile group known as *Movimiento Democracia* (to be "the eyes of the [Cuban Government] in the *Movimiento Democracia*"). A boat pilot, Alonso was directed to and participated in "flotillas" organized by *Movimiento Democracia* in demonstrations against the Cuban Government.

---

Alonso prepared a detailed account of his observation of a July 1996 flotilla to the waters near Cuba in which he participated as a pilot and gave it to Hernandez for forwarding to the Cuban Government. Alonso's report enumerated persons participating in the flotilla and provided navigational information concerning courses and locations pertinent to the flotilla. Alonso also reported on plans for a "flotilla" demonstration to occur near Cuban waters during the Pope's visit in January 1998 and a proposed concert by a popular singer on boats off the coast of Cuba. Reports by Alonso included patriotic slogans in support of the Cuban regime and critical remarks about the anti-Castro activities he pretended to support in his infiltration efforts.

### **Rene Gonzalez**

Rene Gonzalez, a.k.a. "Castor" and "Iselin," resided at 8000 SW 149<sup>th</sup> Avenue, Apartment A-403, Miami and was arrested there on 12 September 1998. Gonzalez is a US citizen, born 13 August 1956. Records of cash payments and other expenses relating to "Castor" are in computer diskettes found in Hernandez's apartment. Also found on the diskettes were frequent communications between Hernandez and Gonzalez using computer diskettes.

The computer diskette demonstrated that Gonzalez reported frequently to Hernandez on the activities of anti-Castro political and humanitarian groups and individuals in the Miami Cuban exile community and that Hernandez routinely forwarded this information to Cuba. The diskettes reflected both written and oral reports from Gonzalez to Hernandez using the code name "Iselin". Specifically, Gonzalez was tasked to report on Brothers to the Rescue (BTTR), *Movimiento Democracia, Militares y Profesionales Por La Democracia*, Commandos United for Liberation, PUND (National Democratic Unified Party), *Comision Nacional Cubano*, and the Cuban American Pilots Association.

Cuba told Hernandez that Gonzalez should become "more aggressive" and be "let loose" once his wife arrived in the United States from Cuba. His wife arrived in December 1996, after Gonzalez and Hernandez devised and implemented a cover story to enlist the assistance of unwitting Cuban-American US Congress persons in obtaining the supposed humanitarian release of the wife to the United States.

Gonzalez was generally tasked to report on information relating to the interests of the Cuban Government. He posed as an FBI informant, ostensibly supplying information about alleged drug smugglers as a means to obtain information regarding FBI activities, its agents, and progress of an investigation of interest to Cuba. In one communication to Hernandez, Cuban authorities detail that one purpose of this supposed cooperation with the FBI was to maintain a channel to use, "(i)f it is of interest to us in an emergency to spark an action by the North American government against these people (Cuban exile groups)." Gonzalez, in one report to Hernandez, reported that he "thwarted (his FBI handler) diplomatically, but I left the door open a crack. I think that I was very convincing . . . ."

### **Nilo Hernandez and Linda Hernandez**

Nilo Hernandez, a.k.a. "Manolo," and Linda Hernandez, a.k.a. "Judith," are a married couple that resided at 3012 SW 18<sup>th</sup> Street, Miami, where they were arrested 12 September 1998. (*Editor's comment: To avoid confusing Nilo Hernandez with Geraldo Hernandez, Nilo will be referred to by his code name "Manolo."*) They resided in the Miami area since at least 1992, having relocated from the New York area. Judith was born in the United States but spent her youth in Cuba, returning to that country before Castro's takeover. She returned to the United States in the mid-1980s.

On the basis of searches of the apartment of Hernandez and Labanino, in communications with Cuba, "Manolo" and "Judith" are often referred to collectively as the "Juniors," the "JRSS," or as "Agents." They were asked to jointly undertake

---

special assignments by Cuba. “Manolo” was a businessman and proprietor, operating export businesses involving the sale of computer peripheral devices and medical testing kits.

On 12 September 1998, “Manolo” admitted knowing Hernandez, claiming it was a social relationship. The FBI had photographed “Judith” meeting with Fernando Gonzalez, a.k.a. Ruben Campa, a.k.a. “Vicky.”

“Manolo” and “Judith,” while subagents reporting to Hernandez, were trusted and reliable agents. In one communication from Cuba, “Manolo” and “Judith” are said to have the military rank of “sublieutenant,” to have worked for the Cuban Government “for a number of years,” and to have maintained positions in the “reserves” and the “militia.”

In taskings from Cuba, the “Juniors” were given special assignments entrusting them with the identities of other Cuban operatives in the United States—a further indication of their elevated status within the spy ring. For example, the computer records reflect that the “Juniors” were to be assigned specifically to conduct countersurveillance or “dry clean(ing)” projects involving a subagent—“throughout the whole operation, you must use the JRSs to dry clean him during the routes from one (telephone) both to another and even at the places themselves”—and to undertake a long-term surveillance mission of two Cuban agents who were thought to be at risk of defection to US authorities.

Among other assignments, “Manolo” was asked to infiltrate CAMACOL, an exile group, and “Judith” was directed to do likewise with ALPHA 66. They were both asked to “conduct an investigation” of a local telecommunications company as well as to develop closer relations with a former employee of the US Navy ultimately to determine his reaction to assisting them by providing information. “Manolo” apparently also provided Hernandez with technical advice regarding computer and software issues.

Hernandez received instructions from Cuba for “Manolo” and “Judith” to carry out assignments involving the mailing of anonymous, misleading, and threatening letters to political figures in the United States, including communication in the guise of an anti-Castro figure threatening a US Senator for his political position. In outlining one such assignment, Cuba directed: “this task should be performed by Manolo as well as Judith and they should stand firm in their security measures, such as avoid leaving fingerprints in the correspondence, deposit them in different areas and mailboxes, stamp with appropriate postage; avoid being seen during the deposit, act in a normal fashion, make the subject of clothing, possible camouflages, etc. Both of these comrades have experience in this type of task and know how to act.”

A court-ordered search of their home revealed the following items, among others: photography development equipment and chemicals; three portable (walkie-talkie) two-way radios; shortwave radios (one portable) with assorted cables and connectors; numerous city and transmit maps for metropolitan US cities, including New York, Miami, Houston, and Las Vegas. Also found were: instructions for routes and meeting places; women’s wigs and hair attachments and temporary hair coloring spray and dyes; contact lenses in different colors; a bag containing a wig and various colored sunglasses; lists of telephone numbers and locations of public pay phones posted on the refrigerator; and a book entitled *Alpha 66 and its Historical Works* dedicated to Linda and signed with the name of Andres Nazario Sargen, the leader of the organization.

A court-ordered search of an automobile registered to “Manolo” revealed, among other things: two minirecorders in the console with adapters to run off the cigarette lighter, a microphone running from a recorder and clipped to the rear-view mirror, and a \$200 receipt for a miniature recorder from Spy World.

---

## **Fernando Gonzalez**

Fernando Gonzalez, a.k.a. Ruben Campa and a.k.a. “Vicky,” is a Cuban intelligence officer. (*Editor’s comment: To avoid confusion between Fernando Gonzalez and Rene Gonzalez, Fernando will be referred to by his alias Campa.*) In the autumn of 1997, Hernandez was temporarily recalled to Cuba. FBI monitoring revealed a conversation in October 1997 between Hernandez and Labanino discussing the arrival of an associate with Hernandez commenting that, by the end of the week, the famous “Vicky” should be there.

In the spring of 1998, Labanino was temporarily recalled to Cuba, and in the summer of 1998, Labanino was absent from Miami on other missions. Monitoring revealed conversations in April 1998 between Hernandez and Labanino discussing the associate who would substitute for Labanino. The anticipated associate was variously said to be Roberta, Camilo, and Vicky. In these conversations between the two men, Camilo was said to be the same as Vicky, the one with the limp, approximately 175 pounds, with a receding hairline and moustache. FBI physical observation of Campa showed him to have a receding hairline and mustache, although not the limp or estimated 175-pound weight.

On 3 July 1998, Campa telephoned Hernandez and said that he would arrive the next day. Between 5 July 1998 and early September 1998, electronic surveillance revealed frequent conversations, both on the telephone and in Hernandez’s apartment, in which Campa participated. The surveillance included conversations of Campa dictating his arrival 4 July, reading numbers aloud with Hernandez, and discussing with either Hernandez or Labanino the use of diskettes; equipment problems in which “if the recorder skips, it will skip either sending or receiving”; delays in communications; and when and whether they had recently spoken with “la nena” or “mami.”

Surveillance also revealed Campa discussing with Hernandez meetings or conversations with subagents and using the subagents’ codenames. In a July 1998

conversation, Campa and Hernandez discussed a recent conversation with a female associate of “Judith.” Campa was photographed meeting with “Judith.”

Campa and Hernandez also discussed encounters with “Manolo,” “Junior,” and the “Juniors.” In an August 1998 conversation, Hernandez asked Campa if he had a video, which Hernandez wanted to show to a named subagent. On another occasion, Campa was surveilled meeting at a shopping mall with another subagent, who delivered a laptop computer to Campa for needed adjustments.

In a July 1998 conversation, Campa and Hernandez discussed mutual acquaintances, including one who had been in Moscow and gotten in trouble, and the acquaintances’ movements through various elements of the Cuban intelligence establishment, such as “ISRI group,” referring to an intelligence school, and “M-2,” referring to a specific foreign country.

In September 1998, surveillance revealed a number of conversations in which Campa discussed with Hernandez or Labanino the apparent theft of Labanino’s laptop computer from a hotel room. In a 4 September conversation, Campa tells Labanino not to worry and that he would talk to the people at the “university.” Labanino replied that all of the “study materials” were also taken. In another telephone conversation, Campa told Hernandez that the problem is that they took the disks; the whole story is there.

## **Joseph Santos and Amarylis Silverio**

Joseph Santos, a.k.a. “Mario,” a naturalized US citizen, and Amarylis Silverio, a.k.a. “Julia,” a permanent resident alien, are a married couple who resided at 355 NW 72<sup>nd</sup> Avenue, Apartment 303, Miami, where they were arrested on 12 September 1998. Before arriving in Miami in mid-1996, they resided in New Jersey. Santos had left Cuba for the United States in 1993.

Santos said he was introduced to Hernandez in December 1998 and told that Hernandez would be his superior. He said he and his wife received orders from Hernandez to collect information on the Southern Command. Financial reports

---

maintained by Hernandez addressed the issue of payments to them. It appears from the records that \$4,800 was originally allocated to them “for operational expenses and financial help,” but that budget was later reduced.

According to the computer records, Santos and Silverio became subagents of Labanino and were sent to Miami specifically to assist him in the penetration of the Southern Command. “Mario and Julia should start working against it, for which instruction has already been given. That they shall both have as their fundamental assignment the penetration of said command.” It was directed that “both comrades should stay apprised and immediately informed, everything there [*sic*], public information or secret.”

Santos was an employee of a food producer in Miami, at a location close to Southern Command headquarters. It was reported that Santos was making “a preliminary study of (the operational situation) in the area where projects of the Southern Command are being carried out, and Julia (is making) another one on the mail (possibly courier) system and its various options . . .” Other computer disks reflect detailed reports, supported by numerous photographs, made by Santo and Silverio on the construction and geography of the Southern Command and its environs. One such report was entitled, “Observations Around the Southcom Installation.”

### **Five Ring Members Get Plea Bargains**

Five members of the Cuban spy ring accepted plea bargains from the prosecution in return for being a prosecution witness at the trial. The first to be sentenced was Alonso who received a seven-year prison sentence on 29 January 2000. He told investigators where to find a fake identity kit—which was hidden inside a leather notebook—a page of code concealed in a false bottom of a lamp, and a pad of water-soluble paper used for secret messages that was inside a stereo speaker.<sup>5</sup>

Santos agreed to become a witness for the US Government against the others, and in return, he and his wife pled guilty in October 1998 to a conspiracy charge of failing to register as a foreign agent. The judge accepted the plea bargain and on 2 February 2000 sentenced Santos to four years in jail.<sup>6</sup> His wife, Amarylis, received a three-and-a-half-year sentence.

Linda and Nilo Hernandez also agreed to cooperate.

### **Cuba Gets Christmas Gift From the United States**

On 23 December 1998, the United States informed the Cuban Mission to the United Nations that three of its diplomats could pack their bags and permanently go home. Expelled were Eduardo Martinez Borbonnet, first secretary; Roberto Azanza Paez, third secretary; and Gonzalo Fernandez Garay, an attache.

### **The Remaining Five Members Tried and Convicted**

With the plea agreements from five members in hand, the trial began on 7 December 2000 of the remaining five captured ring members. The five were charged with spying on US military installations in South Florida. Gerardo Hernandez was specifically charged with giving the Cuban Air Force the flight plans of unarmed Cuban exile planes that were shot down in 1996 by a Cuban MIG jet. Four members of Brothers to the Rescue were killed when their two planes were shot down. Four other members are still at large and presumed to be in Cuba. The trial took 100 days with breaks and postponements in between. More than 200 pages of coded messages were produced as evidence along with the testimony of the ring members.

In early June 2001, the trial finally went to a Federal jury. In the end, all five were convicted of spying for Havana. The federal jury found the defendants guilty of operating as foreign agents and conspiring to penetrate US military bases. The spy ring’s leader, Hernandez, was also convicted of involvement in the

---

Cuban shutdown in 1996 of two unarmed planes operated by Cuban exiles over the Florida Straits.

Hernandez, Labanino, and Guerrero were sentenced to life in prison. Fernando Gonzalez and Rene Gonzalez received lesser sentences. Defense attorneys declined to comment upon leaving Miami's Federal Courthouse. During the trial, the lawyers maintained their clients' primary mission was to monitor what they termed exile extremists who had violated Cuban airspace in the past and backed terrorist campaigns on the island.

### Endnotes

<sup>1</sup> *Sun-Sentinel*, 8 June 2001.

<sup>2</sup> *Ibid.*

<sup>3</sup> MacShan, Angus, "Alleged Cuban Spies had Escape Plan, Attorney Says," Reuters, 16 September 1998.

<sup>4</sup> *Sun Sentinel*, 18 June 2001.

<sup>5</sup> "Confessed Cuban Spy Received Seven Years," *Miami Herald*, 20 January 2000.

<sup>6</sup> *Miami Herald*, 11 January 2001.

## Brian P. Regan

The FBI arrested Brian P. Regan—a retired US Air Force cryptanalyst—as he cleared security at Dulles Airport on 23 August 2001. Regan was scheduled to board a Lufthansa flight for Zurich, Switzerland.



386160AI 8-02

BRIAN P. REGAN

Regan is 30 years old and lived in Bowie, Maryland. He is married and has two daughters and two sons. He served in the US Air Force from August 1980 until retiring in August 2000. His training in the Air Force included cryptanalysis. His responsibilities included the administration of an Intelink Web site—a classified US Government computer system accessible only by certain members of the US Intelligence Community.

Regan's last assignment with the Air Force was at the headquarters of the National Reconnaissance Office (NRO) in Chantilly, Virginia. During Regan's Air Force assignment at the NRO, he had access to classified US national defense information up to the Top Secret level and also had access to sensitive compartmented information (SCI). His access to SCI was terminated when he retired from the Air Force on 30 August 2000.

Regan was employed by TRW in Fairfax, Virginia, in October 2000. On 25 July 2001, his SCI access was reinstated allowing him to return to the NRO as a TRW contractor on 30 July 2001.

In the fall of 2000, a reliable source indicated that a number of US Government documents had been provided to the government of Country A, which the *Washington Post* identified as Libya. The large majority of these documents were classified and related to the US national defense. These documents were not authorized for release to Country A. The remaining documents were portions of classified documents—the portions are unclassified, but the documents in their entirety were not authorized for release to Country A.

Most of the classified documents provided to country A consisted of electronic images classified Secret that were taken from overhead platforms. Another document consisted of classified portions of a CIA intelligence report classified Secret and issued on a specific date. The particular copy of this report provided to Country A had been printed out eight days after the date the report was issued. Another of the documents consisted of two classified pages from a CIA newsletter that is classified Secret overall.

Among the other documents passed to country A were the following:

1. A Secret document relating to a foreign country's satellite capability.
2. The unclassified cover page of a defense intelligence reference document classified Top Secret.
3. One page from a document containing Top Secret information.
4. The unclassified table of contents for a particular intelligence manual classified Top Secret.

The documents also included two photographs—one classified Secret and the other classified Confidential.

Also, in the fall of 2000, a reliable source revealed that an agent had provided the government of Country A with separate information intended to accompany the documents described above. This accompanying information consisted of an introductory message,

---

in English, which contained instructions to prevent detection of the messages by the US Government along with separate encrypted messages.

The encrypted messages, which were decrypted by the US Government, set forth contact instructions, established bona fides, and offered to provide additional classified information. In particular, the encrypted message gave instructions to respond to a specified e-mail address on a free e-mail provider. A “Steven Jacobs,” of a specific address in Alexandria, Virginia, ostensibly established this e-mail address.

Records of the provider indicate that this e-mail address was established on 3 August 2000 and was accessed nine times between August 2000 and January 2001. Eight of the nine times this e-mail address was accessed were from public libraries located in Anne Arundel and Prince George’s Counties, Maryland. Regan’s residence is located one-half mile from a Prince George’s County library with public Internet access.

One of the Anne Arundel County libraries used to access this account is in Crofton, Maryland, approximately five miles from Regan’s residence. Physical surveillance of Regan during May through August 2001 indicated that Regan regularly utilized the public Internet access located in the Crofton library. The ninth access to the address occurred at the Tysons-Pimmit Library in Falls Church, Virginia, which is located along the route Regan used to commute between his residence and his NRO office.

The FBI searched the office formerly occupied by Regan at the NRO in April 2001. A copy of the intelligence manual referred to above (bullet number 4), bearing Regan’s name, was found on a shelf behind his former desk.

The FBI also searched the computer formerly assigned to Regan at the NRO in April 2001. FBI special agents analyzed the hard drive of this computer and found that someone using Regan’s password had surfed a large number of Intelink Uniform Resource Link (URL) addresses pertaining to countries A, B, and C.

One of these URL addresses is for one of the overhead images discussed above. Also on the hard drive of Regan’s computer were four URLs that corresponded to the URL addresses containing direct links to some of the other documents above. In addition, NRO server records indicate that Regan’s computer was used to gain access to three of the other compromised documents.

Intelink audit records indicate that the URL for the CIA intelligence report was accessed from the computer in Regan’s former office at 8:52 p.m. on the date the particular copy of the report had been printed out. NRO records indicate that Regan’s electronic entry badge was used to enter his office suite at 1:55 p.m. on that date. The FBI also established that there were common spelling errors in the messages and in documents typed on Regan’s NRO computer.

The CIA intelligence report, which related to a foreign country’s satellite capability, was composed expressly for and distributed at a course given at Colorado Springs, Colorado, that Regan attended 28 July through 8 August 1997. The course was given for cleared members of the US Intelligence Community—Regan was one of two NRO members who attended the course. Regan was the designated recipient at the NRO for all classified materials distributed at the course.

Separate NRO security records indicate that Regan’s passcode was used to set the alarm on the suite at 1:15 a.m. the following morning. Later that same day, Regan flew on a “space available” US Air Force flight from Norfolk, Virginia, to Iceland, and thereafter traveled to additional locations in other European countries.

The FBI has had Regan under surveillance since June 2001. On several occasions while under surveillance, FBI personnel observed Regan conducting what appeared to be surveillance detection runs; that is, conducting multiple U-turns, pulling over to the side of the road, and appearing to check to see whether he was under surveillance.

---

In early June 2001, FBI surveillance observed Regan log onto the Internet at a public library. When Regan departed, FBI personnel noted that he had failed to sign off the Internet, and they were able to observe which Internet sites Regan had visited. One of the sites that Regan had visited provided the address for a diplomatic office of Country C in Switzerland. Regan had also looked up a hotel in Zurich.

On 21 June 2001, Regan sent an e-mail from an account registered in his own name to an e-mail account in his wife's name. The e-mail attached one page of an alphanumeric encryption key that appears to be similar to the encryption technique described above.

On 26 June 2001, Regan traveled from Washington Dulles International Airport to Munich, Germany, on Lufthansa. Before Regan's flight departed, the FBI searched his checked suitcase, pursuant to a court order. Regan's suitcase contained glue and packing tape. Regan returned to Washington on 3 July 2001.

On 23 August 2001, at approximately 9:00 a.m., while Regan was occupied in a meeting at NRO, the FBI conducted a court-authorized search of Regan's Dodge Caravan. In that search, the FBI found a carry-on bag, which contained four pages of what appeared to be handwritten encrypted messages—one page of which appeared to be a typewritten encrypted message and another page that may be one page of a decryption key. The carry-on bag also contained handwritten addresses and phone numbers for diplomatic offices of Country D in Bern, Switzerland, and Vienna, Austria, and for a diplomatic office of Country C in Vienna. On the same day, the FBI also searched—pursuant to a court order—Regan's brown suitcase. In that suitcase were a bottle of Elmer's glue and a roll of tape. Also on 23 August, the FBI conducted surveillance of Regan's office at the NRO by closed circuit television, pursuant to a court order. He was observed looking at a Secret document on his computer terminal while taking notes in a small notebook that he took from, and returned to, his front pants pocket. A court-authorized search of Regan's computer confirmed that he had been logged onto Intelink accessing classified material.

Regan had reservations to Zurich, Switzerland, through Frankfurt, Germany, on Lufthansa, departing from Washington Dulles on 23 August 2001—which he reconfirmed on 11 August 2001—and returning on 30 August 2001. On 23 August 2001, Regan told a coworker that he was driving to Orlando, Florida, to take his family to Disney World, leaving on 27 August and returning 30 August. In addition, Regan wrote "Orlando, Florida" on a dry-erase board in his office suite, indicating to his colleagues where he would be for this time period. Regan did not report to his employer that he would be traveling outside the country, which he was required to do under NRO regulations concerning foreign travel by personnel having security clearances.

Later on 23 August, Regan drove to Dulles Airport, arriving at approximately 1:00 pm and checked a brown suitcase at the Lufthansa counter. This suitcase was secured by and is in the custody of the FBI. After Regan was bumped to a later flight, he departed Dulles Airport and returned to his NRO office. Regan drove back to Dulles Airport at approximately 5:30 p.m. and was stopped by the FBI in the airport terminal. Regan had the same carry-on bag containing the same documents that were found in the FBI search of his van earlier in the day.

Also in Regan's carry-on bag when the FBI stopped him was an NRO document marked For Official Use Only that listed classes available to members of the US Intelligence Community. This document indicated the security clearance required to attend each class. This document consisted of two pages—front and back—and FBI personnel had earlier observed Regan (via court-authorized closed-circuit television) create this document by cutting and taping together documents and then photocopying the taped-up document. When he was stopped, Regan was also carrying: approximately five blank business-sized envelopes, three rubber gloves, and four finger sleeves.

Regan's carry-on bag also contained a hand-held global positioning system (GPS), which can be used to locate a specific site for use as a deaddrop or as a signal site. He also had a spiral notebook

---

that appeared to be the notebook in which he was taking notes while looking at classified information on his computer terminal earlier in the day. In addition, hidden in Regan's shoe, was a piece of paper on which was written names and addresses in a European country.

FBI special agents at the airport confronted Regan at approximately 5:35 p.m. In response to a question, Regan denied knowledge of cryptology, coding, and decoding. However, when shown photographs of the cryptology-related alphanumeric tables—tables that had been in his carry-on bag—he stated, “This is my stuff.” Regan was arrested shortly thereafter.

Financial checks indicated that, in February 2001, Regan had consumer debts amounting to \$53,000.

## **Avery Dennison**

On 28 April 1999, FBI Director Louis J. Freeh announced that a guilty verdict was reached against a Taiwanese businessman, his daughter, and his company in connection with the theft of trade secrets from Avery Dennison, an Ohio manufacturing facility. Avery Dennison is a subsidiary of Avery Dennison Corporation—one of the nation's largest manufacturers of adhesive products—Pasadena, California. The company employs some 16,000 people worldwide.

Director Freeh stated, “This case marks one of the first convictions of foreign individuals under the Economic Espionage Act of 1996, which has gone to trial. It is also the first case in which a foreign company was charged and found guilty of an Economic Espionage violation.”

A Federal jury convicted Pin Yen Yang, Chairman of Four Pillars Enterprise Co, Ltd.; Yang Hwei Chang, a.k.a. Sally Yang, a company executive; and their company of two counts of violation of Title 18, USC, Section 1832 (a)(4), Attempted Theft of Trade Secrets, and Title 18, USC, Section 1832 (a)(5), Conspiracy.

Director Freeh pointed out that Avery Dennison Corporation provided extensive assistance to the FBI since the inception of this investigation. It was Avery Dennison who, through its own internal investigation, first uncovered evidence of economic espionage and then turned it over to the FBI. Freeh said, “This investigation and conviction clearly demonstrate the importance and value of law enforcement and industry working in partnership under the Economic Espionage Act to combat the theft of American trade secrets and jobs by foreign business interests. It is essential that this partnership continue to adequately combat a crime, which has such an impact on the economic well-being of this nation.”

FBI agents arrested Yang and his daughter, Hwei Chang, on 5 September 1997 at Hopkins International Airport in Cleveland, Ohio. They were traveling to New York to see the US Open

---

tennis championship. Both were charged with mail and wire fraud, conspiracy to steal trade secrets, money laundering, and receipt of stolen goods from the Avery Dennison. The pair was arrested after negotiating with an employee of Avery Dennison to obtain additional trade secrets. That employee was cooperating with the FBI in an undercover capacity. Since July 1989 the defendants had obtained, among other things, Avery Dennison trade secret information relating to formulations for self-adhesive products.

Federal prosecutors said an initial estimate regarding the search and development costs expended by Avery Dennison to develop the information obtained by the defendants could exceed between \$50 million and \$60 million.

Yang is the president of Four Pillars Enterprise Company, Ltd., of Taiwan, which manufactures and sells pressure-sensitive products mainly in Taiwan, Malaysia, Singapore, the United States, and the People's Republic of China. Avery Dennison is one of Four Pillars' chief competitors in the manufacture of adhesives. There was no indication that individuals from the People's Republic of China participated in the scheme.

Hwei Chen is a corporate officer of Four Pillars, which has more than 900 employees and annual revenues of more than \$150 million. She is believed to hold dual citizenship in the United States and Taiwan. Four Pillars previously employed Hwei Chen, who has a Ph.D. in analytical chemistry from New Mexico State University, as an Applied Research Group Leader.

A 21-count indictment was returned in US District Court in Cleveland on 1 October 1997. The indictment alleges that from July of 1989 through 1997 the defendants Yang, Hwei Chen, and Four Pillars Enterprise engaged in a scheme to defraud Avery of the intangible right to the honest service of Dr. Victor Lee and of its confidential and proprietary information and trade secrets.

Dr. Lee, a native of Taiwan, was employed by Avery in 1986 to do scientific research into

adhesives. At all times relevant to this case, Lee was an employee of Avery. In 1989, while Lee was making a presentation in Taiwan, Four Pillars vice-president C.K. Kao introduced him to Yang and Sally. Yang asked Lee to serve as a "consultant" to Four Pillars and offered him compensation of \$25,000 for a year of consultation. The parties agreed that they would keep the arrangement secret. Lee received a check, made out to his sister-in-law, from Four Pillars shortly thereafter.

After his return to the United States, Lee corresponded with Yang and Sally, describing the information he would provide them and indicating that some of the information Lee intended to provide the Yangs was confidential to Avery. On 8 August 1989, Lee sent two confidential Avery rheology<sup>1</sup> reports to the Yangs. The Yangs responded that the information was very helpful.

Lee continued to supply the Yangs with confidential information, including information that Four Pillars could use in making a new acrylic adhesive developed by Avery. The Yangs sent Lee samples of the adhesives they had created using information he had supplied; Lee tested the samples and offered comparisons with Avery's products derived from the same adhesive formula.

The FBI confronted Lee after learning of Lee's industrial espionage. Lee admitted his relationship with the Yangs and Four Pillars and provided the government with materials documenting his activities since 1989. Lee also agreed to cooperate with the government in a sting operation to arrest and prosecute the Yangs. A short time later, Yang told Lee that he would be in the United States during the summer of 1997. Lee volunteered that he had information on a new emulsion coating that he would provide Yang at that time and asked whether Yang might also be interested in information on Avery's operations in Asia. Yang was very interested.

On 4 September 1997, Lee met Yang and Sally in Lee's hotel room in Westlake, Ohio. Lee had consented to the FBI's videotaping this meeting. In the course of the meeting, Lee showed the Yangs

---

documents provided by the FBI, including an Avery patent application relating to a new adhesive product. The documents bore “confidential” stamps, and Lee emphasized to the Yangs that the information was the confidential property of Avery. Yang and Sally, at Yang’s direction, began to tear off the “confidential” stamps. The Yangs discussed with Lee the information Lee had previously provided to Four Pillars. The Yangs were arrested the next day.

Victor Lee, age 47, of Concord, Ohio, and a US citizen, pleaded guilty to a one-count information wire fraud charge. The charge alleges that Lee, who was employed by Avery in Concord, Ohio, as research engineer, disclosed confidential and proprietary information belonging to Avery to Four Pillars. The plea agreement between the government and Lee requires Lee to cooperate fully with the federal prosecutors in all matters relating to the ongoing investigation and prosecution of Four Pillars, P.Y. Yang, and H.C. Yang.

Prior to the conclusion of the trial, the District Court disposed of all but one of the fraud counts and all of the money laundering and receipt of stolen property counts. On 29 April 1999, the jury found the Defendants guilty of attempt and conspiracy to commit theft of a trade secret and acquitted them on the remaining fraud charge.

During the course of the proceedings, the Defendants made numerous motions, including pretrial motions to suppress evidence—a *Batson* challenge to the composition of the jury—and motions for mistrial on several grounds, all of which the District Court denied. In September 1999, the Defendants moved for a new trial and renewed their motions for mistrial. After an evidentiary hearing on these motions, the court denied each of them.

On 5 January 2000, the Defendants were sentenced. The court departed downward 14 levels in establishing the offense level for each of the Defendants; the court, however, departed upward in sentencing Four Pillars, imposing the statutory maximum fine of \$5 million. The

Defendants appealed the denial of their pretrial, trial, and post-trial motions and the District Court’s upward departure in imposing Four Pillars’ fine. The government appealed the District Court’s downward departure for each Defendant.

The principal issues in the appeal were the Defendants’ contention that under the circumstances of this case it was legally impossible for them to have committed the crimes of which they were convicted; Four Pillars’ contention that the District Court erred in departing upward in imposing sentence; and the government’s contention that the District Court erred in departing downward in setting the offense levels of the Defendants. In addition, the Defendants challenge the District Court’s denials of a motion to suppress video- and audiotape evidence, a *Batson* challenge, a motion to prohibit contact between prosecutors and witnesses, motions for mistrial because of alleged prosecutorial misconduct, and motions for new trial on grounds of newly discovered evidence. Finally, the Defendants claim that the District Court’s instruction on the meaning of “theft” was plainly erroneous and that the evidence did not support their convictions.

On appeal the Defendants argued that the District Court erred when it ruled that the government did not have to prove that what the Defendants sought to steal was an actual trade secret. The Defendants contended that the District Court’s reliance on *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998), which held that legal impossibility is no defense to attempt and conspiracy charges, was error because *Hsu* was incorrectly decided.

The court reviewed de novo, the District Court’s definition of the elements of the charged offense, the meaning attached to those elements, and the applicability of the defense of legal impossibility.<sup>2</sup> In *Hsu*, the Third Circuit was faced with a claim nearly identical to that raised by the Yangs, namely, that it was legally impossible for the defendants to be guilty of attempting to steal a trade secret and conspiring to steal a trade secret because that which they were accused of attempting and conspiring to steal was not, as it turned out, an

---

actual trade secret. This issue arose in the context of the defendants' claim that they were entitled to examine the trade secret documents in order to establish their defense of legal impossibility because, in their view, if those documents did not actually contain trade secrets, then the defendants could not be guilty of attempting to steal trade secrets. Hsu was one of several individuals led to believe that a scientist employed by Bristol-Myers Squibb, who was secretly cooperating with the FBI, was willing to sell corporate secrets.<sup>3</sup> A meeting was arranged at which Hsu met with the scientist and personally reviewed and discussed with him Bristol-Myers documents that were clearly marked "CONFIDENTIAL."<sup>4</sup> Immediately thereafter, the FBI arrested Hsu.<sup>5</sup>

Hsu was charged with attempt and conspiracy to steal a trade secret under 18 U.S.C. § 1832. He was not charged with the actual theft of a trade secret. Hsu claimed that, if that which he had sought to steal was not in fact a trade secret, it was legally impossible for him to be guilty of the offense of attempted theft of a trade secret. The Third Circuit rejected this defense. The court noted that virtually no other circuit continued to recognize the defense of legal impossibility and that even in the Third Circuit the defense had been severely limited. In particular, the court reviewed its holding in *United States v. Everett*, 700 F.2d 900 (3d Cir. 1983), that legal impossibility is not a defense to the charge of attempted distribution of a controlled substance under 21 U.S.C. § 846. Consistent with the analysis in *Everett*, the *Hsu* Court reviewed the legislative history of the EEA, particularly the comprehensive nature of the law's approach to the serious and growing economic threat presented by corporate espionage, and the fact that the law was drafted at a time when the defense of legal impossibility had been almost entirely abandoned.<sup>6</sup> The court also observed that, if it were to hold that legal impossibility is available as a defense to the charge of attempted theft of trade secrets, the anomalous result would be that the government would be compelled to use actual trade secrets in its sting operations and would be compelled to turn over those trade secrets to the persons charged with attempting to

steal them. Accordingly, the court concluded that legal impossibility is not a defense to a charge of attempted theft of trade secrets. Rather, the court held that a defendant is guilty of attempting to misappropriate trade secrets if, "acting with the kind of culpability otherwise required for commission of the crime, he . . . purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step in a course of conduct planned to culminate in his commission of the crime."<sup>7</sup> Because the defendant's guilt turns on the "circumstances as he believes them to be," the court held that the government was not required to prove that what the defendant sought to steal was in fact a trade secret, but only that the defendant believed it to be one.

Turning to the charge of conspiracy to steal trade secrets, the Third Circuit held that legal impossibility is not a defense to the charge of conspiracy to steal trade secrets. The court held that the basis of the conspiracy charge is the agreement to commit the unlawful act and not the unlawful act itself. Therefore, because the "illegality of the agreement does not depend upon the achievement of its ends," and because it is "irrelevant that the ends of the conspiracy were from the very inception of the agreement objectively unattainable,"<sup>8</sup> it is also irrelevant that it may have been objectively impossible for the conspirators to commit the substantive offense. Accordingly, the court held that, because legal impossibility is not a defense to the charge of conspiracy to steal trade secrets, the government was not required to prove that the information the defendants conspired to steal was in fact a trade secret.

The Appeals Court found the logic and reasoning of the Third Circuit persuasive. It did not feel it necessary to delve into the question of whether a defense of legal impossibility was recognized at all in the Sixth Circuit, and indeed, was aware of a handful of cases over the past decade in which the court had at least acknowledged the possibility that there is such a defense.<sup>9</sup> Importantly, the Appeals Court, like the Third Circuit, had definitively established in the context of the federal drug laws

---

that impossibility is not a defense. In *United States v. Reeves*, 794 F.2d 1101 (6th Cir. 1986), the court determined that, in light of the congressional desire to enforce federal drug laws as fully as possible, the fact that the defendant did not actually possess or gain possession of cocaine (but instead possessed an innocuous substance) was irrelevant to the defendant's conviction for attempt to distribute and possess cocaine because attempt requires that the government establish (1) an intent to engage in criminal activity, and (2) the commission of an overt act constituting a substantial step toward the commission of the substantive offense. Since neither element required the completion of the substantive offense, or that the material object of the defendant's desires (cocaine or a sham substance) actually be illegal, the court concluded that the defendant was guilty of attempted distribution and possession of cocaine.

Further, like the Third Circuit, the Appeals Court maintained that congressional purpose gives meaning to the extent and reach of a statute.<sup>10</sup> Here, the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets. To follow the Yangs' reasoning and rule as they ask would eviscerate the effectiveness of the act. The government would be severely limited in its ability to use the assistance of people willing to cooperate to catch and convict thieves of trade secrets. In effect, the Yangs' position would, as the Third Circuit pointed out, force "the government to disclose trade secrets to the very persons suspected of trying to steal them, thus gutting enforcement efforts under the EEA."

Under the Model Penal Code a defendant is guilty of attempting to commit a criminal offense when he "purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step . . . planned to culminate in his commission of the crime."<sup>11</sup> The Yangs believed that the information Lee was providing was trade secrets belonging to Avery. They attempted to steal that information. The fact that they actually did not receive a trade secret is irrelevant. Since the Yangs intended

to commit the crime and took a substantial step toward commission of the crime, they violated §1832(a)(4).<sup>12</sup>

The Yangs' conspiracy to steal the trade secrets in violation of §1832(a)(5) was completed when, with the intent to steal the trade secrets, they agreed to meet with Lee in the hotel room and when they took an overt act toward the completion of the crime, that is, when the Yangs went to the hotel room. The fact that the information they conspired to obtain was not what they believed it to be does not matter because the objective of the Yangs' agreement was to steal trade secrets, and they took an overt step toward achieving that objective. Conspiracy is nothing more than the parties to the conspiracy coming to a "mutual understanding to try to accomplish a common and unlawful plan,"<sup>13</sup> where at least one of the conspirators knowingly commits an overt act in pursuit of the conspiracy's objective.<sup>14</sup> It is the mutual understanding or agreement itself that is criminal, and whether the object of the scheme actually is, as the parties believe it to be, unlawful is irrelevant.

In sum, we adopt the reasoning employed by the Third Circuit. The Appeals Court affirmed the District Court's ruling that legal impossibility is not a defense to prosecution under §1832(a)(4) and (5).

The District Court made a number of sentencing departures, which are challenged on appeal. The District Court departed downward 14 levels in setting the adjusted offense level for each of the Defendants. The District Court then departed upward and imposed the statutory maximum fine of \$5 million on Four Pillars. The District Court later denied Four Pillars' motion for correction of sentence pursuant to Federal Rule of Criminal Procedure 35(c).

The Sentencing Guidelines, referencing 18 U.S.C. §3553(b), permit a downward departure when "there exists an aggravating or mitigating circumstance . . . not adequately taken into consideration by the Sentencing Commission."<sup>15</sup> The Appeals Court reviewed the District Court's departures from the recommended Sentencing

---

Guidelines for abuse of discretion.<sup>16</sup> That standard included a review to ensure that the factors upon which the District Court based its decision to depart are a permissible basis for departure—a question of law—since a District Court abuses its discretion when it makes an error of law. Whether the factors are a permissible basis for departure is a question of law. A reviewing court owes no deference to the sentencing court’s resolution of that question.

In deciding whether to depart, the sentencing court must determine whether the factors possibly warranting departure are forbidden, encouraged, or discouraged by the Sentencing Commission.<sup>17</sup> If the sentencing court determines that those factors are permissible and warrant a departure, the court must also provide a statement of reasons sufficiently detailed to permit review of the reasonableness of the departure in light of the grounds for it.<sup>18</sup>

The District Court issued a memorandum of opinion explaining the sentences. In that opinion, the court’s primary justification of its 14-point departure for each of the three Defendants was Avery’s participation in the prosecution, about which the court said, “In my experience no victim has played a more direct role than Avery in prosecuting a criminal case. . . . With Avery’s participation and the acquiescence of the Government, the criminal case has become a tool for Avery to seek vengeance instead of a pursuit of justice.” The District Court chastised Avery for “ha[ving] been an active participant in, and at times, even manipulated, the presentation of the Government’s case to enhance its ability to recoup its losses,” and for “attempting to control the sentence” through the calculation of the loss suffered as a result of the Defendants’ activities. Other than Avery providing to the government the same loss evaluation experts Avery intended to use in the parallel civil case against the Yangs, however, the court pointed to no instances or examples of Avery’s “manipulation” or “control” of the trial or the sentencing. Neither did the court provide any insight into how or why Avery’s participation lessened the Defendants’

culpability or the seriousness of their crime, or how Avery’s participation in the prosecution in any way constituted an “aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission.”<sup>19</sup>

It is unlikely that in determining the applicable sentences for theft of trade secrets—or for any other offense, for that matter—the Sentencing Commission took into consideration the participation of the victim in the prosecution of the crime. Certainly it is not mentioned as a factor whose consideration is forbidden in determining whether to depart from the applicable Sentencing Guidelines. The reason for the omission is, we suspect, that the victim’s participation in the prosecution is wholly irrelevant to either the defendant’s guilt or the nature or extent of his sentence. While the Appeals Court did not dispute the Defendants’ contention that *Coleman*, 188 F.3d at 358, prohibits the District Court from categorically excluding any nonprohibited factor from consideration in determining whether to make a downward departure, the court was also aware of the Supreme Court’s reminder that if a factor is unmentioned in the Guidelines, the court must, after considering the “structure and theory of both relevant individual guidelines and the Guidelines taken as a whole,” decide whether it is sufficient to take the case out of the Guideline’s heartland. The court must bear in mind the Commission’s expectation that departures based on grounds not mentioned in the Guidelines will be “highly infrequent.”<sup>20</sup>

Consideration of the structure and theory of the Guidelines as a whole requires that the court look at the factors to be considered in imposing sentence, as set forth in 18 U.S.C. § 3553(a). None of those factors in any way implicates a consideration of the participation by the victim of the crime in the prosecution of the offender. The structure and theory of the Guidelines as a whole includes the provisions of 28 U.S.C. § 994, which lays out the duties of the Sentencing Commission. Subsections 994 (c) and (d) each lists factors to be considered by the Commission in establishing

---

categories of offenses (§994(c)) and categories of defendants (§994(d)) for use in the Guidelines and policy statements. Those subsections mandate that the Commission consider whether the listed factors, among others, “have any relevance to the nature, extent, place of service, or other incidents . . . of an appropriate sentence, and shall take them into account only to the extent that they do have relevance.”<sup>21</sup> None of the factors in either subsection remotely implicated the participation of the victim in the prosecution of the offender. More importantly, however, those subsections made it clear that the factors the Commission was to consider must be relevant to the offense or the offender. The District Court provided no explanation of how the victim’s participation in the prosecution was in any way relevant to either the offense or the offenders.

The Supreme Court made it clear in *Koon* that the issue in sentencing departures is not “whether the particular factor is within the ‘heartland’ as a general proposition, but whether the particular factor is within the heartland given all the facts of the case.”<sup>22</sup> The District Court provided no basis upon which the Appeals Court could conclude that Avery’s participation in the prosecution of these Defendants takes this case outside the “heartland” of Guidelines cases. Accordingly, the Appeals Court concluded that the District Court abused its discretion in departing downward on this basis.

Contrary to the Defendants’ claims, the District Court did not base its 14-level downward departures on a series of “unquantifiable factors.” The District Court based its departures primarily on its perception that Avery had improperly participated in the prosecution of the offense and additionally on its concern that the government had overcharged the Defendants, that the Defendants’ conduct dating back to the inception of the scheme to steal Avery’s confidential and proprietary information was not illegal at the time, and that the government was using that conduct to enhance the Defendants’ sentences. The participation of Avery in the prosecution of the Defendants the Appeals Court had already concluded was not relevant to the sentencing of these Defendants and,

at least in this case, was not a permissible basis for downward departure. The District Court conceded in the sentencing order that the Defendants were not convicted on any of the counts that constituted overcharging. Finally, if the District Court believed that the conduct in the counts on which the Defendants were acquitted and the pre-EEA theft of Avery’s proprietary information was not relevant conduct and should not be considered in calculating the sentence, the court should have refused to consider it in arriving at the initial offense levels. Instead, however, the court expressly characterized that conduct as relevant conduct and included it in its calculations of loss as well as its determinations of more than minimal planning and role in the offense. If that conduct was relevant for purposes of determining the offense levels and amount of loss, the Appeals Court was at a loss to understand how its consideration can at the same time be the basis for a downward departure.

The Appeals Court held that the District Court abused its discretion in departing downward 14 levels for each of the Defendants. It noted as well that, although the Pre-sentence Reports contained mention of possible grounds for downward departure, the reports did not mention any of the grounds that the District Court in fact relied upon in making these very significant departures. The District Court’s failure to give notice of its intention to depart, we conclude, was error as well.<sup>23</sup>

The District Court, after departing downward 14 levels to an adjusted offense level of six for Four Pillars, for which the fine would have been \$5,000, *see* USSG § 8C2.4(d), or a maximum of \$16,000, *see* USSG § 8C2.6, fined Four Pillars the statutory maximum of \$5 million. Citing USSG § 5E1.2(d)(1) and 5E1.2 cmt. n.4, the court denied Four Pillars’ motion to correct its sentence. The court stated summarily that the Guideline maximum was insufficient to punish, deter, prevent a windfall, and reflect the seriousness of the crime.

The reasons offered by the District Court for the extent of the upward departure were insufficient. A District Court when departing must cite to

---

facts and circumstances that justify the extent of the departure.<sup>24</sup> The size of the departure should correspond to the grounds for the departure. Here, the District Court merely recited sections from the Guidelines and then concluded that \$5 million was the appropriate fine. Furthermore, the Appeals Court found it very difficult to reconcile the 14-level downward departure in offense level with the upward departure necessitated by that downward departure in order to arrive at a fine that, in the District Court's opinion, adequately accomplished the objectives of the Guidelines.

The Appeals Court then vacated the sentences of all Defendants and remanded this matter to the District Court for resentencing consistent with its opinion.

The Defendants, as alluded to above, assign as error a variety of the District Court's orders entered during the course of the proceedings, including (1) denial of a motion to suppress the video- and audiotapes of the hotel room meeting, (2) overruling of a *Batson* challenge to the composition of the jury, (3) denial of a motion to disallow contact between the prosecutors and witnesses, (4) denial of a motion for mistrial based on prosecutorial misconduct, and (5) denial of a motion for a new trial based on newly discovered evidence. The Defendants further claim that the District Court plainly erred in its instruction to the jury on the meaning of "theft" and that the evidence is insufficient to support their convictions. As explained below, the Appeals Court found no merit to these claims.

Sally Yang claimed that denial of her motion to suppress the tapes made by the FBI of the Yangs' meeting with Lee in his hotel room was error. She contended that the taping was unconstitutional because the FBI did not obtain a warrant; further, she claimed that because the tapes included some very brief periods when Lee was not in the room, the taping violated 18 U.S.C. § 2511(2)(c). The Appeals Court reviewed for clear error the District Court's factual determinations with regard to the motion to suppress; it reviewed de novo the court's legal determinations.<sup>25</sup>

The FBI was not required to obtain a warrant because it had Lee's consent to videotape the meeting.<sup>26</sup> The Yangs voluntarily came to the meeting with Lee and voluntarily talked with him in his hotel room. They had relinquished any "justifiable" expectation of privacy.<sup>27</sup> The Appeals Court found no merit to Sally's claim that the entirety of the tapes must be suppressed because they contain brief periods when Lee was not in the room. The record establishes that the technicians taping the meeting were expressly instructed to tape only while Lee was in the room. The technicians erred. The record establishes that the prosecutors learned of this error and, without reviewing the tape, arranged for the unauthorized time periods to be redacted. The un-redacted version was made available to the Defendants, but nothing from the unauthorized time period was ever utilized in the prosecution. Further, the District Court, after an evidentiary hearing, concluded that the government had not acted in bad faith. The Appeals Court found no error here.

The Yangs then claimed that the government exercised its peremptory challenges in a discriminatory manner in violation of the Equal Protection Clause.<sup>28</sup> Specifically, the Yangs contend that, because the government excluded three women—two of whom were black—in exercising three peremptory challenges, the government was excluding jurors on the basis of race and gender. The Appeals Court reviewed for clear error the factual findings upon which the District Court based its ruling.<sup>29</sup>

To establish a violation under *Batson*, the defendant must make a prima facie case by showing that the government removed jurors for a discriminatory reason.<sup>30</sup> The burden of production then shifts to the government to offer a race- (or gender-) neutral justification for its challenges.<sup>31</sup> At this stage, the government's explanation need not be "persuasive, or even plausible," but it must simply be one in which discriminatory intent is not inherent. The final step is for the trial court to determine whether the party challenging the peremptory strikes has proven purposeful discrimination. Here, the District Court may decide to disbelieve

---

an implausible or silly reason, but the burden is on the party challenging the strike to prove that it was motivated by discriminatory animus. The final makeup of the jury is relevant to a finding of discrimination.<sup>32</sup>

In response to the Defendants' *Batson* challenge, the government claimed that it struck one juror because of an apparent "attitude problem," a second because she was unemployed, and a third because she did not have the necessary background to be a juror. The District Court found those explanations to be legitimate and race and gender neutral. Following this ruling, the government did not use its remaining challenges, and the final jury consisted of nine women and five men. The Appeals Court concluded that the reasons offered by the government for its peremptory challenges do not violate equal protection. The Yangs showed neither purposeful discrimination nor that the government's reasons were illogical.

The Yangs argued that the District Court erred when it denied their motion to prevent the prosecutors from having contact with the witnesses whom the prosecution was allegedly coaching. The grant or denial of such a motion is within the sound discretion of the District Court.<sup>33</sup> The Yangs cross-examined the allegedly coached witnesses and commented on the alleged coaching to the jury in their closing arguments.<sup>34</sup> After reviewing the record, the Appeals Court found that the District Court did not abuse its discretion.

The Yangs further appealed the District Court's denial of their motion for a mistrial based on prosecutorial misconduct. For example, the Yangs contend that a prosecutor attempted to improperly influence a juror by making eye contact, smiling, and nodding at the juror as she entered the room. The Yangs also assert that this juror was particularly receptive and attentive during the prosecution's closing argument, while unreceptive to the Defendants' closing arguments. Another instance of misconduct was said to have occurred when a prosecutor was making head gestures while the defense was examining a witness. Finally, the Yangs alleged a number

of examples of the prosecutors' vouching for and improperly bolstering witnesses' credibility, improperly commenting on the lack of evidence, and wrongfully attacking the defense counsel's character.

The Appeals Court reviewed for abuse of discretion the District Court's denial of a motion for mistrial.<sup>35</sup> The District Court denied the Yangs' motions for mistrial and, after extensive discussion, found that "this whole thing . . . has been blown out of proportion." The court, therefore, refused to hold a *Remmer* hearing.<sup>36</sup> A *Remmer* hearing is not required unless the defendant can show that the unauthorized juror contact "created actual juror bias."<sup>37</sup> The Yangs' failed to offer evidence sufficient to support a finding that the alleged juror contact created the "obvious potential" to affect the verdict. The Appeals Court, therefore, rejected their claim that the government engaged in improper jury contact.

Prosecutor comments and actions must be taken in context.<sup>38</sup> Alleged misconduct that is not flagrant seldom constitutes reversible error.<sup>39</sup> Prosecutorial conduct is flagrant if it tends to mislead a jury or prejudice the defendant, if the comments were extensive and not isolated, and if the comments were deliberate. If conduct is not flagrant, this court will not reverse unless "(1) the proof against the defendant was not overwhelming, (2) opposing counsel objected to the conduct, and (3) the district court failed to give a curative instruction."

After thoroughly reviewing the records, the parties' briefs, and the District Court's rulings, the Appeals Court did not find that the District Court abused its discretion. On numerous occasions, the court reminded the jury, in response to the Yangs' objections, that they could consider only the evidence in the record and not what the attorneys said. Even assuming the comments objected to were improper; they were not flagrant and certainly did not prejudice the trial.<sup>40</sup> The comments at issue here were isolated and inadvertent common usages. Taken in context, with the overwhelming proof of the Yangs' guilt and the court's instruction, the comments do not require a new trial.

---

The Defendants also moved for a new trial based on newly discovered evidence of Lee's admission in a civil deposition that he had altered a document he had authenticated for the Yangs' criminal trial and that Lee suffered from mental health problems. After his arrest, Lee either began or continued to suffer from mental health problems. He visited a doctor and went to counseling for his difficulty in coping with the change in his circumstances caused by his arrest. As part of his cooperation with the FBI, Lee had given the government all of his files, including his correspondence with the Yangs. Some of the documents Lee gave to the FBI were incomplete because Lee had removed pages that tended to incriminate him. During trial, Lee authenticated some of the incomplete documents that he had given to the government. Later, Lee admitted in a related civil trial that he had excised portions of the letters. The Yangs, however, had copies of the original, unaltered letters from Lee because Lee had mailed those letters to the Yangs years earlier.

The District Court held a hearing on the Yangs' claims and concluded that, as to the changed documents, the evidence withheld by Lee was not newly discovered, since with due diligence the Yangs could have found the originals in their own records; it related to fraud counts on which the Defendants had been acquitted, but was not material to the trade secret counts and was not likely to produce an acquittal. The court further concluded that evidence of Lee's mental problems would not have changed the outcome of the trial, the mental health records contained no exculpatory information, and the absence of the evidence did not affect the fairness or integrity of the trial. The court ruled that the government had committed no *Brady* violation, and that a new trial was not warranted.

The Appeals Court reviewed for abuse of discretion the District Court's denial of a motion for new trial.<sup>41</sup> To prevail on appeal the Yangs had to show that "(1) the new evidence was discovered after the trial; (2) the evidence could not have been discovered earlier with due diligence; (3) the evidence is material and not merely cumulative or impeaching; and (4) the evidence would likely

produce acquittal."<sup>42</sup> We are satisfied that the District Court did not abuse its discretion. The District Court properly found that the evidence redacted by Lee from the letters, highlighting his criminal involvement, was not material to the Defendants' convictions. Further, the court rightly concluded, in light of the large volume of evidence of guilt and Lee's already largely discredited testimony, that the excised portions of the letters would simply be cumulative and further impeach Lee's credibility. With reference to Lee's medical history, since there was no "reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different," the District Court properly denied the Yangs' motion for a new trial.<sup>43</sup>

The Defendants raised no objection at the trial to the court's jury instruction on the meaning of "steal." The Appeals Court, therefore, reviewed this claim for plain error.<sup>44</sup> "An instruction is not plainly erroneous unless there was 'an egregious error, one that directly leads to a miscarriage of justice.'"<sup>45</sup> The Appeals Court found no plain error. Taken as a whole, the jury instructions fairly and adequately instructed the jury on the issues and the applicable law, and, therefore, if there was any error in this particular instruction, it did not lead to a miscarriage of justice.

Finally, the Defendants asserted that there was insufficient evidence to support their convictions. First, the Defendants claim that the proofs did not establish that the trade secret in question—the Avery patent application—was related to interstate commerce as is required by §1832(a). Second, Sally Yang contends that there was insufficient evidence that she knowingly joined a conspiracy or attempted to steal a trade secret.

The Appeals Court reviewed claims of insufficient evidence to determine whether, taking the evidence in the light most favorable to the prosecution, any reasonable trier of fact could have found the essential elements of the crime beyond a reasonable doubt.<sup>46</sup> The Appeals Court held that the interstate commerce nexus is sufficiently established in the record. Section 1832(a) requires that the trade

---

secret in question be “related to or included in a product that is produced for or placed in interstate or foreign commerce.” The patent application given by Lee to the Yangs involved an Avery product generating sales of \$75-100 million the previous year and related to products produced and sold in at least the United States and Canada. Taken as a whole, the testimony was sufficient to permit a reasonable juror to find that Avery is an international company with sales across the world of the product to which the patent application was attached.

Sally’s claim that she was not knowingly involved in a conspiracy cannot withstand the evidence in the record that she had, on numerous occasions, received confidential information from Lee and that she gave Lee payment for his services. A jury could permissibly conclude from this evidence, combined with her actions in the hotel room, that she was knowingly involved in the conspiracy to steal Avery’s trade secrets. The claims of insufficient evidence are without merit.

For all of the reasons set out above, the Appeals Court affirmed the judgments of conviction but vacated the sentence of each of the Defendants and remanded for resentencing.

## Endnotes

<sup>1</sup> Rheology is the study of adhesives.

<sup>2</sup> *United States vs. Alvarez* 266 F.3d 587,592 (6<sup>th</sup> Cir. 2001).

<sup>3</sup> *Id.* at 192.

<sup>4</sup> *Id.* at 192-93.

<sup>5</sup> *Id.* at 193.

<sup>6</sup> *Hsu*, 155 F.3d at 200-02.

<sup>7</sup> *Id.* (quoting Model Penal Code § 5.01[1][c] [1985]).

<sup>8</sup> *id.* at 203 (quoting *United States v. Jannotti*, 673 F.2d 578, 591 [3d Cir. 1982][en banc]).

<sup>9</sup> *See, e.g., United States v. Mise*, 240 F.3d 527, 530 (6<sup>th</sup> Cir. 2001); *United States v. Hixon*, 987 F.2d 1261, 1267 (6<sup>th</sup> Cir. 1993); *United States v. Peete*, 919 F.2d 1168, 1175-76 (6<sup>th</sup> Cir. 1990).

<sup>10</sup> *See United States v. Barry*, 888 F.2d 1092, 1096-97 (6<sup>th</sup> Cir. 1990) (internal quotations and citation omitted) (noting that the “cardinal canon of statutory construction” is that statutes “should be interpreted harmoniously with their dominant legislative purpose.”).

<sup>11</sup> Model Penal Code §5.01(1)(c). *See also Reeves*, 794 F.2d at 1104 (“In order to prove attempt, the government [must] . . . establish: (1) the intent to engage in criminal activity, and (2) the commission of one or more overt acts . . . towards the commission of the substantive offense.”).

<sup>12</sup> *United States v. Shelton*, 30 F.3d 702, 705 (6<sup>th</sup> Cir. 1994).

<sup>13</sup> *United States v. Pearce*, 912 F.2d 159, 161 (6<sup>th</sup> Cir. 1990) (citation and internal quotations omitted).

<sup>14</sup> *United States v. Hamilton*, 263 F.3d 645, 652 (6<sup>th</sup> Cir. 2001).

<sup>15</sup> US Sentencing Guidelines Manual (USSG) §5K2.0 (2001).

<sup>16</sup> *Koon v. United States*, 518 U.S. 81, 100 (1996).

<sup>17</sup> *United States v. Coleman*, 188 F.3d 354, 358 (6<sup>th</sup> Cir. 1999) (en banc).

<sup>18</sup> *United States v. Crouse*, 145 F.3d 786, 789 (6<sup>th</sup> Cir. 1998).

<sup>19</sup> USSG § 5K2.0.

<sup>20</sup> *Koon*, 518 U.S. at 96 (citations omitted).

<sup>21</sup> 28 U.S.C. § 994(c)-(d).

<sup>22</sup> *Koon*, 518 U.S. at 99-100.

<sup>23</sup> *See Burns v. United States*, 501 U.S. 129, 135, n. 4 (1991).

<sup>24</sup> *Crouse*, 145 F.3d at 789.

<sup>25</sup> *United States v. Guimond*, 116 F.3d 166, 169 (6<sup>th</sup> Cir. 1997).

<sup>26</sup> *United States v. White*, 401 U.S. 745 (1971).

<sup>27</sup> *Id.* at 751-52 (“If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that

same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case.”).

<sup>28</sup> *Batson v. Kentucky*, 476 U.S. 79 (1986).

<sup>29</sup> *United States v. Tucker*, 90 F.3d 1135, 1142 (6th Cir. 1996).

<sup>30</sup> *J.E.B. v. Alabama ex rel T.B.*, 511 U.S. 127 (1994); *Batson*, 476 U.S. at 96.

<sup>31</sup> *Purkett v. Elem*, 514 U.S. 765, 767 (1995) (per curium).

<sup>32</sup> *United States v. Sangineto-Miranda*, 859 F.2d 1501, 1520-21 (6th Cir. 1990).

<sup>33</sup> *United States v. DeJongh*, 937 F.2d 1, 3 (1st Cir. 1991) (citing *Geders v. United States*, 425 U.S. 80, 87 (1976)).

<sup>34</sup> See *United States v. Malik*, 800 F.2d 143, 149 (7th Cir. 1986) (finding that cross-examination and comment during closing is generally sufficient to dispel any ill effects caused by the coaching).

<sup>35</sup> *United States v. Rigsby*, 45 F.3d 120, 125 (6th Cir. 1995).

<sup>36</sup> See *Remmer v. United States*, 347 U.S. 227 (1954).

<sup>37</sup> *United States v. Frost*, 125 F.3d 346, 377 (6th Cir. 1997).

<sup>38</sup> *United States v. Bond*, 22 F.3d 662, 667-68 (6th Cir. 1994).

<sup>39</sup> *United States v. Brown*, 66 F.3d 124, 127-28 (6th Cir. 1995).

<sup>40</sup> See *Bond*, 22 F.3d at 667 (ruling that prosecutor statements do not merit reversal of the District Court unless they permeate the entire trial, making it unfair).

<sup>41</sup> *United States v. Davis*, 15 F.3d 526, 531 (6th Cir. 1994).

<sup>42</sup> *United States v. Seago*, 930 F.2d 482, 488 (6th Cir. 1991).

<sup>43</sup> *Kyles v. Whitley*, 514 U.S. 419, 433-34 (1995) (internal quotations and citation omitted).

<sup>44</sup> *United States v. King*, 169 F.3d 1035, 1040 (6th Cir. 1999).

<sup>45</sup> *Id.* (quoting *United States v. Busacca*, 863 F.2d 433, 435 [6th Cir. 1988]).

<sup>46</sup> *United States v. Prince*, 214 F.3d 740, 746 (6th Cir. 2000).

## Kelly Therese Warren

Kelly Therese Warren, a former US Army clerk, was sentenced on 12 February 1999 to 25 years in prison on charges that she spied for Hungary and Czechoslovakia while based in Germany during the Cold War. Warren, age 32, from Warner-Robbins, Georgia, was the fourth person convicted and sentenced in Florida for conspiring to commit espionage with Clyde Lee Conrad, a US Army sergeant who gave Hungarian and Czechoslovak agents secret US documents detailing US and NATO plans for the defense of Western Europe.

Warren served from 1984 to 1988 at the US Army's 8<sup>th</sup> Infantry Division headquarters in Bad Kreuznach in what was then West Germany, where she worked in the G-2 section as an administrative and clerical assistant, preparing classified documents for publication and distribution. The 8<sup>th</sup> Infantry Division maintained classified US Army, US Air Force, and NATO military documents concerning general defense plans for the allied defense of Europe; plans for the use of tactical nuclear weapons, chemical warfare documents, and coordinating documents used by NATO forces; and technical manuals.

Once Conrad recruited Warren into his ring, she began to either provide documents to him or allowed him to review the documents and files stored in cabinets and distribution boxes located in her office. She also allowed him to remove and photocopy classified information. For example, sometime between the summer 1987 and spring 1988, Warren provided Conrad with a document classified Secret, entitled "Appendix S (CONPLAN LIONHEART ANNEX I [Counterattack Contingency plans] to 8<sup>th</sup> Inf. Div. [MEC] PLAN 3300 9GDP)."

The espionage ring used the mail, telephone, and a one-way radio link to communicate with each other and with agents and officers of the Hungarian and Czech Intelligence Services. Besides Conrad coming to her office, Warren also passed documents to Conrad in a bowling alley and at a church in Bad Kreuznach.

---

After reviewing the documents passed by Warren, retired Gen. Clayton Otis, commander of the US Army in Europe from 1983 to 1988, said the papers contained “detailed information regarding how we planned to defend Europe. The compromise of this classified material was devastating to our national security.”<sup>1</sup>

Conrad was arrested in 1988 by German authorities and was tried on charges of high treason for espionage on behalf of the Hungarian and Czechoslovak intelligence services between 1976 and 1988. The Koblenz State Appellate Court convicted Conrad on 6 June 1990 and sentenced him to life in prison—the severest sentence handed down in the Federal Republic of Germany for espionage since World War II. Conrad died in a German prison on 8 January 1998.

Besides Warren, the others involved in the espionage ring were Roderick James Ramsey, Stephen Rondeau, and Jeffrey Gregory. They were also convicted in Florida in connection with the conspiracy. Ramsey, arrested in 1990 in Tampa, pleaded guilty and was sentenced in August 1992 to 36 years in prison. Rondeau and Gregory were sentenced in June 1994 to 18 years each.<sup>2</sup>

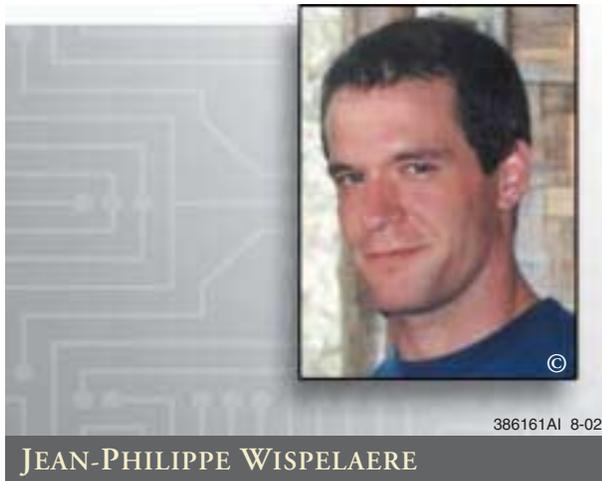
## Endnotes

<sup>1</sup> Reuters, “Former U.S. Army Clerk Gets 25 Years in Spy Case,” 19 February 1999.

<sup>2</sup> See Counterintelligence Reader, Volume Three, “Post-World War II to Closing the 20<sup>th</sup> Century,” for further information on Conrad (page 257), Gregory (page 409), Ramsey (page 412), and Rondeau (page 413).

## Jean-Philippe Wispelaere

Jean-Philippe Wispelaere, a former Australian Government intelligence official, was charged on 17 May 1999 with attempted espionage for selling US defense secrets to an undercover FBI agent posing as a foreign spy. Wispelaere, 28, worked for the Australian Defence Intelligence Organization from July 1998 to January 1999 and held security clearances for access to US top secret and sensitive compartmented information under US-Australian defense treaties.



According to various reports, Wispelaere walked into the embassy of a foreign country in January 1999 in Bangkok, Thailand, and offered to sell classified US documents to that country. The country involved notified US officials, and subsequently, an undercover FBI counterintelligence agent posing as a spy for the foreign country contacted Wispelaere.

Wispelaere corresponded via e-mail with the agent, and in April 1999 he met the man he believed to be a foreign spy in Bangkok and turned over 713 classified US documents in exchange for \$70,000. In early May, Wispelaere mailed more classified documents to the undercover FBI agent at a Virginia post office box in exchange for \$50,000.

On 15 May 1999, Wispelaere flew from London, England, to Dulles International Airport for what

he believed would be a meeting with the foreign spy, but instead, the FBI arrested him upon arrival. After his arrest, he said that he was in “very dire, dire financial need” for a knee operation and “a couple of other concerns, involving females, unfortunately,” the FBI said.

It took nearly two years for the case to come to trial because Wispelaere suffered from a serious spell of schizophrenia and was declared temporarily unable to stand trial in November 1999. Wispelaere said that he was abusing anabolic steroids and using opium and Valium during the period when he stole the documents and tried to sell them. He assured the judge that his five medications now have his illness (hearing voices) under control.

In March 2001, Wispelaere pleaded guilty to attempted espionage. The US Justice Department said that, under a plea agreement, Wispelaere would spend 15 years in jail. Under the plea agreement, Wispelaere is to fully cooperate in debriefings with Australian and US intelligence officials about his activities and to submit to a polygraph test. Prosecutors also agreed to allow Wispelaere to serve five years of his sentence in Australia. He could have faced life in prison.

According to the *Washington Post*, Nina Ginsberg, who represented him, criticized the Australian Government and security service for their lackadaisical attitude toward security vetting. She said the “woefully inadequate vetting process” involved just one face-to-face interview and two phone conversations with people who knew Wispelaere. The Australian spy service apparently did not realize that Wispelaere was using “enormous amounts of steroids” and never questioned him about his travels to more than 100 countries—including several considered terrorist states, Ginsberg said.

Wispelaere took—without any problems—hundreds of spy satellite photos and other classified documents in less than six months with the

---

Australian spy service. “The things he did, he did under the noses of everyone and no one seemed to notice,” Ginsberg said. “It’s almost comical the mistakes he made. It’s really hard to imagine someone doing a worse job of being a spy.”<sup>1</sup>

---

### Endnote

<sup>1</sup> Masters, Brooke, A., “Australian Sentenced for Spying Against the U.S.,” *The Washington Post*, 8 June 2001.

---

## Mariano Faget

At a February 2000 news conference, the FBI reported that, for more than a year, Mariano Faget, a chief in the Miami office of the US Immigration and Naturalization Service (INS), maintained contacts with Cuban operatives in the United States. According to FBI Special Agent Paul Mallett:



*Faget is known to have placed telephone calls to an extension of the Cuban Interests Section, which is a representative office of the Cuban Government in Washington. Faget met with representatives of the Cuban Interests Section. Faget has also had numerous contacts with a Cuban-born resident alien who is the chief executive officer of a business located in New York City, who, in turn, is known to have had several meetings with agents and representatives of the Cuban Government during the past year.*

The Cuban-born, 54-year-old Mariano Faget worked for INS for more than 30 years, rising from a low-level clerk to assume a supervisory position in the agency’s hectic Miami field office.

The FBI became suspicious of Faget after they spotted him meeting with a Cuban Interests Section official at a Miami airport bar more than a year ago. After months of surveillance, the FBI and INS launched a sting operation codenamed “False Blue.” On 11 February 2000, FBI Special Agent in Charge Hector Pesquera appeared at Faget’s

---

office requesting help in preparing immigration documents in a “highly sensitive” and top-secret Cuban defection.

Pesquera identified the defector as Luis Molina, one of two “known Cuban intelligence officers” seen meeting alone with Faget at two different Miami nightspots during 1999. “Let me tell you something,” Faget told Pesquera. “I don’t know if this is going to make a difference, I’ve met this guy before. . . . He was at the Interests Section in Cuba, in Washington, D.C., and I went to a dinner here one day and he happened to be there.” When Pesquera asked, “That’s it? That’s your only contact with him?” Faget responded, “That’s the only contact.”

INS agents told Mariano Faget that they needed him to process asylum papers for a Cuban intelligence officer who was supposedly about to defect. Special Agent Mallett described what allegedly happened next:

*Faget was told that the information he was being entrusted with was secret and very sensitive. The meeting was both videotaped and audiotaped. Approximately twelve minutes after that meeting, Faget placed a telephone call from his office to the offices of the New York businessman. Faget identified the full name of the individual for whom he had been asked to prepare the political asylum document.*

Faget’s call was to his longtime friend and America Cuba Incorporated (ACI) partner, Pedro Font. At the time, Faget was secretary and vice president for ACI, which was formed in 1993 to act as a conduit for American retailers looking to enter Cuba after the fall of Fidel Castro’s communist regime. Font was set to meet on 11 February 2000 with Jose Imperatori, another Cuban Interests Section official they both knew.

At his trial, Faget argued that the lie to Pesquera was immaterial, that he voluntarily disclosed the relationship, and that ACI is a Florida corporation that had done no business at all in the United States—let alone in a foreign country. Faget

claimed his motive was to warn Font to be wary, not so Font could pass along the secret. Prosecutors maintained Faget intended the secret to curry favor with Font and, in turn, Cuban officials.

The FBI also said Faget was guilty of making false statements to federal officials. Faget admitted at his trial that he lied to the FBI and that he disclosed classified information without permission—two factors that formed the foundation for the government’s case. Faget said he did it to protect a lifelong friend and business partner. Prosecutors said he did it for greed and to court favor with Cuban officials he viewed as prospective business contacts. According to prosecutors, that was the first in a long succession of lies told by Faget. Another alleged lie came in May 1998 when he denied any “foreign business contacts” on his reapplication for a security clearance.

The US District Attorney for Miami, Tom Scott, said other suspects could also be charged. “Are we going to charge Cuban agents in Washington? It’s an ongoing investigation, but I think you can anticipate further action and announcements.”

Two weeks later, Faget spoke with a Miami television station from the detention center where he had been held since 17 February. The Cuban-born suspect, who came to the United States as a young man, said he never passed sensitive information to any foreign agents. “I am a moral person. I love this country and I would never do anything to hurt it. And what would I have to gain by giving information? There’s nothing to gain there. I’ve never considered doing anything like that.”

Faget acknowledged he contacted the New York businessman, but insists his intention was not to betray the supposed Cuban defector. He also admits that, in late 1998, he met with Cuban diplomat Imperatori, whom the United States has also expelled from the country for spying. Faget said he was never asked, nor did he volunteer, any US secrets. “That meeting was the first time I met him. We discussed, in general, the future of Cuba. My job never entered into (had any part of) any

---

conversations with him.” Faget was denied bail while awaiting trial and said he is eager to have his day in court.

On 24 February, Miami Federal Magistrate Judge Barry Garber denied bail for Faget saying there was a risk he might flee if released from jail. In court, Faget expressed a desire to clear his name, stating he has never sympathized with communism.

During the trial, prosecutors used the surveillance tapes to prove their case, while Faget’s lawyer challenged the charge—required for a conviction—that Faget intended to harm the United States or help Cuba. “Mariano Faget was a government employee willing to betray the trust of people he was sworn to serve,” Assistant U.S. Attorney Curtis Miner told the jurors. “He disclosed classified information for no better purpose than his own personal reasons, his own personal gain.” Faget’s defense attorney, Edward O’Donnell, called Faget “an honest government servant who made a mistake.” Faget was close to retirement after 34 years with the INS.

It was also learned during the trial that the FBI tried to recruit Faget as an agent working for the United States before arresting him. The FBI wanted to find out all they could about his links to Cuban intelligence, said FBI agent James Laffin. “We did not achieve either objective, because Mr. Faget was manipulative and deceitful,” said Laffin. “It was clear there was no way we could use him” in the future as a counterintelligence agent. “We told him at the end that that was his final chance to tell the truth. We had no choice but to put him under arrest.”

On 30 May 2000, a jury found Faget guilty on four counts of violating the Espionage Act by disclosing official secrets and lying about his contact with Cuban diplomats. He had been in prison without bail since his arrest and remained in custody after the verdict. Federal sentencing guidelines call for a sentence of 62 to 75 months.

The case further strained the thorny relations between Washington and Havana when, three days

after Faget’s arrest, the State Department ordered the expulsion of Washington-based Cuban consular official Jose Imperatori, one of two Cuban officials Faget was known to have met. Imperatori had accompanied Elian Gonzalez’s grandmothers from Washington to Miami on the first of their two visits here, but prosecutors made no links between Faget and the case of the Cuban boy. Cuba has ordered the diplomat to remain in the United States and challenge accusations of espionage.

The US State Department said Imperatori was expelled from the United States for not voluntarily leaving the country by the deadline of midday 26 February 2000. The 46-year-old diplomat, who had worked at the Cuban Interests Section in Washington, was not handcuffed and looked impassive as federal agents took him to Reagan National Airport outside Washington for a government flight to Montreal. A Canadian commercial flight was to take him back to Cuba.

At a 26 February 2000 news conference, Imperatori strongly denied links to Faget. At a separate news conference the same day, Cuban Interests Section spokesman Fernando Ramirez acknowledged his colleague had had contacts with Faget but insisted they were not criminal in nature. “We want to be very clear that he is completely innocent, that he didn’t do anything wrong, that the Cuban Interests Section in Washington does not do any kind of intelligence or espionage activities.”

Ramirez insisted there was a link between Faget’s arrest and the custody battle over six-year-old Gonzalez, a shipwreck victim saved off the US coast and that Havana demanded he be returned to his father in Cuba. Court papers identified Imperatori as the immigration official’s Washington contact.

Imperatori earlier had resigned his post as Consular Affairs Officer, leaving him without diplomatic immunity and insisting he is a victim of what he called a major slander. His refusal to leave voluntarily came as no surprise as Cuban officials signaled they had no intention of willingly abiding by the deportation order.

---

## Echelon

In a statement issued on 22 February 2000 by Cuba's ruling Communist party, the Castro government accused the United States of operating a large spying operation out of its seven-story Interests Section building on the Havana waterfront. The Cuban statement alleged that the building is full of sophisticated listening devices and electronic spying equipment. It also said that most of the people working there are CIA agents, who the Castro government claims work closely with so-called "mercenaries"—a reference to political dissidents and independent journalists within Cuba. There are so many spies in the US Interests Section, according to the communique, that if Cuba asked them all to leave—in the words of the statement—"there would be few or none left."

As for the US allegations against Imperatori, the statement challenged the United States to present the charges in court. The Cuban Government denied ever having used its Interests Section in Washington for espionage. The Castro government claimed the US allegations against Imperatori were designed to undermine the case for returning Gonzalez to his father in Cuba. The statement noted the timing of the accusation, coming just before the federal hearing on the case in Miami.

On 29 June 2001, US District Judge Alan Gold sentenced Faget to five years in prison for disclosing classified information to Cuba. Because US Attorney Guy Lewis said that Faget's disclosure caused "no overt harm to the national security," Judge Gold rejected guidelines calling for a term of 10 years.

The allegations of U.S. industrial espionage have provoked calls for the European Union to set up a committee of inquiry to look into the issue. The demand emerged as a European Union parliamentary committee studied a report by British Journalist Duncan Campbell. Mr. Campbell's report claims the United States, Britain and other key allies have, since the cold war, maintained a sophisticated electronic spy network called "Echelon."

European-Union member Britain helps operate the system, along with listening posts in Canada, Australia, and New Zealand. A British news report says the system led by the US National Security Agency has engaged in industrial espionage against European businesses.

Campbell's report says the network of spy satellites and electronic eavesdropping equipment can monitor phone conversations, faxes, and electronic mail. The report calls the surveillance network a threat to civil liberties and alleges it has been used to collect economically sensitive information that provides a commercial advantage to U-S companies.

Green Party members of the European Parliament demanded a committee of inquiry look into the charges based on Campbell's and other reports on Echelon's monitoring capabilities. They also say information gathered by Echelon helped the United States beat the European Airbus Consortium in selling aircraft to Saudi Arabia in 1994.

According to the British report, the Echelon program monitors worldwide communications with a network of satellite and ground based listening posts. The network was established during the cold war for military surveillance. French officials have alleged that Britain has also benefited commercially from information gathered by the network, allegations British Prime Minister Tony Blair has denied.<sup>1</sup>

---

The European Commission has a problem in investigating these damages. Commission spokesman Jonathan Faull explains that no European business has complained about damages from spying. “Nobody has come forward, and we should certainly be interested in talking to people who want to come forward, but nobody has done so.”

Another problem is that Britain is a member of the European Union. In a letter released by the Commission, the British government cites 1985 legislation that authorizes interception of communications in cases involving safeguarding the nation’s economic well being.

The Commission also has a letter from the State Department stating that the US intelligence community is not engaged in industrial espionage. The letter also says the US Government does not collect information for the benefit of private firms.

Likewise, State Department spokesman James Rubin refused to comment on the existence of the system, but he denied US intelligence agencies are engaged in industrial espionage. “US intelligence agencies are not tasked to engage in industrial espionage, or obtain trade secrets for the benefit of any US company or companies.”

The European Commission has been aggravated by interviews given by the former director of the CIA James Woolsey. He justified industrial espionage by the United States on the basis of the use of bribery by European companies.

Commission spokesman Faull expresses outrage about the justification, while not denying bribery is sometimes used to make a sale. “I do not deny that cases of bribery arise in all sorts of countries by the way, not only in Europe, from time to time, I am not that naive. What I am saying is outrageous is the suggestion is that espionage could be justified in order to redress some apparent imbalance caused by the fact that European companies are considered to bribe more than American companies.”

In the European Parliament’s debate, Portuguese Interior Minister Fernando Gomes says the EU

justice ministers would discuss the Echelon system in their meeting at the end of April. He said the European Union couldn’t accept the existence of such a system that violates data privacy. But he also said there is no evidence that companies ever benefited from communications interception or have been damaged by it.<sup>2</sup>

The following is an edited version of the European Parliament’s report on ECHELON.

On 5 July 2000 the European Parliament decided to create a temporary committee to investigate the ECHELON system. This step was prompted by the debate on the study commissioned by STOA<sup>3</sup> [Scientific and Technical Options Assessment Program, Office of the European Parliament] concerning the so-called ECHELON system,<sup>4</sup> which the author, Duncan Campbell, had presented at a hearing of the Committee on Citizens Freedoms and Rights, Justice and Home Affairs on the subject, the European Union and data protection.

The first STOA report of 1997, which STOA commissioned from the Omega Foundation for the European Parliament in 1997, on *An Appraisal of Technologies of Political Control* described ECHELON in a chapter concerning national and international communications interception networks. The author claimed that all e-mail, the US National Security Agency routinely intercepted telephone and fax communications in Europe.<sup>5</sup> As a result of this report, the alleged existence of a comprehensive global interception system called ECHELON was brought to the attention of people throughout Europe.

In 1999, in order to find out more about this subject, STOA commissioned a five-part study of the development of surveillance technology and risk of abuse of economic information. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particularly the mode of operation of ECHELON.<sup>6</sup>

Concern was aroused in particular by the assertion in the report that ECHELON had moved away

---

from its original purpose of defense against the Eastern Bloc and was currently being used for purposes of industrial espionage. Examples of alleged industrial espionage were given in support of the claim: in particular, it was stated that Airbus and Thomson CFS had been damaged as a result. Campbell bases his claims on reports in the American press.<sup>7</sup> As a result of the STOA study, ECHELON was debated in the parliaments of virtually all the Member States; in France and Belgium, reports were even drafted on it.

At the same time as it decided to set up a temporary committee, the European Parliament drew up its mandate.<sup>8</sup> It reads as follows:

- to verify the existence of the communications interception system known as ECHELON, whose operation is described in the STOA report published under the title Development of surveillance technology and risks of abuse of economic information;
- to assess the compatibility of such a system with Community law, in particular Article 286 of the EC Treaty and Directives 95/46/EC and 97/66/EC, and with Article 6(2) of the EU Treaty, in the light of the following questions:
  - Are the rights of European citizens protected against activities of secret services?
  - Is encryption an adequate and sufficient protection to guarantee citizens privacy or should additional measures be taken and if so what kind of measures?
  - How can the EU institutions be made better aware of the risks posed by these activities and what measures can be taken?
  - To ascertain whether European industry is put at risk by the global interception of communications;
  - Possibly, to make proposals for political and legislative initiatives.

The European Parliament decided to set up a temporary committee because a committee of inquiry can be set up only to investigate violations of Community law under the EC Treaty (Article 193 TEC [Truth About Europe Campaign]), and

such committees can accordingly only consider matters governed by it. Matters falling under Titles V (Common Foreign and Security Policy) and VI (Police and Judicial Cooperation in Criminal Matters) of the Treaty on European Union are excluded. Moreover, under the inter-institutional decision<sup>9</sup> the special powers of a committee of inquiry to call people to appear and to inspect documents apply only if grounds of secrecy or public or national security do not dictate otherwise, which would certainly make it impossible to summon secret services to appear. Furthermore, a committee of inquiry cannot extend its work to third countries, because by definition the latter cannot violate EU law. Thus, setting up a committee of inquiry would only have restricted the scope of any investigations opening up any additional rights, for which reason the idea was rejected by a majority of Members of the European Parliament.

With a view to carrying out its mandate in full, the committee decided to proceed in the following way. A program of proposed work adopted by the committee listed the following relevant topics: certain knowledge about ECHELON; debate by national parliaments and governments; intelligence services and their operations; communications systems and the scope for intercepting them; encryption; industrial espionage; aims of espionage and protective measures; legal context and protection of privacy; and implications for the EU's external relations.

The topics were considered consecutively at the individual meetings, the order of consideration being based on practical grounds and thus not implying anything about the value assigned to the individual topics. At the meetings, in accordance with the requirements of the topic concerned, representatives of national administrations (particularly secret services) and parliaments in their capacity as bodies responsible for monitoring secret services were invited to attend. Also attending were legal experts and experts in the fields of communications and interception technology, business security and encryption technology with both academic and practical

---

backgrounds. Journalists who had investigated this field were also heard.

The meetings were generally held in public, although some sessions were also held behind closed doors where this was felt to be advisable in the interests of obtaining information. In addition, the chairman of the committee and the reporter visited London and Paris together to meet people who for a wide variety of different reasons were unable to attend meetings of the committee but whose involvement in the committee's work nonetheless seemed advisable. For the same reasons, the committee's bureau, the coordinators and the reporter traveled to the USA. The reporter also held many one-to-one talks, in some cases in confidence.

The system known, as ECHELON is an interception system, which differs from other intelligence systems in that it possesses two features, which make it quite unusual. The first such feature attributed to it is the capacity to carry out quasi-total surveillance. Satellite receiver stations and spy satellites in particular are alleged to give it the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents.

The second unusual feature of ECHELON is that the system operates worldwide on the basis of cooperation proportionate to their capabilities among several states (the UK, the USA, Canada, Australia and New Zealand), giving it an added value in comparison to national systems. The states participating in ECHELON can place their interception systems at each other's disposal, share the cost and make joint use of the resulting information.

This type of international cooperation is essential in particular for the worldwide interception of satellite communications, since only in this way is it possible to ensure in international communications that both sides of a dialogue can be intercepted. It is clear that, in view of its size, a satellite receiver station cannot be established on the territory of a state without that state's knowledge. Mutual agreement and proportionate cooperation among several states in different parts of the world is essential.

Possible threats to privacy and to businesses posed by a system of the ECHELON type arise not only from the fact that is a particularly powerful monitoring system, but also that it operates in a largely legislation-free area. Systems for the interception of international communications are not usually targeted at residents of the home country. The person whose messages were intercepted would have no domestic legal protection, not being resident in the country concerned. Such a person would be completely at the mercy of the system.

Parliamentary supervision would also be inadequate in this area, since the voters, who assume that interception only affects people abroad, would not be particularly interested in it, and elected representatives chiefly follow the interests of their voters. That being so, it is hardly surprising that the hearings held in the US Congress concerning the activities of the NSA were confined to the question of whether US citizens were affected by it, with no real concern expressed regarding the existence of such a system in itself. It thus seems all the more important to investigate this issue at European level.

### **The Operations of Foreign Intelligence Services**

In addition to police forces, most governments run intelligence services to protect their country's security. As their operations are generally secret, they are also referred to as secret services. These services have the following tasks: gathering information to avert dangers to state security; counter-espionage in general; averting possible dangers to the armed forces; and gathering information about situations abroad.

Governments have a need for systematic collection and evaluation of information about certain situations in other states. This serves as a basis for decisions concerning the armed forces, foreign policy and so on. They therefore maintain foreign intelligence services, part of whose task is to systematically assess information available from public sources. The reporter has been informed

---

that on average this accounts for at least 80% of the work of the intelligence services.<sup>10</sup> However, particularly significant information in the fields concerned is kept secret from governments or businesses and is therefore not publicly accessible. Anyone who nonetheless wishes to obtain it has to steal it. Espionage is simply the organized theft of information.

The classic targets of espionage are military secrets, other government secrets or information concerning the stability of or dangers to governments. These may for example comprise new weapons systems, military strategies or information about the stationing of troops. No less important is information about forthcoming decisions in the fields of foreign policy, monetary decisions or inside information about tensions within a government. In addition there is also interest in economically significant information. This may include not only information about sectors of the economy but also details of new technologies or foreign transactions.

Espionage involves gaining access to information, which the holder would rather protect from being accessed by outsiders. This means that the protection needs to be overcome and penetrated. This is the case with both political and industrial espionage. Thus the same problems arise with espionage in both fields, and the same techniques are accordingly used in both of them. Logically speaking there is no difference, only the level of protection is generally lower in the economic sphere, which sometimes makes it easier to carry out industrial espionage. In particular, businessmen tend to be less aware of risks when using interceptible communication media than does the state when employing them in fields where security is a concern.

Protection of secret information is always organized in the same way:

- Only a small number of people, who have been vetted, have access to secret information;
- There are established rules for dealing with such information;

- Normally the information does not leave the protected area, and if it does so, it leaves only in a secure manner or encrypted form. The prime method of carrying out organized espionage is therefore by gaining access to the desired information directly through people (human intelligence). These may be:

1. Plants (agents) acting on behalf of the service/business engaging in espionage;
2. People recruited from the target area.

Recruits generally work for an outside service or business for the following reasons:

- Sexual seduction;
- Bribery in cash or in kind;
- Blackmail;
- Ideological grounds;
- Attachment of special significance or honor to a given action (playing on dissatisfaction or feelings of inferiority).

A borderline case is unintentional cooperation by means of which information is creamed off. This involves persuading employees of authorities or businesses to disclose information in casual conversation, for example by exploiting their vanity, under apparently harmless circumstances (through informal contact at conferences or trade fairs or in hotel bars).

The use of people has the advantage of affording direct access to the desired information. However, there are also disadvantages:

- Counter-espionage always concentrates on people or controlling agents;
- Where an organization's staff are recruited, the weaknesses which laid them open to recruitment may rebound on the recruiting body;
- People always make mistakes, which means that sooner or later they will be detected through counterespionage operations.

Where possible, therefore, organizations try to replace the use of agents or recruits with non-human espionage. This is easiest in the case

---

of the analysis of radio signals from military establishments or vehicles.

The form of espionage by technical means with which the public is most familiar is that which uses satellite photography. In addition, however, electromagnetic signals of any kind are intercepted and analyzed (Signals Intelligence-SIGINT).

In the military field, certain electromagnetic signals, e.g. those from radar stations, may provide valuable information about the organization of enemy air defenses (electronic intelligence-ELINT). In addition, electromagnetic radiation, which could reveal details of the position of troops, aircraft, ships or submarines, is a valuable source of information for an intelligence service. Monitoring other states spy satellites, which take photographs, and recording and decoding signals from such satellites, is also useful.

Ground stations record the signals from low-orbit satellites or from quasi-geostationary SIGINT satellites. This aspect of intelligence operations using electromagnetic means consumes a large part of services' interception capacity. However, this is not the only use made of technology.

The foreign intelligence services of many states intercept the military and diplomatic communications of other states. Many of these services also monitor the civil communications of other states if they have access to them. In some states, services are also authorized to monitor incoming or outgoing communications in their own country. In democracies, intelligence services monitoring of the communications of the country's own citizens is subject to certain triggering conditions and controls. However, domestic law in general only protects nationals within the territory of their own country and other residents of the country concerned

## **The Operations of Certain Intelligence Services**

Public debate has been sparked primarily by the interception operations of the US and British intelligence services. They have been criticized for recording and analyzing communications (voice, fax, E-mail). A political assessment requires a yardstick for judging such operations. The interception operations of foreign intelligence services in the EU may be taken as a basis for comparison. Table 1 provides an overview. It shows that interception of private communications by foreign intelligence services is by no means confined to the US or British foreign intelligence services.

Country	Communications in foreign countries	State communications	Civilian communications
<b>Belgium</b>	+	+	+
<b>Denmark</b>	+	+	+
<b>Finland</b>	+	+	+
<b>France</b>	+	+	+
<b>Germany</b>	+	+	+
<b>Greece</b>	+	+	-
<b>Ireland</b>	-	-	-
<b>Italy</b>	+	+	+
<b>Luxembourg</b>	-	-	-
<b>Netherlands</b>	+	+	+
<b>Austria</b>	+	+	-
<b>Portugal</b>	+	+	-
<b>Sweden</b>	+	+	+
<b>Spain</b>	+	+	+
<b>UK</b>	+	+	+
<b>USA</b>	+	+	+
<b>Canada</b>	+	+	+
<b>Australia</b>	+	+	+
<b>New Zealand</b>	+	+	+

Table 1: Interception operations by intelligence services in the EU and in the UKUSA states.<sup>11</sup>

---

## Technical Conditions Governing the Interception of Telecommunications

If people wish to communicate with one another over a given distance, they need a medium. This medium may be air (sound waves); light (Morse lamp, fiber optic cable); electric current (telegraph, telephone); or an electromagnetic wave (all forms of radio). Any third party who succeeds in accessing the medium can intercept the communications. This process may be easy or difficult, feasible anywhere or only from certain locations. Two extreme cases are discussed below—the technical possibilities available to a spy working on the spot, on the one hand, and the scope for a worldwide interception system, on the other.

On the spot, any form of communication can be intercepted if the eavesdropper is prepared to break the law and the target does not take protective measures. Conversations in rooms can be intercepted by means of planted microphones (bugs) or laser equipment which picks up vibrations in windowpanes. Screens emit radiation, which can be picked up at a distance of up to 30 meters, revealing the information on the screen.

Telephone, fax, and e-mail messages can be intercepted if the eavesdropper taps into a cable leaving the relevant building. Although the infrastructure required is costly and complex, communications from a mobile phone can be intercepted if the interception station is situated in the same radio cell (diameter 300-m in urban areas, 30 km in the countryside).

Closed-circuit communications can be intercepted within the USW-radio range. Conditions for the use of espionage equipment are ideal on the spot, since the interception measures can be focused on one person or one target and almost every communication can be intercepted. The only disadvantage may be the risk of detection in connection with the planting of bugs or the tapping of cables.

Today, various media are available for all forms of intercontinental communication (voice, fax and data). The scope for a worldwide interception system is restricted by two factors: restricted access to the communication medium and the need to filter out the relevant communication from a huge mass of communications taking place at the same time.

All forms of communication (voice, fax, e-mail, and data) are transmitted by cable. Access to the cable is a prerequisite for the interception of communications of this kind. Access is certainly possible if the terminal of a cable connection is situated on the territory of a state, which allows interception. In technical terms, therefore, within an individual state all communications carried by cable can be intercepted, provided this is permissible under the law. However, foreign intelligence services generally have no legal access to cables situated on the territory of other states. At best, they can gain illegal access to a specific cable, although the risk of detection is high.

From the telegraph age onwards, intercontinental cable connections have been achieved by means of underwater cables. Access to these cables is always possible at those points where they emerge from the water. If several states join forces to intercept communications, access is possible to all the terminals of the cable connections situated in those states. This was historically significant, since both the underwater telegraph cables and the first underwater coaxial telephone cables linking Europe and America landed in Newfoundland and the connections to Asia ran via Australia, because regenerators were required.

Today, fiber optic cables follow the direct route, regardless of the mountainous nature of the ocean bed and the need for regenerators, and do not pass via Australia or New Zealand. Electric cables may also be tapped between the terminals of a connection, by means of induction (i.e. Electromagnetically, by attaching a coil to the cable), without creating a direct, conductive connection. Underwater electric cables can also be tapped in this way from submarines, albeit at very high cost. This technique was employed by the USA in order

---

to tap into a particular underwater cable laid by the USSR to transmit unencrypted commands to Soviet atomic submarines. The high costs alone rule out the comprehensive use of this technique.

In the case of the older-generation fiber optic cables used today, inductive tapping is only possible at the regenerators. These regenerators transform the optical signal into an electrical signal, strengthen it and then transform it back into an optical signal. However, this raises the issue of how the enormous volumes of data carried on a cable of this kind can be transmitted from the point of interception to the point of evaluation without the laying of a separate fiber optic cable.

On cost grounds, the use of a submarine fitted with processing equipment is conceivable only in very rare cases, for example in wartime, with a view to intercepting the enemy's strategic military communications. The use of submarines for the routine surveillance of international telephone traffic can be ruled out.

The new-generation fiber optic cables use erbium lasers as regenerators. Interception by means of electromagnetic coupling is thus no longer possible. Communications transmitted using fiber optic cables of this kind can thus only be intercepted at the terminals of the connection.

The practical implication for the UKUSA states is that communications can be intercepted at acceptable cost only at the terminals of the underwater cables, which land on their territory. Essentially, therefore, they can only tap incoming or outgoing cable communications. In other words, their access to cable communications in Europe is restricted to the territory of the United Kingdom, since hitherto internal communications have mostly been transmitted via the domestic cable network. The privatization of telecommunications may give rise to exceptions, but these are specific and unpredictable.

This is valid at least for telephone and fax communications. Other conditions apply to

communications transmitted over the Internet via cable. The situation can be summarized as follows:

- Internet communications are carried out using data packets and different packets addressed to the same recipient may take different routes through the network.
- At the start of the Internet age, spare capacity in the public network was used for the transmission of e-mail communications. For that reason, the routes followed by individual data packets were completely unpredictable and arbitrary. At that time, the most important international connection was the science backbone between Europe and America.
- The commercialization of the Internet and the establishment of Internet providers also resulted in a commercialization of the network. Internet providers operated or rented their own networks. They therefore made increasing efforts to keep communications within their own network in order to avoid paying user fees to other operators. Today, the route taken through the network by a data packet is therefore not solely determined by the capacity available on the network, but also hinges on cost considerations.
- An E-mail sent from a client of one provider to a client of another provider is generally routed through the firm's network, even if this is not the quickest route. Routers, computers situated at network junctions and which determine the route by which data packets will be transmitted, organize the transition to other networks at points known as switches.
- At the time of the science backbone, the switches for the routing of global Internet communications were situated in the USA. For that reason, at that time intelligence services could intercept a substantial proportion of European Internet communications. Today, only a small proportion of intra-European Internet communications is routed via the USA.<sup>12</sup>
- A small proportion of intra-European communications is routed via a switch in London to which, since foreign communications are involved, the British monitoring station GCHQ has access. The majority of communications do not leave the continent:

---

for example, more than 95% of intra-German Internet communications are routed via a switch in Frankfurt.

In practical terms, this means that the UKUSA states have access only to a very limited proportion of Internet communications transmitted by cable.

The interceptibility of radio communications depends on the range of the electromagnetic waves employed. If the radio waves run along the surface of the earth (so-called ground waves), their range is restricted and is determined by the topography of the earth's surface, the degree to which it is built up and the amount of vegetation. If the radio waves are transmitted towards space (so-called space waves), two points a substantial distance apart can be linked by means of the reflection of the sky wave from layers of the ionosphere. Multiple reflections substantially increase the range.

The range is determined by the wavelength:

- Very long and long waves (3 kHz  $\text{\textcircled{C}}$  300 kHz) propagate only via ground waves, because space waves are not reflected. They have very short ranges.
- Medium waves (300 kHz  $\text{\textcircled{C}}$  3 MHz) propagate via ground waves and at night also via space waves. They are medium-range radio waves.
- Short waves (3 MHz  $\text{\textcircled{C}}$  30 MHz) propagate primarily via ground waves; multiple reflections make worldwide reception possible.
- Ultra-short waves (30 MHz  $\text{\textcircled{C}}$  300 MHz) propagate only via ground waves, because space waves are not reflected. They propagate in a relatively straight line, like light, with the result that, because of the curvature of the earth, their range is determined by the height of the transmitting and receiving antennae. Depending on power, they have ranges of up to 100 km (roughly 30 km in the case of mobile phones).
- Decimeter and centimeter waves (30 MHz  $\text{\textcircled{C}}$  30 GHz) propagate in a manner even more akin to light than ultra-short waves. They are easy to focus, clearing the way for low-power, unidirectional transmissions (ground-based

microwave radio links). They can only be received by antennae situated almost or exactly in line-of-sight.

Long and medium waves are used only for radio transmitters, radio beacons, etc. Short wave and above all, USW and decimeter/centimeter waves are used for military and civil radio communications.

The details outlined above show that a global communications interception system could only intercept short-wave radio transmissions. In the case of all other types of radio transmission, the interception station must be situated within a 100-km radius (e.g. on a ship, in an embassy). The practical implication for the UKUSA states with terrestrial listening stations is that they can intercept only a very limited proportion of radio communications.

As already referred to above, decimeter and centimeter waves can very easily be focused to form microwave radio links. If a microwave radio link is set up transmitting to a telecommunications satellite in a high, geostationary orbit and the satellite receives the microwave signals, converts them and transmits them back to earth, large distances can be covered without the use of cables. The range of such a link is essentially restricted only by the fact that the satellite can receive and transmit only in a straight line. For that reason, several satellites are employed to provide worldwide coverage. If UKUSA States operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax and data traffic transmitted via such satellites.

It has long been known that special AWACS aircraft are used for the purpose of locating other aircraft over long distances. The radar equipment in these aircraft works in conjunction with a detection system designed to identify specific objectives, which can locate forms of electronic radiation, classify them and correlate them with radar sightings. They have no separate SIGINT capability.<sup>13</sup> In contrast, the slow flying EP-3 spy

---

plane used by the US Navy has the capability to intercept microwave, USW and short-wave transmissions. The signals are analyzed directly on board and the aircraft is used solely for military purposes.<sup>14</sup> In addition, surface ships, and in coastal regions, submarines are used to intercept military radio transmissions.<sup>15</sup>

Provided they are not focused through the use of appropriate antennae, radio waves radiate in all directions, i.e. also into space. Low-orbit Signals Intelligence Satellites can only lock on to the target transmitter for a few minutes in each orbit. In densely populated, highly industrialized areas interception is hampered to such a degree by the high density of transmitters using similar frequencies that it is virtually impossible to filter out individual signals.<sup>16</sup> The satellites cannot be used for the continuous monitoring of civilian radio communications.

Alongside these satellites, the USA operates so-called quasi-geostationary SIGINT satellites stationed in a high earth orbit (42 000 km).<sup>17</sup> Unlike the geostationary telecommunications satellites, these satellites have an inclination of between 3 and 10°, an apogee of between 39,000 and 42,000 km, and a perigee of between 30,000 and 33,000 km. The satellites are thus not motionless in orbit, but move in a complex elliptical orbit, which enables them to cover a larger area of the earth in the course of one day and to locate sources of radio transmissions. This fact, and the other non-classified characteristics of the satellites, points to their use for purely military purposes. The signals received are transmitted to the receiving station by means of a strongly-focused, 24 GHz downlink.

When foreign communications are intercepted, no single telephone connection is monitored on a targeted basis. Instead, some or all of the communications transmitted via the satellite or cable in question are tapped and filtered by computers employing keywords—analysis of every single communication would be completely impossible.

It is easy to filter communications transmitted along a given connection. Specific faxes and e-mails can also be singled out through the use of keywords. If the system has been trained to recognize a particular voice, communications involving that voice can be singled out. However, the automatic recognition to a sufficient degree of accuracy of words spoken by any voice is not yet possible. Moreover, the scope for filtering out is restricted by other factors: the ultimate capacity of the computers, the language problem and, above all, the limited number of analysts who can read and assess filtered messages.

When assessing the capabilities of filter systems, consideration must also be given to the fact that in the case of an interception system working on the basis of the vacuum-cleaner principle, those technical capabilities are spread across a range of topics. Some of the keywords relate to military security, some to drug trafficking and other forms of international crime, some to the trade in dual-use goods and some to compliance with embargoes. Some of the keywords also relate to economic activities. Any move to narrow down the range of keywords to economically interesting areas would simply run counter to the demands made on intelligence services by governments; what is more, even the end of the Cold War was not enough to prompt such a step.

### **The Example of the German Federal Intelligence Service**

Department 2 of the German Federal Intelligence Service (FIS) obtains information through the interception of foreign communications. This activity was the subject of a review by the German Federal Constitutional Court. The details made public during the court proceedings combined with the evidence given to the Temporary Committee on 21 November 2000 by Mr. Ernst Uhrlau, the coordinator for the secret services in the Federal Chancellor's Office, give an insight into the scope for obtaining intelligence by intercepting satellite communications.<sup>18</sup>

---

On the basis of differing legal provisions or the availability of a greater number of analysts, the capabilities of other intelligence services may be greater in detail terms in given areas. In particular, the monitoring of cable traffic increases the statistical likelihood of success, but not necessarily the number of communications, which can be analyzed. In fundamental terms, the example of the FIS demonstrates the capabilities and strategies employed by foreign intelligence services in connection with the monitoring of foreign communications, even if those services do not disclose such matters to the public.

The FIS endeavors, by means of strategic telecommunications monitoring, to secure information from foreign countries about foreign countries. With that aim in view, satellite transmissions are intercepted using a series of search terms (which in Germany must be authorized in advance by the so-called G10 Committee<sup>19</sup>). The relevant figures break down as follows (year 2000): of the roughly 10 million international communications routed to and from Germany every day, some 800 000 are transmitted via satellite. Just under 10% of these (75 000) are filtered through a search engine.

This limitation is not imposed by the law (in theoretical terms, and at least prior to the proceedings before the Federal Constitutional Court, a figure of 100% would have been allowable), but derives from technical restrictions, e.g. the limited capacity for analysis. The number of usable search terms is likewise restricted on technical grounds and by the need to secure authorization.

The grounds for the judgment handed down by the Federal Constitutional Court refer, alongside the purely formal search terms (connections used by foreign nationals or foreign firms abroad), to 2,000 search terms in the sphere of nuclear proliferation, 1,000 in the sphere of the arms trade, 500 in the sphere of terrorism and 400 in the sphere of drug trafficking. However, the procedure has proved relatively unsuccessful in connection with terrorism and drug trafficking.

The search engine checks whether authorized search terms are used in fax and telex communications. Automatic word recognition in voice connections is not yet possible. If the search terms are not found, in technical terms the communications automatically end up in the waste bin; they cannot be analyzed, owing to the lack of a legal basis. Every day, five or so communications are logged, which are covered by the provisions governing the protection of the German constitution. The monitoring strategy of the FIS is geared to finding clues on which to base further monitoring activities. The monitoring of all foreign communications is not an objective. This also applies to the SIGINT activities of other foreign intelligence services.

### **Satellite Communications Technology**

Today, telecommunications satellites form an essential part of the global telecommunications network and have a vital role to play in the provision of television and radio programs and multimedia services. Nevertheless, the proportion of international communications accounted for by satellite links has decreased substantially over the past few years in Central Europe; it lies between 0.4 and 5%.<sup>20</sup> This can be explained by the advantages offered by fiber optic cables, which can carry a much greater volume of traffic at a higher connection quality.

Today, voice communications are also carried by digital systems. The capacity of digital connections routed via satellites is restricted to 1,890 ISDN-standard [Integrated Services Digital Network] (64 kbits/sec) voice channels per transponder on the satellite in question. In contrast, 241,920 voice channels with the same standard can be carried on a single optical fiber. This corresponds to a ratio of 1:128.

In addition, the quality of connections routed via satellite is lower than those routed via underwater fiber optic cables. In the case of normal voice transmissions, the loss of quality resulting from the long delay times of several hundred milliseconds is hardly noticeable—although it is perceptible. In

---

the case of data and fax connections, which involve a complicated handshaking procedure, cable offers clear advantages in terms of connection security. At the same time, however, only 15% of the world's population are connected to the global cable network.<sup>21</sup>

For certain applications, therefore, satellite systems will continue to offer advantages over cable in the long term. Here are some examples from the civilian sphere:

- National, regional and international telephone and data traffic in areas with a low volume of communications, i.e. in those places where the low rate of use would make a cable connection unprofitable;
- Temporary communications systems used in the context of rescue operations following natural disasters, major events, large-scale building sites, etc.;
- UN missions in regions with an underdeveloped communications infrastructure.
- Flexible/mobile business communications using very small earth stations (VSATs, see below).

This wide range of uses to which satellites are put in the communications sphere can be explained by the following characteristics: the footprint of a single geostationary satellite can cover almost 50% of the earth's surface—impassable regions no longer pose a barrier to communication. In the area concerned, 100% of users are covered, whether on land, at sea or in the air. Satellites can be made operational within a few months, irrespective of the infrastructure available on the spot, they are more reliable than cable and can be replaced more easily.

The following characteristics of satellite communications must be regarded as drawbacks: the relatively long delay times, the path attenuation, the shorter useful life, by comparison with cable, of 12 to 15 years, the greater vulnerability to damage and the ease of interception.

By using appropriate antennae microwaves can be very effectively focused, allowing cables to be replaced by microwave radio links. If the transmitting and the receiving antenna are not in

line of sight, but rather, as they are on the earth, on the surface of a sphere, then from a given distance onwards the receiving antenna, disappears below the horizon owing to the curvature of the earth. The two antennae are thus no longer in line of sight. This would apply, for example, to an intercontinental microwave radio link between Europe and the USA.

The antennae would have to be fitted to masts 1.8 km high in order for a link to be established. For this reason, an intercontinental microwave radio link of this kind is simply not feasible, setting aside the issue of the attenuation of the signal by air and water vapor. However, if a kind of mirror for the microwave radio link can be set up in a fixed position high above the earth in space, large distances can be overcome, despite the curvature of the earth, just as a person can see round corners using a traffic mirror. The principle described above is made workable through the use of geostationary satellites.

If a satellite is placed into a circular orbit parallel to the equator in which it circles the earth once every 24 hours, it will follow the rotation of the earth exactly. Looking up from the earth's surface, it seems to stand still at a height of roughly 36 000 km—it has a geostationary position. Most communications and television satellites are satellites of this type.

The transmission of signals via satellite can be described as follows:

- The signal coming from a cable is transmitted by an earth station equipped with a parabolic antenna to the satellite via an upward microwave radio link, the **uplink**.
- The satellite receives the signal, regenerates it and transmits it back to another Earth station via a downward microwave radio link, the **downlink**.
- From there, the signal is transferred back to a cable network.

---

In the case of mobile communications satellite telephones the signal is transmitted directly from the mobile communications unit to the satellite, from where it can be fed into a cable link, via an Earth station, or directly transmitted to a different mobile unit.

### **The Most Important Satellite Communication Systems**

If necessary, communications coming from public cable networks (not necessarily state networks) are transmitted between fixed earth stations, via satellite systems of differing scope, and then fed back into cable networks. A distinction is drawn between the following forms of satellite systems:

- Global systems (e.g. INTELSAT).
- Regional (continental) systems (e.g. EUTELSAT).
- National systems (e.g. ITALSAT).

Most of these satellites are in a geostationary orbit; 120 private companies throughout the world operate some 1,000 satellites.<sup>22</sup>

In addition, the far northern areas of the earth are covered by satellites in a highly elliptical orbit (Russian molnyia orbits) in which the satellites are visible to users in the far north for half their orbit. In principle, two satellites can provide full regional coverage,<sup>23</sup> which is not feasible from a geostationary position above the equator. In the case of the Russian Molnyia satellites, which have been in service as communications satellites since 1974 (prototype launched in 1964), three equidistant satellites orbit the earth once every 12 hours and thus guarantee continuous transmission of communications.<sup>24</sup>

Alongside this, the global INMARSAT system—originally established for use at sea—provides a mobile communications system by means of which satellite links can be established anywhere in the world. This system also uses geostationary satellites. The worldwide satellite-based mobile telephone system Iridium, which employed a number of satellites placed at time intervals in low orbits, recently ceased operating on economic grounds (over-capacity).

There is also a rapidly expanding market for so-called VSAT links (VSAT—very small aperture terminal). This involves the use of very small earth stations with antennae with a diameter of between 0.9 and 3.7 meters, which are operated either by firms to meet their own needs (e.g. videoconferences) or by mobile service providers to meet short-term communications requirements (e.g. in connection with meetings).

In 1996, 200,000 very small earth stations were in operation around the world. Volkswagen AG operates 3,000 VSAT units, Renault 4,000, General Motors 100,000 and the largest European oil company 12,000. If the client does not arrange for encryption, communication is entirely open.

Through the positioning of satellites above the Atlantic, Indian and Pacific regions, these satellite systems cover the entire globe.

### ***INTELSAT***

INTELSAT (International Telecommunications Satellite Organization) was founded as an authority in 1964 with an organizational structure similar to that of the UN and with the commercial purpose of providing international communications. The members of the organization were state-owned telecommunications companies. Today, 144 governments are INTELSAT members. In 2001, INTELSAT will be privatized.

INTELSAT now operates a fleet of 20 geostationary satellites, which provide links between more than 200 countries and whose services are rented out to the members of INTELSAT. The members operate their own ground stations. Following the establishment of INTELSAT Business Service (IBS) in 1984, non-members (e.g. telephone companies, large firms, and international concerns) can also use the satellites. INTELSAT offers global services such as communications, television, etc. Telecommunications are transmitted via the C-band and the Ku-band.

---

INTELSAT satellites are the most important international telecommunications satellites, accounting for a very large proportion of the world market in such communications. The satellites cover the Atlantic, Indian and Pacific regions. Ten satellites are positioned above the Atlantic between 304°E and 359°E. The Indian region is covered by six satellites situated between 62°E and 110m.5°E and the Pacific region by three satellites situated between 174°E and 180°E. The high volume of traffic in the Atlantic region is covered by a number of individual satellites positioned at the relevant longitudes.

### ***INTERSPUTNIK***

In 1971 the international communications organization INTERSPUTNIK was founded by nine countries as an agency of the former Soviet Union with a task similar to that of INTELSAT. Today, INTERSPUTNIK is an international organization, which the government of any country can join. It now has 24 member countries (including Germany) and some 40 users (including France and the UK), which are represented by their post offices or national telecommunications companies. Its headquarters are in Moscow.

Telecommunications are transmitted via the C-band and the Ku-band. Its satellites (Gorizont, Express and Express A, owned by the Russian Federation, and LMI-1, the product of the Lockheed-Martin joint venture) also cover the entire globe: one satellite is positioned above the Atlantic region, with a second planned, three are positioned above the Indian region and two are positioned above the Pacific region.

### ***INMARSAT***

Since 1979 INMARSAT (Interim International Maritime Satellite) has provided, by means of its satellite system, worldwide mobile communications at sea, in the air and on land and an emergency radio system. INMARSAT was set up as an international organization at the instigation of the International Maritime Organization. INMARSAT has since been privatized and has its headquarters in London.

The INMARSAT system consists of nine satellites in geostationary orbits. Four of these satellites—the INMARSAT-III generation—cover the entire globe with the exception of the high polar areas. Each individual satellite covers roughly one-third of the earth's surface. Through their positioning above the four ocean regions (West and East Atlantic, Pacific, Indian Ocean), global coverage is provided. At the same time, each INMARSAT has a number of spot beams, which make it possible to focus energy in areas with heavier communications traffic. Telecommunications are transmitted via the L-band and the Ku-band.

### ***PANAMSAT***

PanAmSat was founded in 1988 as a commercial provider of a global satellite system and has its headquarters in the USA. PanAmSat now has a fleet of 21 satellites, which provide services such as television, Internet and telecommunications on a worldwide basis, albeit chiefly in the USA. Telecommunications are transmitted via the C-band and the Ku-band. Of the 21 satellites, seven cover the Atlantic region, two the Pacific region and two the Indian Ocean region. The footprints of the remaining satellites cover North and South America. The PanAmSat satellites play only a secondary role in communications in Europe.

### **Regional Satellite Systems**

The footprints of regional satellite systems cover individual regions/continents. As a result, the communications transmitted via them can be received only in those regions.

### ***EUTELSAT***

EUTELSAT was founded in 1977 by 17 European postal administrations with the aim of meeting Europe's specific satellite communication requirements and supporting the European space industry. It has its headquarters in Paris and some 40-member countries. EUTELSAT is to be privatized in 2001.

---

EUTELSAT operates 18 geostationary satellites, which cover Europe, Africa and large parts of Asia and establish a link with America. The satellites are positioned between 12.5°W and 48°E. EUTELSAT mainly offers television (850 digital and analog channels) and radio (520 channels) services, but also provides communication links—primarily within Europe, including Russia, e.g. for videoconferences—for the private networks run by large undertakings (including General Motors and Fiat), for press agencies (Reuters, AFP), for providers of financial information and for mobile data transmission services. Telecommunications are transmitted via the Ku-band.

### **ARABSAT**

ARABSAT is the counterpart to EUTELSAT in the Arab region and was founded in 1976. Membership is made up of 21 Arab countries. ARABSAT satellites are used both for the transmission of television services and for communications. Telecommunications are transmitted mainly via the C-band.

### **PALAPA**

The Indonesian PALAPA system has been in operation since 1995 and is the south-Asian counterpart to EUTELSAT. Its footprint covers Malaysia, China, Japan, India, Pakistan and other countries in the region. Telecommunications are transmitted via the C-band and the Ku-band.

### **National Satellite Systems**

Many states meet their own requirements by operating satellite systems with restricted footprints.

One purpose of the French telecommunications satellite TELECOM is to link the French departments in Africa and South America with mainland France. Telecommunications are transmitted via the C-band and the Ku-band.

ITALSAT operates telecommunications satellites, which cover the whole of Italy by means of a series

of restricted footprints. Reception is therefore possible only in Italy. Telecommunications are transmitted via the Ku-band.

AMOS is an Israeli satellite whose footprint covers the Middle East. Telecommunications are transmitted via the Ku-band.

The Spanish HISPASAT satellites cover Spain and Portugal (KU-spots) and transmit Spanish television programs to North and South America.

### **The Allocation of Frequencies**

The International Telecommunications Union (ITU) is responsible for the allocation of frequencies. For ease of organization, for radio communication purposes the world has been divided into three regions:

1. Europe, Africa, former Soviet Union, Mongolia;
2. North and South America and Greenland;
3. Asia, with the exception of countries in region 1, Australia and the South Pacific.

This division, which has become established over the years, was taken over for the purposes of satellite communications and has led to the positioning of large numbers of satellites in certain geostationary areas. The most important frequency bands for satellite communications are:

- The L-band (0.4 to 1.6 GHz) for mobile satellite communications, e.g. via IMMARSAT;
- The C-band (3.6 to 6.6 GHz) for earth stations, e.g. via INTELSAT;
- The Ku-band (10 to 20 GHz) for earth stations, e.g. INTELSAT Ku-spot and EUTELSAT;
- The Ka-band (20 to 46 GHz) for earth stations, e.g. military communications satellites;
- The V-band (46 to 56 GHz) for very small earth stations (VSATs).

The footprint is the area on the earth covered by a satellite antenna. It may embrace up to 50% of the earth's surface, or, by means of signal focusing, be restricted to small, regional spots. The higher the frequency of the signal emitted, the more it can be

---

focused and the smaller the footprint becomes. The focusing of the satellite signal on smaller footprints can increase the energy of the signal. The smaller the footprint, the stronger the signal, and thus the smaller the receiving antennae may be.

Parabolic antennae with a diameter of between 0.5 and 30m are used as receiving antennae on the earth. The parabolic mirror reflects all incoming waves and focuses them. The actual receiving system is situated in the focal point of the parabolic mirror. The greater the energy of the signal at the receiving point is, the smaller the diameter of the parabolic antenna need be.

The footprints of the INTELSAT satellites are divided into various beams. Each satellite's global beam (G) covers roughly one-third of the earth's surface; the hemispheric beams (H) each cover an area slightly smaller than half that covered by the global beams. Zone beams (Z) are spots in particular areas of the earth; they are smaller than the hemi-beams. In addition there are so-called spot beams; these are small, precise footprints.

The key factor in connection with the investigations conducted for this report is that a proportion of intercontinental communications are transmitted via the C-band in the global beams of the INTELSAT satellites and other satellites (e.g. INTERSPUTNIK) and those satellite antennae with a diameter of roughly 30-m are needed to receive some of these communications. Antennae of that size were also needed for the first stations set up to intercept satellite communications, since the first generation of INTELSAT satellites had only global beams and signal transmission technology was much less sophisticated than it is today. These antennae, some of which have a diameter of more than 30 m, are still used at the stations in question, even though they are no longer required on purely technical grounds. Today, the typical antennae required for INTELSAT communications in the C-band have a diameter of between 13 and 20 m.

Antennae with a diameter of between 2 and 5 m are required for the Ku-spots of the INTELSAT satellites and other satellites (EUTELSAT Ku-

band, AMOS Ku-band, etc.). In the case of very small earth stations, which operate in the V-band and whose signal, by virtue of the high frequency, can be focused even more strongly than those in the Ku-band, antennae with a diameter of between 0.5 and 3.7 m are adequate (e.g. VSATs from EUTELSAT or INMARSAT).

## **Satellite Communications for Military Purposes**

Communications satellites play an important role in the military sphere as well. Many countries, including the USA, the United Kingdom, France and Russia, operate their own geostationary military communications satellites, with the aid of which independent global communication is possible. The USA has stationed one satellite roughly every 10° around the earth in some 32 orbital positions. However, some use is also made of commercial geostationary satellites for the purposes of providing military communications.

The frequency bands used for military communications lie in the range between 4 GHz and 81 GHz. The bands typically used by military communications satellites are X-band (SHF - 3-30 GHz) and the Ka-band (EHF - 20-46 GHz).

A distinction must be drawn between mobile stations, which may have a diameter of only a few decimeters, and fixed stations, which generally have a diameter not exceeding 11m. There are, however, two types of antenna (to receive signals from DSCS satellites) with a diameter of 18m.

The US MILSTAR program (Military Strategy, Tactical and Relay Satellite System), which operates six geostationary satellites worldwide, enables US armed forces to communicate with each other and with command centers using small earth stations, aircraft, ships and man-packs. Through the link among the satellites themselves worldwide communications availability is guaranteed even if all the US earth stations cease operating.

---

The DSCS (Defense Satellite Communications System) also provides global communications by means of five geostationary satellites. The US armed forces and some use the system government agencies.

The British military satellite system SKYNET also provides global communications. The French system SYRACUSE, the Italian system SICRAL and the Spanish system fly piggy-back on their respective national civilian communications satellites and provide military communications, albeit only on a regional basis, in the S-band. The Russians guarantee their armed forces' communications by means of transponders in the X-band used by the Molnya satellites.

NATO operates its own communications satellites (NATO IIID, IVA and IVB). The satellites provide voice, telex and data links between military units.

### **Clues to the Existence of at Least One Global Interception System**

It is only natural that secret services do not disclose details of their work. Consequently there is, at least officially, no statement by the foreign intelligence services of the UKUSA states that they work together to operate a global interception system. The existence of such a system thus needs to be proved by gathering as many clues as possible, thereby building up a convincing body of evidence.

The trail of clues which constitutes evidence of this kind is made up of three elements:

- Evidence that the foreign intelligence services in the UKUSA states intercept private and business communications;
- Evidence that interception stations operated by the UKUSA states are to be found in the parts of the world where they would be needed in the light of the technical requirements of the civilian satellite communication system;
- Evidence that there is a closer than usual association between the intelligence services of these states.

For the purposes of proving the existence of such an association, it is irrelevant whether this extends to the acceptance from partners of applications for the interception of messages, which are then forwarded to them in the form of unevaluated raw material. This question is only relevant when investigating the hierarchies within such an interception association.

At least in democracies, intelligence services work on the basis of laws, which define their purpose and/or powers. It is thus easy to prove that in many of these countries foreign intelligence services exist which intercept civilian communications. This is true of the five UKUSA states, which all operate such services. There is no need for specific additional proof that any of these states intercept communications entering and leaving their territory.

Satellite communications also permit some intelligence communications intended for recipients abroad to be intercepted from the country's own territory. In none of the five UKUSA states is there any legal impediment to intelligence services doing this. The logic underlying the method for the strategic monitoring of foreign communications, and its at least partly overtly acknowledged purpose, make it practically certain that the intelligence services do in fact use it to that end.

The only restriction on the attempt to build up worldwide monitoring of satellite communications arises from the technical constraints imposed by these communications themselves. There is no place from which all satellite communications can be intercepted. It would be possible for a worldwide interception system to be constructed, subject to three conditions:

- The operator has national territory of its own in all the necessary parts of the world;
- The operator has, in all the necessary parts of the world, either national territory of its own or a right of access entitling it to operate or share the use of stations;
- The operator is a group of states, which has formed an intelligence association and operates the system in the necessary parts of the world.

---

None of the UKUSA states would be able to operate a global system on its own. The USA has, at least formally, no colonies. Canada, Australia and New Zealand also have no territory outside the narrower confines of their countries, and the UK would also not be able to operate a global interception system on its own.

On the other hand it has not been disclosed whether and to what extent the UKUSA states cooperate with one another in the intelligence field. Normally cooperation between intelligence services takes place bilaterally and on the basis of an exchange of evaluated material. A multilateral alliance is in itself something very unusual; if one adds to this the regular exchange of raw material, this would be a qualitatively new form of cooperation. The existence of such an association can only be proved on the basis of clues.

### **How Can a Satellite Communications Interception Station be Recognized?**

Installations with large antennae belonging to the post office, broadcasting organizations or research institutions are accessible to visitors, at least by appointment; interception stations are not. They are generally operated, at least in name, by the military, which also carries out at least part of the technical work of interception. In the case of the stations run by the USA, for example, operations are carried out jointly with NSA by the Naval Security Group (NAVSECGRU), the United States Army Intelligence and Security Command (INSCOM) or the Air Intelligence Agency (AIA). In the British stations, the British intelligence service GCHQ operates the installations jointly with the Royal Air Force (RAF). This arrangement enables the installations to be guarded with military efficiency and at the same time serves as cover.

Various types of antennae are used in the installations, which fulfil criterion 1, each with a different characteristic shape, which provides evidence as to the purpose of the interception station. Arrangements of tall rod antennae in a large-diameter circle (Wullenweber antennae), for example, are used for locating the direction of

radio signals. Similarly, circular arrangements of rhombic-shaped antennae (Pusher antennae) serve the same purpose. Omnidirectional antennae, which look like giant conventional TV antennae, are used to intercept non-directional radio signals. To receive satellite signals, however, only parabolic antennae are used. If the parabolic antennae are standing on an open site, it is possible to calculate on the basis of their position, their elevation and their compass (azimuth) angle which satellite is being received. This is possible, for example, in Morwenstow (UK), Yakima (USA) or Sugar Grove (USA).

However, most often parabolic antennae are concealed under spherical white covers known as radomes: these protect the antennae, but also conceal which direction they are pointing in. If parabolic antennae or radomes are positioned on an interception station site, one may be certain that they are receiving signals from satellites, though this does not prove what type of signals these are.

Satellite receiving antennae on a site, which meets criterion 1, may be intended for various purposes:

- Receiving station for military communications satellites;
- Receiving station for spy satellites (pictures, radar);
- Receiving station for SIGINT satellites;
- Receiving station for interception of civilian communications satellites.

It is not possible to tell from outside what function these antennae or radomes serve. However, the diameter of the antennae gives some clues as to their purpose. There are minimum sizes, dictated by technical requirements, for antennae intended to receive the global beam in the C-band of satellite-based civilian international communications. The first generation of these satellites needed antennae with a diameter of 25-30 m; nowadays 15-20 m is enough. The automatic computer filtering of signals received calls for the highest possible signal quality, so for intelligence purposes an antenna at the upper end of the scale is chosen.

---

In the sphere of military communications as well, command centers have two types of antenna with a diameter of roughly 18 m (AN/FSC-78 and AN/FSC-79). However, most antennae for military communications have a much smaller diameter, since they must be transportable (tactical stations).

In view of the nature of the signals transmitted back to the station (high degree of focusing and high frequency), earth stations for SIGINT satellites need only small antennae. This also applies to antennae, which receive signals from spy satellites. If a site houses two or more satellite antennae with a diameter of at least 18-m, one of its tasks is certainly that of intercepting civilian communications. In the case of a station housing US forces, one of the antennae may also be used to receive military communications.

Official descriptions of the tasks of some stations have been published. In that connection governments and military units are regarded as official sources. If this criterion has been met, the others become superfluous.

### **Publicly Accessible Data About Known Interception Stations**

With a view to determining which stations meet the criteria and thus form part of the global interception system and establishing what tasks they have, the relevant, somewhat contradictory, literature (Hager,<sup>25</sup> Richelson,<sup>26</sup> Campbell<sup>27</sup>) declassified documents,<sup>28</sup> the homepage of the Federation of American Scientists and operators' homepages<sup>29</sup> (NSA, AIA, etc.) and other Internet publications were analyzed. In the case of the New Zealand station in Waihopai, the New Zealand Government has drawn up an official description of its tasks.<sup>30</sup> In addition, the footprints of telecommunications satellites were collated, the requisite antenna sizes were calculated and these footprints and antenna locations were entered, along with the locations of possible stations, on world maps.

The following principles relating to the physics of satellite communications apply in connection with the analysis:

- A satellite antenna can only record communications transmitted within the footprint in which it is located. In order to receive communications, which are mainly transmitted in the C-band and Ku-band, an antenna must lie within the footprints containing those bands.
- A satellite antenna is required for each separate global beam, even if beams from two satellites overlap.
- If a satellite has other footprints in addition to the global beam, which is typical of today's generations of satellites, a single satellite antenna can no longer record all the communications transmitted via that satellite, since a single satellite antenna cannot be located in every one of the satellite's footprints. In order to capture a satellite's hemispheric beam and its global beam, therefore, two satellite antennae are required in different areas.

If further beams (zone and spot beams) are involved, further satellite antennae are required. In principle, different, overlapping from a single satellite can be captured by one satellite antenna, since it is technically feasible to separate different frequency bands when reception takes place, although this leads to deterioration in the signal-noise ratio.

In addition, the non-accessibility of the installations, on the grounds that they are operated by the military,<sup>31</sup> the fact that parabolic antennae are required to receive satellite signals and the fact that the size of the satellite antennae needed to capture the C-band in the global beam at least 30 m for the first INTELSAT generation and more than 15 to 18 m for later generations and the official descriptions of the tasks of some of the stations have been cited as evidence of their role in interception operations.

A global interception system must grow as communications develop. Accordingly, the start of the satellite communications era must lead to the establishment of stations and the introduction of new generations of satellites must lead to the establishment of new stations and the building of new satellite antennae which can cope with the new

---

technical requirements. The number of stations and the number of satellite antennae must increase whenever this is necessary in order to cover the full volume of communications traffic.

If we turn this equation round, it is no coincidence that, when new footprints come into being, new stations are established and new satellite antennae is built. Instead, this can be seen as a clue to the existence of a communications interception station.

Since the INTELSAT satellites were the first telecommunications satellites, and, moreover, the first to cover the entire globe, it is only logical that the introduction of the new generations of INTELSAT satellites should go hand-in-hand with the establishment of new and bigger stations. As long ago as 1965 the first INTELSAT satellite (Early Bird) was placed in a geostationary orbit. Its transmission capacity was still low and its footprint covered only the Northern Hemisphere.

When the second and third INTELSAT generations came into operation, in 1967 and 1968 respectively, global coverage was achieved for the first time. The satellites' global beams covered the Atlantic, Pacific and Indian Ocean areas. Satellite systems with smaller footprints had not yet been introduced. Three satellite antennae were thus needed in order to record all communications. Since two of the global beams overlapped over the European continent, in that area the global footprints of two satellites could be covered by two satellite antennae trained in different directions.

In addition, there are further stations which, although they do not meet the criterion of antenna size, and although there is no other clear evidence underpinning the assumption, may still form part of the global interception system. These stations could be used to cover the zone or spot beams of satellites whose global beams are intercepted by other stations or for whose global beam no large satellite antennae are required.

## **The Stations in Detail**

In the detailed descriptions of the stations a distinction is drawn between stations, which are clearly used to intercept transmissions from telecommunications satellites and stations whose role cannot definitely be proven with the aid of those criteria.

The following stations meet the criteria, which point to a role in intercepting transmissions from telecommunications satellites.

### ***Yakima, USA (120°W, 46°N)***

The station was established in the 1970s, at the same time as the first generation of satellites were put into orbit. Since 1995, the Air Intelligence Agency (AIA), 544<sup>th</sup> Intelligence Group (Detachment 4), has been stationed in Yakima, along with the Naval Security Group (NAVSECGRU). Six satellite antennae have been installed on the site; the sources give no clue as to the size of the antennae. Hager describes the antennae as large and claims that they are trained on INTELSAT satellites over the Pacific (two satellite antennae) and INTELSAT satellites over the Atlantic, and on INMARSAT Satellite 2.

The fact that Yakima was established at the same time as the first generation of INTELSAT satellites went into orbit, and the general description of the tasks of the 544<sup>th</sup> Intelligence Group, suggest that the station has a role in global communications surveillance. A further clue is provided by Yakima's proximity to a normal satellite receiving station, which lies 100 miles to the north.

### ***Sugar Grove, USA (80°W, 39°N)***

Sugar Grove was established at the same time as the second generation of INTELSAT satellites came into operation, in the late 1970s. The NAVSECGRU and the AIA, 544<sup>th</sup> Intelligence

---

Group (Detachment 3) are stationed at Sugar Grove. According to information provided by a variety of authors, the station has 10 satellite antennae, three of which have a diameter greater than 18 m (18.2 m, 32.3 m and 46 m) and which are thus clearly used to intercept transmissions from telecommunications satellites. One of the tasks performed at the station by Detachment 3 of the 544<sup>th</sup> IG is to provide intelligence support for the collection by Navy field stations of information transmitted by telecommunications satellites.<sup>32</sup> In addition, Sugar Grove is situated close (60 miles) to the normal satellite receiving station in Etam.

### ***Sabana Seca, Puerto Rico (66°W, 18°N)***

NAVSECGRU was first stationed in Sabana Seca in 1952. In 1995, it was joined by the AIA, 544<sup>th</sup> IG (Detachment 2). The station has at least one satellite antenna with a diameter of 32 m and four further small satellite antennae. According to official information, the station's tasks are to perform 'satellite communication processing', to provide 'cryptologic and communications service' and to support Navy and DoD operations, including the collection of COMSAT information (from a description of the 544<sup>th</sup> IG). In the future, Sabana Seca is set to become the first field station for the analysis and processing of satellite communications.

### ***Morwenstow, England (4°W, 51°N)***

Like Yakima, Morwenstow was established in the early 1970s, at the same time as the first generation of INTELSAT satellites went into space. The British Intelligence Service (GCHQ) operates Morwenstow. The Morwenstow site houses some 21-satellite antennae, three of which have a diameter of 30 m; no details are available of the size of the other antennae. No official information has been issued regarding the station's role; however, the size and number of the satellite antennae and the location of the station, only 110 km from the telecommunications station in Goonhilly, leave no doubt as to its task of intercepting transmissions from telecommunications satellites.

### ***Menwith Hill, England (2°W, 53°N)***

Menwith Hill was established in 1956 and by 1974 already housed eight satellite antennae. Today, the figure is roughly 30, some 12 of which have a diameter of more than 20 m. At least one of the large antennae, although certainly not all, is a receiving antenna for military communications (AN/FSC-78). The British and Americans work together at Menwith Hill. The US services stationed there are NAVSECGRU, the AIA (451<sup>st</sup> IOS) and INSCOM, which has command of the station. The land on which Menwith Hill stands belongs to the UK Defense Ministry and is rented to the US Administration. According to official information, Menwith Hill's role is "to provide rapid radio relay and to conduct communications research." According to statements by Richelson and the Federation of American Scientists, Menwith Hill is both an earth station for spy satellites and an interception station for transmissions from Russian telecommunications satellites.

### ***Geraldton, Australia (114°O, 28°S)***

The station was established in the early 1990s. It is run by the Australian Secret Service (DSD), and it is partly manned by British servicemen previously stationed in Hong Kong. According to Hager, four satellite antennae, of the same size (diameter of roughly 20 m) are trained on satellites above the Indian Ocean and the Pacific. According to statements made under oath in the Australian Parliament by an expert, transmissions from civilian telecommunications satellites are intercepted at Geraldton.<sup>33</sup>

### ***Pine Gap, Australia (133°O, 23°S)***

The station in Pine Gap was established in 1966. It is run by the Australian Secret Service (DSD), and roughly half of the 900 station personnel are Americans from the CIA and NAVSECGRU. Pine Gap has 18 satellite antennae, one with a diameter of roughly 30 m and another with a diameter of roughly 20 m. According to official sources, and information provided by various authors, since its

---

inception Pine Gap has been an earth station for SIGINT satellites. Station personnel control and guide various spy satellites and receive, process and analyze their signals. The large satellite antennae also suggest that transmissions from telecommunications satellites are intercepted, since no such antennae are required for work with SIGINT satellites. Until 1980 no Australians were allowed to work in the signals analysis department; since then, they have been granted free access to all parts of the station, with the exception of the Americans own cryptography room.

### ***Misawa, Japan (141°O, 40°N)***

The station in Misawa was established in 1948 as the site for an HFDF antenna. Japanese and Americans man it. The US services represented are NAVSECGRU, INSCOM and some AIA groups (544<sup>th</sup> IG, 301<sup>st</sup> IS). The site houses around 14 satellite antennae, some of which have a diameter of roughly 20-m (estimate). Officially, Misawa acts as a “cryptology operations Center.” According to information supplied by Richelson, the station is used to intercept transmissions from the Russian Molnya satellites and other Russian telecommunications satellites.

### ***Waihopai, New Zealand (173°O, 41°S)***<sup>34</sup>

Waihopai was established in 1989. It started with one large antenna, with a diameter of 18 m, and two smaller antennae were added later. According to Hager, the antennae are trained on INTELSAT 701 in orbit above the Pacific. Official information released by the GCSB (General Communications Security Bureau) Waihopai’s task is to intercept transmissions from communications satellites and to decrypt and process the signals.<sup>35</sup> Since the station has only two satellite antennae, the New Zealand secret service can intercept only a small proportion of communications in the Pacific region. To serve any purpose, therefore, the station must work jointly with other stations in the region. Hager often names Geraldton in Australia as Waihopai’s “sister station.”<sup>36</sup>

### ***Hong Kong (22°N, 114°O)***

The station was established in the late 1970s, at the same time as the second generation of INTELSAT satellites was put in space, and was equipped with large satellite antennae. No details are available of the exact sizes. In 1994, a start was made on the decommissioning of the station; the antennae were taken to Australia. It is not clear which station (Geraldton, Pine Gap or Misawa, Japan) has taken over the Hong Kong station’s tasks, which may have been divided among several stations.

### **Further Stations**

The roles of the following stations cannot be clearly established on the basis of the criteria referred to above:

### ***Leitrim, Canada (75°W, 45°N)***

Leitrim is part of an exchange program between Canadian and US military units. According to the Navy, therefore, some 30 persons are stationed in Leitrim. In 1985 the first of four satellite antennae was installed, of which the two larger have a diameter of no more than roughly 12 m (estimate). According to official information, the station’s task is to provide “cryptologic rating” and to intercept diplomatic communications.

### ***Bad Aibling, Germany (12°O, 47°N)***

At present roughly 750 Americans work at the station near Bad Aibling. INSCOM (66th IG, 718<sup>th</sup> IG) which has the command, NAVSECGRU, and various AIA groups (402ndIG, 26th IOG) are stationed in Bad Aibling. The station has 14 satellite antennae, none of which has a diameter of more than 18 m. According to official information, Bad Aibling has the following tasks: “Rapid Radio Relay and Secure Common, Support to DoD and Unified Commands, Medium and Longhand Common HF & Satellite, Communication Physics Research, Test and Evaluate Common Equipment.” According to Richelson, Bad Aibling

---

is an earth station for SIGINT satellites and a listening station for transmissions from Russian telecommunications satellites. In accordance with a Department of Defense decision, the station is to be closed on 30 September 2002. Personnel will be transferred to other units.<sup>37</sup>

### ***Ayios Nikolaos, Cyprus (32°O, 35°N)***

Ayios Nikolaos on Cyprus is a British station. The station, which has 14 satellite antennae whose size is unknown, is manned by two units, the 'Signals Regiment Radio and the Signals Unit (RAF)'. The station's location, close to the Arab states, and the fact that Ayios Nikolaos is the only station sited within certain footprints (above all spot beams) in this area, point to its having an important role in intelligence gathering.

### ***Shoal Bay, Australia (134°O, 13°S)***

Shoal Bay is a station run solely by the Australian Intelligence Service. The station reportedly has 10 satellite antennae; no official information is available regarding their size. Of the satellite antennae visible on photographs, the five larger ones have a maximum diameter of 8 m, and the sixth antenna visible is smaller still. According to information provided by Richelson, the antennae are trained on the Indonesian PALAPA satellites. It is not clear whether the station is part of the global system for the interception of civilian communications.

### ***Guam, Pacific (144°O, 13°S)***

Guam was established in 1898. It now houses a Naval Computer and Telecommunications Station manned by the 544<sup>th</sup> IG of the AIA and Navy soldiers. The station has at least four satellite antennae, two of which have a diameter of roughly 15-m.

### ***Kunia, Hawaii (158°W, 21°N)***

NAVSECGRU and the AIA have operated this station since 1993 as a Regional Security Operations Center (RSOC). Its tasks include the

provision of information and communications and cryptological support. Its broader role is not clear.

### ***Buckley Field, Denver, Colorado, USA (104°W, 40°N)***

The station was established in 1972 and is home to the 544<sup>th</sup> IG (Detachment 45). The site houses at least six satellite antennae, four of which have a diameter of roughly 20-m. The station's official task is to collect, process and analyze data about nuclear events obtained by SIGINT satellites.

### ***Medina Annex, Texas, USA (98°W, 29°N)***

Like Kunia, Medina, which was established in 1993, is an RSOC operated by NAVSECGRU and AIA units with tasks in the Caribbean.

### ***Fort Gordon (81°W, 31°N)***

Fort Gordon is also an RSOC, operated by INSCOM and the AIA (702<sup>nd</sup> IG, 721<sup>st</sup> IB, 202<sup>nd</sup> IB, 31<sup>st</sup> IS), whose tasks are unclear.

### ***Fort Meade, USA (76°W, 39°N)***

Fort Meade is the headquarters of the NSA.

The following conclusions can be drawn from the information collected concerning the stations and satellites and from the requirements outlined above:

1. In each footprint there are interception stations which cover at least some of the global beams and are equipped with at least one antenna with a diameter greater than 20 m. They are stations which are operated by the Americans or British or where American or British servicemen carry out intelligence activities.
2. The expansion of INTELSAT communications and the establishment, at the same time, of the corresponding interception stations show that the system is intended to provide global coverage.
3. According to official information, some of these stations have the task of intercepting transmissions from communications satellites.

- 
4. The information regarding stations contained in the declassified documents can be regarded as proof of the existence and activities of the stations concerned.
  5. Some stations are located in the areas covered by the beams or spots of several satellites, so that a large proportion of the relevant communications can be intercepted.
  6. There are some other stations, which, although they have no large antennae, may also be part of the system, since they can receive communications from the beams and spots. In this case, evidence other than the size of the antennae must be adduced.
  7. Some of the stations are situated in immediate proximity to normal earth stations for telecommunications satellites.

### **The UKUSA Agreement**

A SIGINT agreement signed in 1948 between the United Kingdom, the United States and Australia, Canada and New Zealand is referred to as the UKUSA Agreement.<sup>38</sup> The UKUSA Agreement represents a continuation of the cooperation between the USA and the UK, which dates back to the First World War and which became very close during the Second World War.

It was the Americans who instigated the establishment of a SIGINT alliance at a meeting with the British in London in August 1940.<sup>39</sup> In February 1941, US code breakers delivered a cipher machine (PURPLE) to the United Kingdom. Cooperation in the sphere of code breaking began in spring 1941.<sup>40</sup> Intelligence cooperation was stepped up in response to the joint fleet operations in the North Atlantic in summer 1941. In June 1941 the British broke the German fleet code, ENIGMA.

America's entry into the war led to SIGINT cooperation being stepped up. In 1942, US code breakers from the Naval SIGINT Agency began work in the United Kingdom.<sup>41</sup> Liaison between the submarine tracking rooms in London, Washington and, from May 1943 onwards, Ottawa in Canada was so close that, according to a

statement by one individual involved at the time, they worked like a single organization.<sup>42</sup>

In spring 1943 the BRUSA-SIGINT Agreement was signed, and personnel were exchanged. The agreement primarily concerns the division of work and its main substance is summarized in the first three paragraphs: they cover the exchange of all information obtained by means of the discovery, identification and interception of signals and the cracking of codes and encryption processes. The Americans were primarily responsible for Japan, the British for Germany and Italy.<sup>43</sup>

Following the war, the UK was the prime mover behind the continuation of a SIGINT alliance. The foundations were laid in the course of a world tour undertaken in spring 1945 by British intelligence agents, including Sir Harry Hinsley. One aim was to transfer SIGINT personnel from Europe to the Pacific to take part in the war against Japan. In that connection, an agreement was reached to provide the Australian intelligence services with resources and personnel (British). The intelligence agents returned to the USA via New Zealand and Canada.

In September 1945 Truman signed a top-secret memorandum whose provisions formed the cornerstone of a peacetime SIGINT alliance.<sup>44</sup> Immediately thereafter, negotiations on an agreement opened between the British and Americans. In addition, a British delegation made contact with the Canadian and Australians with a view to discussing their involvement.

In February and March 1946 a top-secret Anglo-American SIGINT conference took place at which the details of an alliance were discussed. The British were authorized by the Canadians and Australians to act on their behalf. The conference produced what was still a classified agreement, running to some 25 pages, which laid down the detailed arrangements for a SIGINT agreement between the United States and the British Commonwealth. Further discussions took place during the two following years, culminating in the signing of the definitive text of the UKUSA Agreement in June 1948.<sup>45</sup>

---

For a long time, the signatory states refused officially to acknowledge the existence of the UKUSA Agreement. However, the annual report of the Intelligence and Security Committee, the UK's parliamentary monitoring body refers explicitly to the agreement: "The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ."<sup>46</sup>

A publication of the New Zealand Department of the Prime Minister from the year 2000, dealing with the management of the New Zealand's security and intelligence services, also refers clearly to the agreement: "The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) Australia's Defense Signals Directorate (DSD) and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own."<sup>47</sup> Moreover, there is further evidence of the agreement's existence.

According to the US Navy,<sup>48</sup> UKUSA stands for "United Kingdom-USA" and refers to a "5-nation SIGINT agreement."

The Head of the Australian Intelligence Service (DSD) confirmed the existence of the agreement in an interview: according to the information he gave, the Australian Secret Service cooperates with other overseas intelligence agencies under the UKUSA Agreement.<sup>49</sup>

A Canadian Security and Intelligence Committee report describes how Canada cooperates with some

of its closest and longest-standing allies in the intelligence sphere. The report names the allies concerned: the United States (NSA), the United Kingdom (GCHQ), Australia (DSD) and New Zealand (GCSB). The report does not name the agreement.

In an interview with Christopher Andrew, a professor at Cambridge University, conducted in November 1987 and April 1992, the former Deputy Director of the NSA, Dr Louis Torella, who was present when the agreement was signed, confirmed that it does exist.<sup>50</sup>

The former Head of GCHQ, Joe Hooper, refers to the UKUSA Agreement in a letter of 22 July 1969 to the former Director of the NSA, Marshall S. Carter.

Under the 1966 Freedom of Information Acts (5 USC § 552) and the Department of Defense's 1997 FOIA Regulation 5400.7-R, formerly classified documents were declassified and thus made available to the public.

The documents concerning the National Security Archive, founded in 1985 at George Washington University in Washington DC, are accessible to the public. The author Jeffrey Richelson, a former member of the National Security Archive, has published 16 documents on the Internet which give an insight into the emergence, development, management and mandate of the National Security Agency (NSA).<sup>51</sup>

In two of these documents, ECHELON is named. These documents have repeatedly been cited by various authors writing about ECHELON as evidence for the existence of the ECHELON global espionage system. The documents made available by Richelson also include some which confirm the existence of the National Reconnaissance Office and its function as a manager and operator of intelligence satellites.<sup>52</sup> Following our conversation with Jeffrey Richelson in Washington he forwarded further declassified documents to the Temporary Committee. Those relevant to our investigations have been taken into account here.

---

The documents contain fragmentary descriptions of or references to the following topics:

- In National Security Council Intelligence Directive 9 (NSCID 9) of 10 March 1950 the term foreign communications is defined for COMINT purposes: it comprises any government communications in the widest sense (not only military) and all other communications, which might contain information of military, political, scientific or economic value.
- The Directive (NSCID 9 rev, 29.12.1952) expressly states that the FBI alone is responsible for internal security.
- The Department of Defense (DoD) Directive of 23 December 1971 on the NSA and the Central Security Service (CSS) outlines the concept for the NSA as follows:
  - The NSA is a separately organized office within the DoD headed by the Secretary of Defense;
  - The NSA's task is firstly to fulfil the USA's SIGINT mission, and secondly to provide secure communications systems for all departments and offices;
  - The NSA's SIGINT activities do not cover the production and distribution of processed intelligence: this is the sphere of other departments and offices.

The 1971 DoD Directive also sketches out the structure of the NSA and CSS. In its statement to the House Permanent Select Committee on Intelligence on 12 April 2000,<sup>53</sup> Gen. Michael Hayden, the NSA Director, defined the NSA's tasks as follows:

- Collecting foreign communications for the military and for policymakers by means of electronic surveillance;
- Supplying intelligence for US Government consumers about international terrorism, drugs and arms proliferation;
- The NSA does not have the task of collecting all electronic communications.

- The NSA may only pass on information to recipients authorized by government, not direct to US firms.

In a memorandum by Vice-Admiral W.O. Studeman of the US Navy on behalf of the Government on 8 April 1992,<sup>54</sup> reference was made to the increasingly global access of the NSA in addition to ,support of military operations.

### **Powers of the Intelligence Agencies<sup>55</sup>**

It is clear from US Signals Intelligence Directive 18 (USSID 18) that both cable and radio signals are intercepted. The duties of the US Communications Intelligence Board include monitoring all arrangements with foreign governments in the COMINT field. One of the tasks of the NSA Director is to arrange all contacts with foreign COMINT services.<sup>56</sup>

The NAVSECGRU Instructions C5450.48A<sup>57</sup> describe the duties, function and purpose of the Naval Security Group Activity (NAVSECGRUACT), 544<sup>th</sup> Intelligence Group, in Sugar Grove, West Virginia. They state that one particular task is to maintain and operate an ECHELON site; they also mention that one task is the processing of intelligence information.

In the document "History of the Air Intelligence Agency" (1 January to 31 December 1994)<sup>58</sup> the Air Intelligence Agency (AIA), Detachment 2 and 3, is mentioned under the heading, Activation of ECHELON Units.

These documents do not give any information on what an 'ECHELON site' is, what is done at an 'ECHELON site', or what the codename ECHELON stands for. These documents do not reveal anything about the UKUSA Agreement.

### **Information From Authors and Journalists**

The ECHELON system was first described in detail in the book, *Secret Powers: New Zealand's role in the international spy network*, published in 1996 by the New Zealand author Nicky Hager. He draws

---

on interviews with more than 50 persons who were employed by the New Zealand intelligence service, GCSB, or otherwise involved in intelligence activities. He also analyzed a wide range of documents from national archives, newspapers and other published sources. According to Hager, the global interception system is referred to as ECHELON, and the network computers as ECHELON Dictionaries.

According to Hager, the origins of cooperation between intelligence services under the UKUSA Agreement can be traced back to 1947, when, following their cooperation in the war, the UK and USA concluded an agreement on continuing COMINT activities on a joint basis around the globe, under which the two countries were to cooperate on the creation of an interception system providing the maximum possible global coverage, share the special installations required and the associated costs and pool the fruits of their labors. Canada, Australia and New Zealand subsequently signed up to the UKUSA agreement.

Hager says that interception of satellite communications is the core activity of the current system. The interception by ground stations of messages sent via Intel satellites began in the 1970s. The computer searches such messages for specific keywords and/or addresses in order to filter out the relevant communications. Surveillance activity was later extended to other satellites, such as those of Inmarsat,<sup>59</sup> which concentrated on maritime communications.

In his book, Hager points out that the interception of satellite communications represents only a small, albeit important, part of the eavesdropping system, for there are also numerous facilities for monitoring microwave and cable links, although these are less well documented and their existence is more difficult to prove, since, unlike ground stations, they are rather inconspicuous. ECHELON is thus synonymous with a global eavesdropping system.

In his statement to the Temporary Committee, made on 24 April 2001, Hager emphasized that the interception system was not all-powerful. Since

the limited resources had to be used as effectively as possible, not all communications could be intercepted, but rather only those likely to offer up important information. For that reason, the communications targeted were those of political and diplomatic interest. If communications were intercepted with a view to obtaining economic intelligence, the information concerned the macro—rather than the microeconomic sphere.

As far as the interception system's operating methods were concerned, each partner state had its own list of search words on the basis of which communications were intercepted. In addition, however, the USA using "dictionary managers" screened communications for keywords entered into the system. The British therefore had no control over the screening process and had no idea what information was collected in Morwenstow, since it was forwarded directly to the USA. In that connection, Hager emphasized the risk posed to continental Europe by the British interception stations.

Citing several examples, he pointed out that the UKUSA partner states were spying on allies and trading partners in the Pacific. The only countries not being spied on were the UKUSA partner states themselves. In Hager's view, like their New Zealand counterparts the British secret services would probably be very loath to call the UKUSA partnership into question by refusing to cooperate and intercept communications originating from continental Europe. There would be no reason for the United Kingdom to forfeit information of interests to its intelligence services, and, since that information would always remain secret, espionage under the UKUSA Agreement would not rule out an official policy of loyalty vis-à-vis Europe.

In his many publications the British journalist Duncan Campbell draws on the work of Hager and Richelson, on conversations with former intelligence service staff and on other research. According to his statements, ECHELON is part of the global system, which intercepts and analyses international satellite communications. Each partner state uses 'dictionary' computers, which screen the intercepted messages for keywords.

---

In STOA Study 2/5 of 1999, which provides an in-depth analysis of the technical aspects, Campbell describes in detail how any medium used for transmitting information can be intercepted. In one of his latest writings, however, he makes it clear that even ECHELON has its limits and that the initial view that total monitoring of communications was possible has turned out to be erroneous. Neither ECHELON nor the signals intelligence system of which it is part can do this. Nor is equipment available with the capacity to process and recognize the content of every speech message or telephone call.

In his statement to the Temporary Committee, made on 22 January 2001, Campbell expressed the view that the USA used its intelligence services to help US firms win contracts. Relevant information was passed on to firms via the CIA with the assistance of the Advocacy Center and the Office of Executive Support in the Department of Commerce. In support of this argument he put forward documents providing evidence of intervention by the Advocacy Center to the benefit of US firms; moreover, much of the information concerned can be found on the homepage of the Advocacy Center. The claim that the success of the Advocacy Center is based on the interception of communications is speculation and is not supported by the documents.

Campbell emphasized that the interception capabilities of several European countries (e.g. Switzerland, Denmark, France) had increased substantially in recent years. The intelligence sector had also seen an expansion in bilateral and multilateral cooperation.

The US author, Jeffrey Richelson, a former member of the National Security Archives, has made available on the Internet 16 previously classified documents, which give an insight into the inception, development, management and remit of the National Security Agency. In addition, he is the author of various books and articles on the intelligence activities of the USA.

In his work he draws on many declassified documents, the research carried out by Hager and his own research. During his meeting with the delegation from the Temporary Committee, held in Washington DC on 11 May 2001, he stated that ECHELON referred to a computer network used to filter data which was then exchanged between intelligence services. In his 1985 book "The Ties That Bind" he describes in detail the negotiations which led up to the signing of the UKUSA Agreement and the activities under that agreement of the secret services of the USA, the United Kingdom, Canada, Australia and New Zealand.

In his very comprehensive 1999 book "The US Intelligence Community" he gives a survey of the USA's intelligence activities and describes the organizational structure of the intelligence services and their methods of collecting and analyzing information. In Chapter 8 of the book he examines in detail the SIGINT capabilities of the intelligence services and describes some earth stations. In Chapter 13 he outlines the USA's relations with other intelligence services, for example under the UKUSA Agreement.

In his article entitled "Desperately Seeking Signals," which appeared in 2000, he gives brief details of the substance of the UKUSA Agreement, names installations used to intercept transmissions from communications satellites and outlines the scope for and the limits on the interception of civilian communications.

US author James Bamford, whose work is based both on archive research and the questioning of intelligence service staff, was one of the first people to tackle the subject of the NSA's SIGINT activities. As long ago as 1982 he published the book "The Puzzle Palace," chapter 8 of which, entitled "Partners," describes the UKUSA Agreement in detail. According to his new book, "Body of Secrets," which builds on the findings outlined in "The Puzzle Palace," the computer network linking the intelligence services is known as "Platform." ECHELON is the name of the software used in all the relevant stations, providing for uniform processing of data and direct access to

---

the data held by other intelligence services. In the subsequent chapters, however, he also uses the term ECHELON to denote the interception system set up under the UKUSA Agreement.

In “Body of Secrets,” and in the chapter of most relevance to the work of the Temporary Committee, entitled “Muscle,” Bamford gives a historical survey of the development of communications surveillance by the NSA and describes the scope of the system, the way the UKUSA partnership operates and its objectives. He emphasizes that, according to interviews conducted with dozens of current and former NSA employees, the NSA is at present not involved in the work of gathering competitive intelligence.

He confirmed this statement when giving evidence to the Temporary Committee on 23 April 2001. The NSA could only be given the task of gathering competitive intelligence on the basis of a clear political decision taken at the very highest level, a decision, which has thus far not been taken. In the course of 20 years’ research, Bamford had never uncovered evidence of the NSA passing on intelligence to US firms, even though it intercepts communications from private firms, for example with a view to monitoring compliance with embargoes.

According to Bamford, the main problem for Europe is not the issue of whether the ECHELON system steals firms’ business secrets and passes them on to competitors, but rather that of the violation of the fundamental right to privacy. In “Body of Secrets” he describes in detail how the protection of ‘US persons’ (i.e. US citizens and persons legally resident in the USA) has developed and makes clear that at least internal restrictions have been laid down in respect of other UKUSA residents. At the same time, he points out that other persons enjoy no protection, that there is no requirement to destroy data concerning such persons, and that the NSA’s data storage capacities are unimaginably huge.

However, Bamford also emphasizes the limits of the system, which stem from the fact that, firstly, only

a small proportion of international communications are now transmitted via satellites—transmissions via fiber optic cable are much more difficult to intercept—and secondly, that the NSA has only limited capacities when it comes to the final analysis of intercepted communications. Moreover, those capacities must be set against an ever-increasing volume of communications, transmitted in particular via the Internet.

Bo Elkjaer and Kenan Seeburg, two Danish journalists told the Temporary Committee on 22 January 2001 that ECHELON was already very advanced in the 1980s. Denmark, which greatly expanded its interception capabilities in the 1990s, has been cooperating with the USA since 1984. Echoing their article in *Ekstra Bladet*,<sup>60</sup> in which they referred to an illustrated lecture (25 slides) given by an unnamed officer of the 544<sup>th</sup> Intelligence Group of the Air Intelligence Agency, they claimed that various NGOs (including the Red Cross) were also ECHELON targets.

Margaret Newsham<sup>61</sup> was employed from 1974 to 1984 by Ford and Lockheed and says she worked for the NSA during that period. She had been trained for her work at NSA Headquarters at Fort George Meade in Maryland, USA, and had been deployed from 1977 to 1981 at Menwith Hill; the US ground station on UK territory. There she established that a conversation conducted by US Senator Strohm Thurmond was being intercepted. As early as 1978, ECHELON was capable of intercepting telecommunications messages to and from a particular person via satellite.

As regards her role in the NSA, she was responsible for designing systems and programs, configuring them and preparing them for operation on powerful computers. The software programs were named SILKWORTH and SIRE, whilst ECHELON was the name of the network.

Wayne Madsen,<sup>62</sup> former NSA employee, also confirms the existence of ECHELON. He is of the opinion that economic intelligence gathering has top priority and is used to the advantage of US companies. He fears in particular that

---

ECHELON could spy on NGOs such as Amnesty International or Greenpeace. He argues that the NSA had to concede that it held more than 1000 pages of information on Princess Diana, because her conduct ran counter to US policy, owing to her campaign against land mines. During his meeting with the committee delegation in Washington DC Madsen expressed particular concern at the risks to the privacy of European citizens posed by the global espionage system.

Mike Frost worked for more than 20 years for the CSE, the Canadian secret service.<sup>63</sup> The listening post in Ottawa was just one part of a worldwide network of spy stations.<sup>64</sup> In an interview with CBS, he said that all over the world, every day, telephone conversations, e-mails and faxes are monitored by ECHELON, a secret government surveillance network.<sup>65</sup> This also included civilian communications.

In an interview he gave for an Australian TV channel, he said by way of example that the CSE actually had entered the name and telephone number of a woman in a database of possible terrorists because she had used an ambiguous phrase in a harmless telephone conversation with a friend. When searching through intercepted communications, the computer had found the keyword and reproduced the conversation. The analyst was unsure and therefore recorded her personal details.<sup>66</sup>

The intelligence services of the UKUSA states also helped each other by spying on each other's behalf so that at least local intelligence services could not be accused of anything. For instance, GCHQ asked the CSE to spy on two British government ministers when Prime Minister Thatcher wanted it to tell her if they were on her side.<sup>67</sup>

Fred Stock says he was expelled from CSE, the Canadian secret service, in 1993 because he had criticized the new emphasis on economic intelligence and civil targets. The communications intercepted contained information on trade with other countries, including negotiations on NAFTA, Chinese purchases of cereals and

French arms sales. Stock says the service also routinely received communications concerning environmental protests by Greenpeace vessels on the high seas.<sup>68</sup>

### **Information From Government Sources**

James Woolsey, the former director of the CIA, said at a press conference<sup>69</sup> he gave at the request of US State Department, that the USA did conduct espionage operations in continental Europe. However, 95% of 'economic intelligence' was obtained by evaluating publicly accessible information sources, and only 5% came from stolen secrets. Espionage was used to secure economic intelligence from other countries where compliance with sanctions and dual-use goods were concerned, and in order to combat bribery in connection with the award of contracts. Such information is not, however, passed to US companies.

Woolsey stressed that, even if espionage yielded economically usable intelligence, it would take an analyst a very long time to analyze the large volume of available information, and that it would be wrong to use their time on spying on friendly trading partners. He also pointed out that, even if they did so, complex international interlinkages would make it difficult to decide which companies were US companies and thus should be allowed to have the information.

Answers to various questions in the House of Commons<sup>70</sup> reveal that the station at RAF Menwith Hill is owned by the UK Ministry of Defense, but is made available to the US Department of Defense, specifically the NSA,<sup>71</sup> which provides the chief of station,<sup>72</sup> as a communications facility.<sup>73</sup> In mid-2000, there were 415 US military, 5 UK military, 989 US civilian and 392 UK civilian personnel working at RAF Menwith Hill, excluding GCHQ staff present on the site.<sup>74</sup>

The presence of US military personnel is governed by the North Atlantic Treaty and special confidential<sup>75</sup> administrative arrangements appropriate to the relationship, which exists between the governments of the UK and the USA for the purposes of common defense.<sup>76</sup> The

---

station is an integral part of the US Department of Defense's worldwide network, which supports the interests of the UK, the USA and NATO.<sup>77</sup>

In the Intelligence and Security Committee's 1999/2000 annual report, emphasis is specifically placed on the value of the close cooperation under the UKUSA Agreement, as reflected in the quality of the intelligence gathered. It is pointed out in particular that when the NSA's equipment was out of action for some three days, US customers as well as UK customers were served direct from GCHQ.<sup>78</sup>

Martin Brady, Director of the Australian intelligence service DSD,<sup>79</sup> confirmed in a letter to the "Sunday" program on Australia's Channel 9 that DSD cooperated with other intelligence services as part of the UKUSA Agreement. In the same letter, he stressed that all Australia's intelligence facilities were operated by Australian services alone or jointly with US services. Where use of such facilities is shared, the Australian Government has full knowledge of all activities and Australian personnel are involved at all levels.<sup>80</sup>

A document published by the New Zealand Department of the Prime Minister in 2000, which deals with the role of the national security and intelligence services refers explicitly to the partnership between the intelligence services of the USA, the UK, Canada, Australia and New Zealand and emphasizes the benefits for New Zealand.<sup>81</sup>

On 19 January 2001, the Netherlands Minister for Defense presented a report to the Netherlands Parliament on technical and legal aspects of the global surveillance of modern telecommunications systems.<sup>82</sup> In it, the Netherlands Government takes the view that, although it had no information of its own on this matter, it was highly likely, on the basis of available third-party information, that the ECHELON network did exist, but that there were also other systems with the same capabilities. The Netherlands Government came to the conclusion that global interception of communications systems was not confined to countries involved in the

ECHELON system, but was also carried on by government authorities of other countries.

Luigi Ramponi, former director of SISMI, the Italian intelligence service, leaves no room for doubt in the interview he gave for 'Il Mondo' that ECHELON does exist.<sup>83</sup> Ramponi says explicitly that, as Head of SISMI, he knew of Echelon's existence. Since 1992, he had been kept in the picture about intensive interception of low-, medium- and high frequencies. When he joined SISMI in 1991, most dealings were with the UK and the USA.

### **Parliamentary Reports**

The Belgian monitoring committee, the Comité Permanent R, has already discussed ECHELON in two reports. The third chapter of its 1999 activity report was devoted to how the Belgian intelligence services are reacting to the possible existence of an ECHELON system of communications surveillance. The 15-page report concludes that both the Belgian intelligence services, the Sûreté de l'Etat and the Service General du Renseignement (SGR), only found out about ECHELON through documents in the public domain.

The second report deals with the ECHELON system in much greater detail. It gives a view on the STOA study and devotes one section to explaining the technical and legal background to telecommunications monitoring. It concludes that ECHELON does in fact exist and is also in a position to listen in to all information carried by satellite (approximately 1% of total international telephone communications), in that it searches for keywords, and that its decoding capacity is much greater than the Americans claim. Doubt remains about the accuracy of statements that no industrial espionage is carried out at Menwith Hill. The report makes it clear that it is impossible to ascertain with any certainty what ECHELON does or does not do.

The French National Assembly's Committee on National Defense has drawn up a report on surveillance systems. At the meeting held on 28

---

November 2000, Arthur Paecht, presented the report's findings to the Temporary Committee. Following a detailed discussion of a wide variety of aspects, Arthur Paecht came to the conclusion that ECHELON exists and is, in his view, the only known multinational surveillance system. The system's capacities are real but have reached their limits not only because the expenditure can no longer keep pace with the explosion in communications but also because certain targets now know how to protect themselves.

The ECHELON system has moved away from its original goals, which were linked to the Cold War, and this means that it is not impossible that the intelligence gathered may be used for political and industrial purposes against other NATO states. ECHELON might indeed present a danger to fundamental freedoms and in this context it raises numerous problems that demand appropriate answers. It would be wrong to imagine that the ECHELON member states will give up their activities. On the contrary, there are several indications of a new system being created with new partners as a way of acquiring additional resources to overcome Echelon's limits.

In Italy the parliamentary Committee on Intelligence and Security Services drew up a report entitled "The role of the intelligence and security services in the ECHELON case,"<sup>84</sup> which was forwarded to the President of the Italian Parliament on 19 December 2000. The conclusions concerning the existence of a system named ECHELON are vague.

According to the report, "during the hearings in committee the existence of an integrated interception system of that name, operated by the five signatory states to the UKUSA Agreement (USA, United Kingdom, Australia, New Zealand and Canada) and designed to intercept communications on a worldwide basis was largely ruled out." Although the existence of closer cooperation among the English-speaking countries was not in doubt, the committee had failed to find evidence that the cooperation was geared to the

establishment of an integrated interception system or even a worldwide interception network.

The committee felt it was likely that the name ECHELON denoted a stage reached in the development of technology for the interception of satellite communications. The report made explicitly clear that the Italian secret service SISMI had ruled out the existence of an automatic system for the recognition of words used in conversations, so that the targeted interception of conversations containing given keywords was not feasible.

### **Might There be Other Global Interception Systems?**

Listening in to international communications transmitted by first-generation satellites requires receiving stations in the Atlantic, the Indian Ocean and the Pacific area. In the case of the newer generation of satellites, which can transmit to sub-regions, further requirements with regard to the geographical position of listening stations would have to be met if all communications via satellite were to be intercepted. Any other interception system operating on a global scale would be forced to establish its stations outside the territory of the UKUSA states.

The establishment of an interception system of this kind operating on a global scale would, however, also have to make economic and political sense for the operator or operators. The beneficiary or beneficiaries of such a system would have to have global economic, military or other security interests, or at least believe that they were among the world's superpowers. Consequently, we are essentially talking only about China and the G-8 States, excluding the United States and the United Kingdom.

France has its own territories, departments and regional authorities in all three areas listed above. In the Atlantic, there is St Pierre and Miquelon east of Canada (65° W/47° N), Guadeloupe, northeast of South America (61° W/16° N), and Martinique (60° W/14° N) and French Guyana on the northeast coast of South America (52° W/5° N).

---

In the Indian Ocean there is Mayotte to the east of southern Africa (45° E/12° S) and Réunion (55° E/20° S) and to the very south the French Southern and Antarctic Territories. In the Pacific there is New Caledonia (165° E/20° S), the Wallis and Futuna Islands (176° W/12° S) and French Polynesia (150° W/16° S).

Very little information is available about possible stations operated by the French intelligence service (DGSE) in these overseas areas. According to reports by French journalists,<sup>85</sup> there are stations in Kourou in French Guyana and in Mayotte. No details are available as to the size of the stations, the number of satellite antennae or their size. There are apparently other stations in France at Domme near Bordeaux and at Alluets-le-Roi near Paris. Vincent Jauvert estimates that there are a total of 30 satellite antennae. The author, Erich Schmidt-Eenboom<sup>86</sup> claims that a station is also operating in New Caledonia and is used by the German Federal Intelligence Service.

Theoretically, since it meets the geographical, technical and financial requirements, France could also operate a global interception system. However, there is insufficient information available in the public domain to seriously assume that this is the case.

The Russian intelligence service FAPSI (Federal Agency of Government Communications and Information, Federalnoye Agentstvo Pravitelstvennoy Svyazi), which is responsible for communications security and SIGINT, operates ground stations in Latvia, Vietnam and Cuba in cooperation with the Russian military intelligence service GRU. On the basis of the relevant legal provisions, FAPSI's role is to collect political, economic, military and scientific and technological information with a view to fostering economic, military and scientific and technological development.<sup>87</sup> In addition, in 1997 the Director of FAPSI described its primary tasks as the interception of encrypted foreign communications and global interception.

In the Atlantic area, the Federation of American Scientists claims that there is a facility at Lourdes in Cuba (82° W/23° N), which is operated jointly with the Cuban intelligence service. With the aid of this station, Russia both gathers strategic intelligence and intercepts military and commercial communications. In the Indian Ocean there are stations in Russia, about which no further information is available. A further station in Skundra in Latvia was closed in 1998.

In the Pacific there is apparently a station at Cam Rank Bay in North Vietnam. No detailed information is available about the stations as far as the number and size of the antennae are concerned. Together with the stations available in Russia itself, global coverage is theoretically possible. However, here too, the information available is insufficient to draw any firm conclusions.

Neither the other G-8 states nor China has territories or close allies in the parts of the world that would enable them to operate a global interception system.

### **Compatibility of an ECHELON Type Communications Interception System With Union Law**

The committee's remit includes the specific task of examining the compatibility of an 'ECHELON' type communications interception system with Community law. In particular, it is to examine whether such a system complies with the two data protection Directives 95/46/EC and 97/66/EC, with Article 286 TEC, and Article 8(2) TEU. This matter has to be considered from two different angles.

The first arises from the circumstantial evidence, which indicates that the system known as "ECHELON" was designed as a communications interception system to provide the US, Canadian, Australian, New Zealand and British secret services with information about events abroad by collecting and evaluating communications data. As such, it

---

is a conventional espionage tool used by foreign intelligence services. Initially, therefore, we will examine the compatibility of such an intelligence system with Union law.

In addition, the STOA report by Duncan Campbell alleges that the system has been misused for purposes of obtaining competitive intelligence, causing serious losses to the industries of European countries. Furthermore, there are statements by the former CIA Director R. James Woolsey, that although the USA was spying on European firms, this was only to restore a level playing field since contracts had only been secured as a result of bribery. If it is true that the system is used to obtain competitive intelligence, the further issue arises of whether this is compatible with Community law.

In principle, activities and measures undertaken for the purposes of state security or law enforcement do not fall within the scope of the EC Treaty. On the basis of the principle of limited authority, the European Community can only take action where a corresponding competence has been conferred on it. The Community rightly excluded these areas from the scope of application of the data protection directives, which are based on the EC Treaty, and in particular Article 95 (ex-Article 100a) thereof.

Directive 59/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector do not apply to “the processing of data/activities concerning public security, defense, state security (including the economic well-being of the state when the activities relate to state security matters) and the activities of the state in areas of criminal law.”<sup>88</sup>

Exactly the same wording has been used in the proposal for a directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, which is currently before Parliament. The involvement of a Member State in an interception system for the

purposes of State security cannot therefore be in breach of the EC’s data protection directives.

Similarly, there can be no breach of Article 286 TEC, which extends the scope of the data protection directives to data processing by Community institutions and bodies. The same applies to Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. This regulation is also applicable only in so far as the bodies are acting within the framework of the EC Treaty. To avoid misunderstandings, it should be clearly emphasized at this point that no sources whatsoever contend that there is any involvement of Community bodies and institutions in a surveillance system.

As far as the areas covered by Title V (common foreign and security policy) and Title VI (police and judicial cooperation in criminal matters) are concerned, there are no data protection provisions comparable to those of the EC directives. The European Parliament has already pointed out on numerous occasions that action is much needed in this area.<sup>89</sup>

The protection of the fundamental rights and freedoms of the individual in these spheres is ensured only by Articles 6 and 7, in particular by Article 6(2) TEU, in which the Union undertakes to respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and as they derive from the constitutional traditions common to the Member States. Not only are fundamental rights, and in particular the ECHR, binding on the Member States, but the Union is also required to comply with fundamental rights in its legislation and administration. However, since at EU level there are still no regulations concerning the admissibility of the interception of telecommunications for security or intelligence purposes,<sup>90</sup> the issue of infringement of Article 6(2) TEU does not yet arise.

---

If a Member State were to promote the use of an interception system, which was also used for industrial espionage, by allowing its own intelligence service to operate such a system or by giving foreign intelligence services access to its territory for this purpose, it would undoubtedly constitute a breach of EC law. Under Article 10 TEC, the Member States are committed to acting in good faith and, in particular, from abstaining from any measure which could jeopardize the attainment of the objectives of the Treaty. Even if the interception of telecommunications is not carried out for the benefit of the domestic industry (which would, in fact, be equivalent in effect to State aid, and thus in breach of Article 87 TEC), but for the benefit of a non-member state, activities of this kind would be fundamentally at odds with the concept of a common market underpinning the EC Treaty, as it would amount to a distortion of competition.

This follows not only from the wording of the regulation as regards its scope, but also from the sense of the law. If intelligence services use their capability to gather competitive intelligence, these activities are not being carried out for the purposes of security or law enforcement but for other purposes and would consequently fall fully within the scope of the directive. Article 5 of the directive requires the Member States to ensure the confidentiality of communications. "In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users." Pursuant to Article 14, exceptions may be made only where they are necessary to safeguard national security, defense and law enforcement. As industrial espionage is no justification for an exception, it would, in this case, constitute an infringement of Community law.

To sum up, it can therefore be said that the current legal position is that in principle an ECHELON type intelligence system is not in breach of Union law because it does not concern the aspects of Union law that would be required for there to be incompatibility. However, this applies only where the system is actually used exclusively for

the purposes of state security in the broad sense. On the other hand, were it to be used for other purposes and for industrial espionage directed against foreign firms, this would constitute an infringement of EC law. Were a Member State to be involved in such action, it would be in breach of Community law. Convention on mutual assistance in criminal matters between the Member States of the European Union (OJ 2000 C 197/1, Art. 17), which regulates the conditions under which mutual assistance in criminal matters with regard to telecommunications interception is possible. These provisions in no way curtail the rights of the subjects of tapping as the Member State in which the subject is to be found has the right to refuse mutual assistance if it is not authorized under national law.

### **The Compatibility of Communications Surveillance by Intelligence Services With the Fundamental Right to Privacy**

Any act involving the interception of communications, and even the recording of data by intelligence services for that purpose,<sup>91</sup> represents a serious violation of an individual's privacy. Only in a "police state" is the unrestricted interception of communications permitted by government authorities. In contrast, in the EU Member States, which are mature democracies, the need for state bodies, and thus also intelligence services, to respect individuals' privacy is unchallenged and is generally enshrined in national constitutions. Privacy thus enjoys special protection: potential violations are authorized only following analysis of the legal considerations and in accordance with the principle of proportionality.

The UKUSA states are also well aware of the problem. However, these states' protection provisions are geared to respect for the privacy of their own inhabitants, so that as a rule European citizens do not benefit from them in any way. For example, the US provisions which lay down the conditions governing electronic surveillance do not set the state's interest in operating a properly functioning intelligence service against the interests

---

of effective, general protection fundamental rights, but rather against the need to protect the privacy of “US persons.”<sup>92</sup>

Many agreements under international law specify respect for privacy as a fundamental right.<sup>93</sup> At world level, particular mention should be made of the International Covenant on Civil and Political Rights,<sup>94</sup> which was adopted by the UN in 1966. Article 17 of the Covenant guarantees the protection of privacy. In connection with complaints submitted by other states, all the UKUSA states have complied with the decisions taken by the Human Rights Committee set up pursuant to Article 41 of the Covenant to rule on breaches of the Covenant under international law. The Optional Protocol,<sup>95</sup> which extends the powers of the Human Rights Committee to cover complaints submitted by private individuals, has not been signed by the USA, however, so that such individuals cannot appeal to the Human Rights Committee in the event of the violation of the Covenant by the USA.

At EU level, efforts have been made to establish specifically European arrangements for the protection of fundamental rights through the drafting of a Charter of Fundamental Rights of the EU. Article 7 of the Charter, entitled “Respect for private and family life,” even lays down explicitly in law the right to respect for communications.<sup>96</sup> In addition, Article 8 lays down in law the fundamental right to the “protection of personal data.” This would have protected individuals in those cases involving the (computerized or non-computerized) processing of their data, something, which generally occurs when voice communications are intercepted and invariably does when other forms of communication are intercepted.

The Charter has not yet been incorporated into the Treaty. It is binding, therefore, only on the three institutions which pledged to comply with it in the Formal Declaration adopted during the Nice European Council: the Council, the Commission and the European Parliament. They are not involved in any secret service activities. Even

when the Charter acquires full legal force through its incorporation into the Treaty, due account will have to be taken of its limited scope. Pursuant to Article 51, the Charter applies to “the institutions and bodies of the Union—and to the Member State only when they are implementing Union law.” Accordingly, the Charter would at best take effect via the ban on state aid schemes, which run counter to the principles of competition. The only effective international instrument for the comprehensive protection of privacy is the ECHR.

The protection of fundamental rights provided by the ECHR is particularly important in that the Convention has been ratified by all the EU Member States, thereby creating a uniform level of protection in Europe. The contracting parties have given an undertaking under international law to guarantee the rights enshrined in the ECHR and have declared that they will comply with the judgments of the European Court of Human Rights in Strasbourg.

The relevant national legal provisions can thus be reviewed by the European Court of Human Rights as to their conformity with the ECHR and, in the event of a breach of human rights, a judgment may be handed down against the contracting party concerned and it may be required to pay compensation. The ECHR has gained further in importance by being repeatedly invoked by the CJEC [Court of Justice of the European Communities], alongside the general legal principles adhered to by the Member States, when that body takes decisions in cases involving legal reviews. Moreover, following the adoption of the Treaty of Amsterdam Article 6(2) of the Treaty on European Union commits the EU to respecting fundamental rights as enshrined in the ECHR.

The rights enshrined in the ECHR represent generally recognized human rights and are thus not linked to nationality. They must be granted to all persons covered by the jurisdiction of the contracting parties. In other words, the human rights in question must at all events be guaranteed throughout the territory of the contracting parties, so that local exceptions would represent a breach

---

of the Convention. In addition, however, they are also valid outside the territory of the contracting parties, provided that state authority is exercised in such places. Persons outside the territory of that state thus also enjoy the rights guaranteed by the ECHR vis-à-vis a contracting state if those persons suffer interference in the exercise of their right to privacy.<sup>97</sup>

The latter point is particularly important here, since a specific characteristic of the issue of fundamental rights in the area of telecommunications surveillance is the fact that there may be a substantial geographical distance between the state responsible for the surveillance, the person under surveillance and the location in which interception is actually carried out. This applies in particular to international communications, but may also apply to national communications if information is transmitted via connections situated abroad. Indeed, this is typical of interceptions carried out by foreign intelligence services. It is also possible that information obtained by an intelligence service by means of surveillance will be passed on to other states.

Pursuant to Article 8(1) of the ECHR, “everyone has the right to respect for his private and family life, his home and his correspondence.” No explicit reference is made to the protection of telephony or telecommunications, but under the terms of the case law of the European Court of Human Rights, they are protected by the provisions of Article 8, since they are covered by the concepts of “private life” and “correspondence.”<sup>98</sup> The scope of the protection of this fundamental right covers not only the substance of the communication, but also the act of recording external data. In other words, even if the intelligence service merely records data such as the time and duration of calls and the numbers dialed, this represents a violation of privacy.<sup>99</sup>

Pursuant to Article 8(2) of the ECHR, exercise of this fundamental right is not unrestricted. Interference in the exercise of the fundamental right to privacy may be admissible if there is a legal basis under national law.<sup>100</sup> The law must be generally accessible and its consequences must be foreseeable.<sup>101</sup>

In that connection, the Member States are not free to interfere in the exercise of this fundamental right as they see fit. They may do so only for the purposes listed in the second paragraph of Article 8 of the ECHR, in particular in the interests of national security, public safety or the economic well-being of the country.<sup>102</sup> However, this does not justify industrial espionage, since it only covers forms of interference “necessary in a democratic society.” In connection with any instance of interference, the least invasive means appropriate must be employed to achieve the objective; in addition, adequate guarantees must be laid down to prevent misuse of this power.

These general principles have the following implications for the organization of the work of intelligence services in a manner consistent with this basic right: if, for the purpose of safeguarding national security, there seems to be a need to authorize intelligence services to record the substance of telecommunications, or at least external data relating to the connections in question, this power must be established in national law and the relevant provisions must be generally accessible. The consequences for individuals must be foreseeable, but due account must be taken of the particular requirements in the sphere of national security.

Accordingly, in a ruling on the conformity with Article 8 of secret checks on employees in areas relating to national security, the European Court of Human Rights noted that in this special case the arrangements governing the foreseeable requirement must differ from those in other areas.<sup>103</sup>

In this context as well, however, it stipulated that the law must at all events state under what circumstances and subject to what conditions the state may carry out secret, and thus potentially dangerous, interference in the exercise of the right to privacy.<sup>104</sup> In connection with the organization of the activities of intelligence services in a manner consistent with human rights, due account must be taken of the fact that, although national security can be invoked to justify an invasion of privacy, the principle of proportionality, as defined in Article

---

8(2) of the ECHR, also applies: national security represents valid grounds only in cases where action to protect it is necessary in a democratic society.

In that connection, the European Court of Human Rights has clearly stated that the interest of the state in protecting its national security must be weighed up against the seriousness of the invasion of an individual's privacy.<sup>105</sup> Invasions of privacy may not be restricted to the absolute minimum, but mere usefulness or desirability is not sufficient justification.<sup>106</sup> The view that the interception of all telecommunications, even if permissible under national law, represents the best form of protection against organized crime would amount to a breach of Article 8 of the ECHR.

In addition, given the specific nature of the activities conducted by intelligence services, activities, which demand secrecy and, therefore, a particularly careful weighing-up of interests, provision must be made for more stringent monitoring arrangements. The European Court of Human Rights has explicitly drawn attention to the fact that a secret surveillance system operated for the purpose of protecting national security carries with it the risk that, under the pretext of defending democracy, it may undermine or even destroy the democratic system, so that more appropriate and more effective guarantees are needed to prevent such misuse of powers.<sup>107</sup> Accordingly, the legally authorized activities of intelligence services are only consistent with fundamental rights if the ECHR contracting party has established adequate systems of checks and other guarantees to prevent the misuse of powers.

In connection with the activities of Sweden's intelligence services, the European Court of Human Rights emphasized the fact that it attaches particular importance to the presence of MPs in police supervisory bodies and to supervision by the Minister of Justice, the parliamentary Ombudsman and the parliamentary Committee on Legal Affairs. Against this background, it must be regarded as unsatisfactory that France, Greece, Ireland, Luxembourg and Spain have no parliamentary committee with responsibility for monitoring

the secret services<sup>108</sup> and have made no move to set up a supervisory system similar to the office of parliamentary Ombudsman pioneered by the Nordic states.<sup>109</sup> Your reporter therefore welcomes the efforts made by the French National Assembly Committee on National Defense to set up a monitoring committee,<sup>110</sup> particularly as France has exceptional intelligence capabilities, in both technical and geographical terms.

The contracting parties must comply with a set of conditions in order to demonstrate that the activities of their intelligence services are compatible with Article 8 of the ECHR. It is quite obvious that intelligence services cannot be allowed to circumvent these requirements by employing assistance from other intelligence services subject to less stringent rules. Otherwise, the principle of legality, with its twin components of accessibility and foreseeable would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

The first implication of this is that exchanges of data between intelligence services are permissible only on a restricted basis. An intelligence service may seek from one of its counterparts only data obtained in a manner consistent with the conditions laid down in its own national law. The geographical scope for action laid down by law in respect of the intelligence service concerned may not be extended by means of agreements with other services. By the same token, it may carry out operations on behalf of another country's intelligence service, in accordance with the latter's instructions, only if it is satisfied that the operations are consistent with the national law of its own country.

Even if the information is intended for another country, this in no way alters the fact that an invasion of privacy which could not be foreseen by the legal subject concerned constitutes a violation of fundamental rights. The second implication is that states which are ECHR contracting parties may not allow other countries' intelligence services to carry out operations on their territory if they have reason to believe that those operations are not consistent with the conditions laid down by the ECHR.<sup>111</sup>

---

By ratifying the ECHR the contracting parties undertook to subject the exercise of their sovereignty to a review of its consistency with fundamental rights. They cannot seek to circumvent this requirement by foregoing the exercise of that sovereignty. These states remain responsible for their territory and thus have an obligation to European legal subjects if the exercise of sovereignty is usurped by the activities of the intelligence services of another state.

The established case law of the European Court of Human Rights now emphasizes that the contracting parties have a duty to take positive measures to protect privacy, in order to ensure that private individuals do not violate Article 8 of the ECHR. In other words, they must take action even at a horizontal level, where private individuals are not confronted with the actions of the state, but rather of other private individuals.<sup>112</sup>

If a state allows another country's intelligence service to work on its territory, the protection requirement is much greater, because in that case another authority is exercising its sovereignty. The only logical conclusion is that states must carry out checks to ensure that the activities of intelligence services on their territory do not represent a violation of human rights.

In Bad Aibling in Germany an area of land has been declared US territory for the sole purpose of housing a satellite receiving facility. In Menwith Hill in the United Kingdom authorization has been given for the shared use of land for the same purpose. If, in these stations, a US intelligence service were to engage in the interception of non-military communications conducted by private individuals or firms from an ECHR contracting party, supervisory requirements would come into play under the ECHR. In practical terms, as ECHR contracting parties Germany and the United Kingdom are required to establish that the activities of the American intelligence services do not represent a violation of fundamental rights. This is all the more relevant because representatives of NGOs and the press have repeatedly expressed

concerns regarding the activities of the US National Security Agency (NSA).

According to information available to the committee, in Morwenstow in the United Kingdom GCHQ, working in cooperation with the NSA and in strict accordance with the latter's instructions, intercepts civilian communications and passes on the recordings to the USA as raw intelligence material. The requirement to check that interception operations are consistent with fundamental rights also applies to work carried out on behalf of third parties.

In the case of operations involving two ECHR contracting parties, both can assume, up to a certain point, that the other is complying with the ECHR. At all events, this applies until evidence emerges that an ECHR contracting party is violating the Convention on a systematic, long-term basis. Things are very different, however, in the case of the USA: it is not an ECHR contracting party and it has not made its intelligence operations subject to a similar supervisory system. There are very precise rules governing the activities of its intelligence services, in so far as those activities concern US citizens or persons legally present on US territory. However, other rules apply to the activities of the NSA abroad, and many of the relevant rules are classified and thus inaccessible to the public. A further fact gives greater cause for concern, namely that although the US intelligence service is subject to monitoring by the relevant House of Representatives and Senate committees, these committees show little interest in the activities of the NSA abroad.

There would seem to be good reason, therefore, to call on Germany and the United Kingdom to take their obligations under the ECHR seriously and to make the authorization of further intelligence activities by the NSA on their territory contingent on compliance with the ECHR. In this connection, three main factors must be considered.

1. Under the terms of the ECHR, interference in the exercise of the right to privacy may

---

only be carried out on the basis of legal rules which are generally accessible and whose implications for individuals are foreseeable. This requirement can be met only if the USA discloses to the public in Europe how and under what circumstances intelligence gathering is carried out. If incompatibilities with the ECHR emerge, US rules must be brought into line with the level of protection provided in Europe.

2. Under the terms of the ECHR, interference in the exercise of the right to privacy must be proportional and, in addition, the least invasive methods must be chosen. As far as European citizens are concerned, an operation constituting interference carried out by a European intelligence service must be regarded as less serious than one conducted by a US intelligence service, since only in the first instance is legal redress available in the national courts.<sup>113</sup> Operations constituting interference must therefore be carried out, as far as possible, by the German or UK authorities, particularly when investigations are being conducted for law enforcement purposes. The US authorities have repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes.<sup>114</sup> It should be pointed out to the Americans that all EU Member States have properly functioning criminal justice systems. If there is evidence that crimes have been committed, the USA must leave the task of law enforcement to the host countries. If there is no such evidence, surveillance must be regarded as unproportional, a violation of human rights and thus inadmissible. In other words, compliance with the ECHR can be guaranteed only if the USA restricts itself to surveillance measures conducted for the purpose of safeguarding its national security, but not for law enforcement purposes.
3. As already outlined above, in its case law the European Court of Human Rights has stipulated that compliance with fundamental rights is contingent on the existence of adequate monitoring systems and guarantees against abuse. This implies that US telecommunications surveillance operations

carried out on European territory are consistent with human rights only if the USA introduces appropriate, effective checks on such operations carried out for the purpose of safeguarding its national security or if the NSA makes its operations on European territory subject to the authority of the control bodies set up by the host state, i.e. Germany or the United Kingdom.

The conformity of US telecommunications interception operations with the ECHR can only be guaranteed and the uniform level of protection provided in Europe by the ECHR can only be maintained if the requirements set out in the three points above are met.

Although the activities of intelligence services may be covered by the CFSP [Treaty on European Union] in future, as yet no relevant rules have been drawn up at EU level, so that any arrangements to protect citizens against the activities of intelligence services can only be made under national legal systems. In this connection, the national parliaments have a dual role to play: as legislators, they take decisions on the nature and powers of the intelligence services and the arrangements for monitoring their activities.

When dealing with the issue of the admissibility of telecommunications surveillance, the national parliaments must work on the basis of the restrictions laid down in Article 8 of the ECHR, i.e. the relevant legal rules must be necessary and proportional and their implications for individuals must be foreseeable. In addition, adequate and effective monitoring arrangements must be introduced commensurate with the powers of the intelligence agencies.

Moreover, in most states the national parliament plays an active role as the monitoring authority, given that, alongside the adoption of legislation, scrutiny of the executive, and thus also the intelligence services, is the second time-honored function of a parliament. However, the Member State parliaments carry out this task in a very wide variety of differing ways, often on the basis

---

of cooperation between parliamentary and non-parliamentary bodies.

As a rule, the state may carry out surveillance measures for the purposes of enforcing the law, maintaining domestic order and safeguarding national security (*vis-à-vis* foreign intervention).<sup>115</sup> In all Member States, the principle of telecommunications secrecy may be breached for law enforcement purposes, provided that there is sufficient evidence that a crime (possibly one perpetrated under particularly aggravating circumstances) has been committed by a specific person.

In view of the seriousness of the interference in the exercise of the right to privacy, a warrant is generally required for such an action<sup>116</sup> it lays down precise details concerning the permissible duration of the surveillance, the relevant supervisory measures and the deletion of the collected data. For the purposes of guaranteeing national security and order, the state's right to obtain information is extended beyond the scope of individual investigations prompted by firm evidence that a crime has been committed.

National law authorizes the state to carry out additional measures to secure information about specific persons or groups with a view to the early detection of extremist or subversive movements, terrorism and organized crime. The relevant data is collected and analyzed by specific domestic intelligence services. Finally, a substantial proportion of surveillance measures is carried out for the purposes of safeguarding state security. As a rule, responsibility for processing, analyzing and presenting relevant information about foreign individuals or countries lies with the state's own foreign intelligence service.

In general the surveillance targets are not specific persons, but rather set areas or radio frequencies. Depending on the resources and legal powers of the foreign intelligence service concerned, surveillance operations may cover a wide spectrum, ranging from purely military surveillance of short-wave radio transmissions to the surveillance of all foreign

telecommunications links. In some Member States the surveillance of telecommunications for purely intelligence purposes is simply prohibited<sup>117</sup> in other Member States—in some cases subject to authorization by an independent commission<sup>118</sup>—it is carried out on the basis of a ministerial order,<sup>119</sup> possibly even without restriction in the case of some communication media.<sup>120</sup> The relatively broad powers enjoyed by some foreign intelligence services can be explained by the fact that their operations are targeted on the surveillance of foreign communications and thus only concern a small proportion of their own legal subjects, hence the substantially concern regarding lesser degree of misuse of their powers.

Effective and comprehensive monitoring is particularly important for two reasons: firstly, because intelligence services work in secret and on a long-term basis, so that the persons concerned often learn that they were surveillance targets only long after the event or, depending on the legal situation, not at all; and, secondly, because surveillance measures often target broad, vaguely defined groups of persons, so that the state can very quickly obtain a very large volume of personal data.

Irrespective of the form they take, all monitoring bodies naturally face the same problem: given the very nature of secret services, it is often extremely difficult to determine whether all the requisite information has in fact been provided, or whether some details are being held back. The relevant rules must therefore be framed all the more carefully. As a matter of principle, the effectiveness of the monitoring can be said to be high, and far-reaching guarantees that the interference is consistent with the law can be said to exist, if the power to order telecommunications surveillance is reserved for the highest administrative authorities, if the surveillance can be implemented only on the basis of a warrant issued by a judge and if an independent body scrutinizes the performance of the surveillance measures. In addition, on democratic and constitutional grounds it is desirable that the work of the intelligence service as a whole should be subject to monitoring

---

by a parliamentary body, in accordance with the principle of the division of powers.

In Germany, these conditions have largely been met. The responsible federal minister orders telecommunications surveillance measures at national level. Unless there is a risk that further delay may frustrate the operation, prior to the implementation of surveillance measures an independent commission not bound by government instructions (G10 Commission<sup>121</sup>) must be notified so that it can rule on the need for and the admissibility of the proposed measure. In those cases in which the German Federal Intelligence Service, FIS, can be authorized to carry out surveillance of non-cable telecommunications traffic with the aid of filtering on the basis of search terms, the Commission rules on the admissibility of the search terms as well. The G10 Commission is also responsible for checking that the persons under surveillance are notified, as required by the law, and that the FIS destroys the collected data.

Alongside this, there is a parliamentary monitoring body (PMB),<sup>122</sup> which comprises nine Members of the Bundestag and scrutinizes the activities of all three German intelligence services. The PMB has the right to inspect documents, to take evidence from intelligence service staff, to visit the premises of the services and to have information notified to it; this last right can be denied only on compelling grounds concerning access to information, if it is necessary to protect the right of privacy of third parties, or if the core area of government responsibility is concerned. The proceedings of the PMB are secret and its members are required to maintain confidentiality even after they have left office. At the halfway point and at the end of the parliamentary term, the PMB submits to the German Bundestag a report on its monitoring activities.

It must be said, however, that comprehensive, monitoring of intelligence services is the exception in the Member States. In France <sup>123</sup> for example, only those surveillance measures entailing the tapping of a cable require the authorization of the

Prime Minister. Only measures of that kind are subject to monitoring by the Commission set up for that purpose (National Commission for the Monitoring of Security-related Interceptions), whose members include an MP and a Senator. Applications for authorization to carry out an interception operation are submitted by a minister or his or her representative to the chairman of the Commission, who, if the lawfulness of the proposed operation is in doubt, may convene a meeting of the Commission, which issues recommendations and, if there are grounds for suspecting a breach of the criminal law, informs the state prosecutor's office. Measures carried out in defense of national interests, which entail the interception of radio transmissions, and thus also satellite communications, are not subject to any restrictions, including monitoring by a commission. Moreover, the work of the French intelligence services is not subject to scrutiny by a parliamentary monitoring committee; however, moves are afoot to set up such a committee. The Defense Committee of the National Assembly has already approved such a proposal<sup>124</sup> but no discussion of that proposal has yet taken place in plenary.

In the United Kingdom, every communications surveillance measure carried out on British soil requires the authorization of the Home Secretary. However, the wording of the law does not make it clear whether the non-targeted interception of communications, communications, which are then checked using keywords, would also be covered by the concept of 'interception' as defined in the Regulation of Investigatory Powers Act 2000 (RIP) if the intercepted communications were not analyzed on British soil, but merely transmitted abroad as 'raw material'. Commissioners—sitting or retired senior judges appointed by the Prime Minister carry out checks on compliance with the provisions of the RIP on an ex-post facto basis. The Interception Commissioner monitors the granting of interception authorizations and supports investigations into complaints concerning interception measures. The Intelligence Service Commissioner monitors the authorizations granted

---

for the activities of the intelligence and security services and supports investigations into complaints concerning those services.

The Investigatory Powers Tribunal, which is chaired by a senior judge, investigates all complaints concerning interception measures and the activities of the services referred to above. Parliamentary scrutiny is carried out by the Intelligence and Security Committee (ISC),<sup>125</sup> which monitors the activities of all three civilian intelligence services (MI5, MI6 and GCHQ). In particular, it is responsible for scrutinizing the expenditure and administration and monitoring the activities of the security service, the intelligence service and GCHQ. The committee comprises nine members drawn from the two Houses of Parliament; ministers may not be members. Unlike the monitoring committees set up by other states, which are generally elected by the national parliament or appointed by the Speaker of that parliament, they are appointed by the Prime Minister after consulting the Leader of the Opposition.

These examples already demonstrate clearly that the level of protection varies very substantially. As far as parliamentary scrutiny is concerned, the existence of a monitoring committee responsible for scrutinizing the activities of intelligence services is very important: in contrast to the normal parliamentary committees, they have the advantage of enjoying a higher degree of trust among the intelligence services, given that their members are bound by the confidentiality rule and committee meetings are held in camera. In addition, with a view to the performance of their special task they are endowed with special rights vital to the monitoring of activities in the intelligence sector. Most of the EU Member States have set up a separate parliamentary monitoring committee to scrutinize the activities of the intelligence services. In Belgium,<sup>126</sup> Denmark,<sup>127</sup> Germany,<sup>128</sup> Italy,<sup>129</sup> the Netherlands,<sup>130</sup> and Portugal,<sup>131</sup> there is a parliamentary monitoring committee responsible for scrutinizing both the military and civilian intelligence service. In the United Kingdom<sup>132</sup> the special monitoring committee scrutinizes only

the admittedly much more significant activities of the civilian intelligence services; the military intelligence service is monitored by the normal defense committee.

In Austria<sup>133</sup> the two arms of the intelligence service are dealt with by two separate monitoring committees, which are, however, organized in the same way and endowed with the same rights. In the Nordic states Finland<sup>134</sup> and Sweden<sup>135</sup> parliamentary scrutiny is carried out by Ombudsmen, who are independent and elected by parliament. France, Greece, Ireland, Luxembourg and Spain have no special parliamentary committees; in these countries, the standing committees, as part of their general parliamentary work, carry out monitoring tasks.

The situation for European citizens in Europe is unsatisfactory. The powers of national intelligence services in the sphere of telecommunications surveillance differ very substantially in scope, and the same applies to the powers of the monitoring committees. Not all those Member States, which operate an intelligence service, have also set up independent parliamentary monitoring bodies endowed with the appropriate supervisory powers. A uniform level of protection is still a distant objective.

From a European point of view, this is all the more regrettable, because this state of affairs does not primarily affect the citizens of the Member States concerned, who can influence the level of protection by means of their voting behavior in elections. Nationals of other states feel the adverse impact above all since foreign intelligence services, by their very nature, carry out their work abroad. Individuals are essentially at the mercy of foreign systems, and here the need for protection is greater still. It must also be borne in mind that, by virtue of the specific nature of intelligence services, EU citizens may be affected by the activities of several such services at the same time. In this context, a uniform level of protection consistent with democratic principles would be desirable. Consideration should also be given to the issue of

---

whether data protection provisions in this sphere would be workable at EU level.

Moreover, the issue of the protection of European citizens will be placed in an entirely new context when, under a common security policy, the first moves are made towards cooperation among the Member States' intelligence services. Citizens will then look to the European institutions to adopt adequate protection provisions. The European Parliament, as an advocate of constitutional principles, will then have the task of lobbying for the powers it needs, as a democratically elected body, to carry out appropriate monitoring. In this connection, the European Parliament will also be required to establish conditions under which the confidential processing of sensitive data of this kind and other secret documents by a special committee whose members are bound by a duty of discretion can be guaranteed. Only once these conditions have been met will it be realistic, and, with a view to effective cooperation among intelligence services to press for these monitoring rights.

### **Protection Against Industrial Espionage**

The information held by firms falls into three categories as far as the need for secrecy is concerned. Firstly, there is information, which is deliberately disseminated as widely as possible. This includes technical information about a firm's products (e.g. specifications, prices, etc.) and promotional information which has a bearing on a firm's image. Secondly, there is information, which is neither protected nor actively disseminated, because it has no bearing on a firm's competitive position. Examples include the date of the works outing, the menu in the works canteen or the make of fax machine used by a firm. Finally, there is information, which is protected against third parties. The information is protected against competitors, but also, if a firm intends to break the law (tax provisions, embargo rules, etc.), against the state. There are various degrees of protection, culminating in strict secrecy, e.g. in the case of research findings prior to the registration of a patent or armaments production.<sup>136</sup> In the case under discussion here, espionage involves

obtaining information kept secret by a firm. If the assailant is a rival firm, the term used is competitive intelligence. If the assailant is a state intelligence service, the relevant term is industrial espionage.

Strategic information relevant to espionage against firms can be classified according to sectors of the economy or the departments of individual firms. It is perfectly obvious that information in the following sectors is of particular interest: biotechnology, genetic technology, medical technology, environmental technology, high-performance computers, software, opto-electronics, image sensing and signaling systems, data storage systems, industrial ceramics, high-performance alloys and nano-technology. The list is not comprehensive and changes constantly in line with technological developments. In these sectors of industry, espionage primarily involves stealing research findings or details of special production techniques.

The following departments are logical espionage targets: research and development, procurement, personnel, production, distribution, sales, marketing, product lines and finance. The significance and value of such information is often underestimated.

The strategic position of a firm on the market depends on its capabilities in the following spheres: research and development, production procedures, product lines, funding, marketing, sales, distribution, procurement and personnel.<sup>137</sup> Information on these capabilities is of major interest to any of the firm's competitors, since it gives an insight into the firm's plans and weaknesses and enables rivals to take strategic countermeasures.

Some of this information is publicly available. There are highly specialized consultants, including such respected firms as Roland & Berger in Germany, which draw up, on an entirely legal basis, analyses of the competitive position on a given market. In the USA competitive intelligence has now become a standard management tool. Professional analysis can turn a wide range of

---

individual items of information into a clear picture of the situation as a whole.

The transition from legality to a criminal act of competitive intelligence is bound up with the choice of means used to obtain information. Only if the means employed are illegal under the laws of the country concerned do efforts to obtain information become a criminal act—the provision of analyses is not in itself punishable under the law. Naturally enough, information of particular interest to competitors is protected and can only be obtained by criminal means. The techniques employed for this purpose are in no way different from general espionage methods.

No precise details are available concerning the scale of competitive intelligence operations. As in the case of conventional espionage, the official figures represent only the tip of the iceberg. Both parties concerned (perpetrator and victim) are keen to avoid publicity. Espionage is always damaging to the image of the firms concerned and the assailants naturally have no interest in public light being shed on their activities. For that reason, very few cases come to court. Nevertheless, reports dealing with competitive intelligence repeatedly appear in the press. The conclusion to be drawn is that cases of competitive intelligence repeatedly come to light, but do not determine firms' day-to-day behavior.

In view of the high number of unrecorded cases, it is difficult to determine precisely the extent of the damage caused by competitive intelligence/ industrial espionage. In addition, some of the figures quoted are inflated because of vested interests. Security firms and counterintelligence services have an understandable interest in putting the losses at the high end of the realistically possible scale. Despite this, the figures do give some idea of the problem.

As early as 1988, the Max Planck Institute estimated that the damage caused by industrial espionage in Germany amounted to at least DM 8 billion.<sup>138</sup> The chairman of the association of security consultants in Germany, Klaus-Dieter Matschke, quotes a figure

of DM 15 bn a year, based on expert evidence. The President of the European police trade unions, Hermann Lutz, puts the damage at DM 20 bn a year. According to the FBI,<sup>139</sup> US industry suffered losses of US\$ 1.7 bn as a result of competitive intelligence and industrial espionage in the year's 1992/1993. The former chairman of the Secret Service monitoring committee of the House of Representatives in the USA has spoken of losses of US\$ 100 bn sustained through lost contracts and additional research and development costs. It is claimed that between 1990 and 1996 this resulted in the loss of 6 million jobs.<sup>140</sup>

Basically the exact scale of the losses is irrelevant. The state has an obligation to combat competitive intelligence and industrial espionage using the police and counterintelligence services, irrespective of the level of damage to the economy. Similarly, decisions taken by firms on the protection of information and counterespionage measures cannot be based on total damage figures. Every firm has to calculate for itself the maximum possible damage as a result of the theft of information, assess the likelihood of such events occurring and compare the potential losses with the costs of security. The real problem is not the lack of accurate figures for the overall losses, the position is rather that such cost/benefit calculations are rarely carried out, except in large firms, and consequently security is disregarded.

According to a study by the auditors Ernest Young LLP,<sup>141</sup> 39% of industrial espionage is carried out on behalf of competitors, 19% for clients, 9% for suppliers and 7% for secret services. Company employees carry out espionage, private espionage firms paid hackers and secret service professionals.<sup>142</sup>

According to the literature examined, the expert evidence presented to the committee there is a consensus that the greatest risk of espionage arises from disappointed and dissatisfied employees. As employees of the firm, they have direct access to information, can be recruited for money and will spy on their employer to obtain industrial secrets for those who hire them. Major risks also arise when employees change jobs. Today it is not necessary to copy mountains of paper in order to

---

take important information out of the firm. Such information can be stored on diskettes unnoticed and taken to the new employer when employees change job.

The number of firms specializing in espionage is on the increase. Former members of the intelligence services sometimes work in these firms. Frequently the firms concerned also operate as security consultants and as detective agencies employed to obtain information. In general, the methods used are legal but there are also firms, which employ illegal means.

Hackers are computer specialists with the knowledge to gain access to computer networks from the outside. In the early days, hackers were computer freaks who got a kick out of breaking through the security devices of computer systems. Nowadays there are contract hackers in both the services and on the market.

### **Intelligence Services**

Since the end of the Cold War, the focus of the intelligence services' work has shifted. International organized crime and economic data are among their new tasks.

According to information provided by the counterintelligence authorities and by the heads of security of large firms, all tried and tested intelligence service methods and instruments are used for the purposes of industrial espionage. Firms have a more open structure than military and intelligence service facilities or government entities. In connection with industrial espionage, they are therefore exposed to additional risks: the recruitment of employees is simpler, as the facilities available to industrial security services cannot be compared to those of the counter-intelligence authorities; workplace mobility means that important information can be taken around on a laptop.

The theft of laptops or the secret copying of hard disks after hotel room break-ins is thus one of the standard methods of industrial espionage; it is

easier to break into firm's computer networks than those of security-sensitive State bodies, as small and medium-sized firms in particular have much less developed security awareness and security precautions; local tapping of communications is also easier for the same reasons. Evaluation of the information gathered on these matter shows that industrial espionage is mainly carried out locally or through mobile workstations, with a few exceptions where the information sought cannot be obtained by intercepting international telecommunications networks.

After the end of the Cold War, intelligence service capacity was released and it can now be used more than before in other areas. The United States readily admits that some of its intelligence service's activities also concern industry. This includes, for example, monitoring of the observance of economic sanctions, compliance with rules on the supply of weapons and dual-use goods, developments on commodities markets and events on the international financial markets. The US services are not alone in their involvement in these spheres, nor is there any serious criticism of this.

Criticism is leveled when state intelligence services are misused to put firms within their territory at an advantage in international competition through espionage. A distinction has to be made here between two cases.<sup>143</sup>

Highly developed industrial states can indeed gain advantage from industrial espionage. By spying on the stage of development reached in a specific sector, it is possible to take foreign trade and subsidy measures either to make domestic industry more competitive or to save subsidies. Another focus of such activities may be efforts to obtain details of particularly valuable contracts.

Some of these states are concerned to acquire technological know-how to enable their own industry to catch up without incurring development costs and license fees. The aim may also be to acquire product designs and production methods in order to be able to compete on the world market with copies produced more cheaply by virtue of

---

lower wages. There is evidence that the Russian intelligence services have been instructed to carry out such tasks. The Russian Federation's Law No 5 on foreign intelligence specifically mentions obtaining industrial and scientific/technical information as one of the intelligence service's tasks.

Another group of states—Iran, Iraq, Syria, Libya, North Korea, India and Pakistan—is concerned to acquire information for their national arms programs, particularly in the nuclear sector and in the area of biological and chemical weapons. A further aspect of the activities of the services of these states is the operation of front companies, which can purchase dual-use goods without raising suspicion.

The strategic monitoring of international telecommunications can produce useful information for industrial espionage purposes, but only by chance. In fact, sensitive industrial information is primarily to be found in the firms themselves, which means that industrial espionage is carried out primarily by attempting to obtain the information via employees or infiltrators or by breaking into internal computer networks. Only where sensitive data is sent outside via cable or radio (satellite) can a communications surveillance system be used for industrial espionage. This occurs systematically in the following three cases:

1. In connection with firms, which operate in three time zones, so that interim results are sent from Europe to America and then on to Asia;
2. in the case of videoconferences in multinational companies conducted by VSAT or cable;
3. when important contracts have to be negotiated locally (construction of facilities, telecommunications infrastructure, rebuilding of transport systems, etc.), and the firm's representatives have to consult their head office.

If firms fail to protect their communications in such cases, interception can provide competitors with valuable data.

There are some cases of industrial espionage and/or competitive intelligence, which have been described in the press or in the relevant literature.

Some of these sources have been analyzed and the results are summarized in the following table. Brief details are given of the persons involved, when the cases occurred, the detailed issues at stake, the objectives and the consequences. It is noticeable that sometimes a single case is reported in very different ways. One example is the Enercom case, in connection with which either the NSA, or the US Department of Commerce or the competitor, which took the photographs, is described as the “perpetrator.”

Case	Who	When	What	How	Aim	Consequence	Source
Air France	DGSRE	Until 1994	Conversation Between traveling businessmen	Bus were discovered in the first class cabins of Air France aircraft—public apology by company	Obtaining information	Not stated	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz?” von Arno Schutze, 1/98
Airbus	NSA	1994	Information on an order for aircraft concluded between Airbus and the Saudi Arabian airline	Interception of faxes and telephone calls between the negotiating parties	Forwarding of info to Airbus’s American competitors-Boeing and McDonnell-Douglas	Americans won the contract (US \$6 bn)	“Antennen gedreht,” Wirtschafts-woche Nr. 46/ 9 Nov 2000
Airbus	NSA	1994	Contract with Saudi Arabia worth US\$6 bn uncovering of bribes paid by the European Airbus Consortium	Interception of faxes and telephone calls, routed via tele-communications, satellites, between Airbus Consortium and the Saudi Arabian national airline/ Government	Uncovering of bribes	McDonnell-Douglas, Airbus’ competitor, won the contract	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Market Manager	Not stated	Description of the process of a raw material for skin creams by BASF (cosmetics division)	Not stated	Not stated	None, because the attempt was discovered	“Nicht gerade zimperlich,” Wirtschafts-woche Nr. 43/ 16 October 1992
Federal German Ministry of Economic Affairs	CIA	1997	Information concerning high-tech products held by the Federal Ministry of Economic Affairs	Use of an agent	Obtaining information	Agent unmasked and expelled from country	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98

Case	Who	When	What	How	Aim	Consequence	Source
Federal Ministry of Economic Affairs	CIA	1997	Background to the Mykonos trial in Berlin, Hermes loads concerning exports to Iran, setting up of German firms supplying high-tech products to Iran	CIA agent disguised as US Ambassador holds friendly conversations with the Head of the Department in the Federal Ministry of Economic Affairs responsible for the Arab region (particular responsibility: Iran)	Obtaining Information	Not stated Civil servant contacts the German security authorities, who inform the Americans that the CIA operations are unwelcome. CIA agent then “withdrawn”	Industrial espionage. Firms as a target for foreign intelligence services, Badem-Wurttemberg Constitutional Protection Agency, Stuttgart as at 1998
Dasa	Russian Intel Service	1996-1999	Purchase and forwarding of armaments-related documents drawn up by a Munich arms firm (according to SZ of 20.05.2000: arms firm Dasa in Ottobrunn)	2 Germans working on behalf of the Russians	Obtaining information on guided missiles, armaments systems (anti-tank and anti-aircraft missiles)	SZ.30.05.2000 “(...) Betrayal of secrets ‘not particularly serious’ from a military point of view. The court ruled that this also applied to the economic damage suffered.”	“Anmerkungen zur Sicherheitslage der deutschen Wirtschaft,” ASW: Bonn, April 2001  “Haftstrafe wegen Spionage für Russland, SZ/ 30 May 2000
Embargo	FIS	Around 1990	Resumption of exports of embargoed technology to Libya (e.g. by Siemens)	Interception of telephone calls	Uncovering illegal arms and technology transfer	No particular consequences, deliveries not prevented	“Maulwürfe in Nadelstreifen,” Andreas Foster, p 110
Enercon	Wind power expert from Oldenburg and Kentech employee	Not stated	Wind-power plant developed by Enercon, a firm located in Aurich	Not stated	Not stated	Not stated	“Anmerkungen zur Sicherheit der deutschen Wirtschaft,” ASW: Bonn, April 2001
Enercon	NSA	Not stated	Wind wheel for electricity generation, developed by Aloys Wobben, an engineer from East Frisia	Not stated	Forwarding of technical details to Wobben’s wind wheel to a US firm	US firm patents the wind wheel before Wobben: Wobben taken to court by US lawyers (breach of patent rights)	“Aktenkrieger,” SZ, 29 March 2001

Case	Who	When	What	How	Aim	Consequence	Source
Enercon	US firm Kene-tech Wind-power	1994	Important details of a high-tech wind-powered electricity generating plant (from switch gears to sails)	Photographs	Successful patent application in the USA	Enercon abandons plans to attack the US market	“Sicherheit muss künftig zur Chefsache werden,” HB/ 29 August 1996
Enercon	Engineer W. from Oldenburg, and US firm Kene-tech	March 1994	Type E-40 wind powered electricity generator developed by Enercon	Engineer W. passes on details, Kenetech employee photographs the plant and electrical components	Kenetech: seeking evidence for later (1995) legal action vs. Enercon for breach of patent rights Enercon: industrial espionage TV news man claims ex NSA employee told him detailed info about Enercon obtained using Enercon and passed to Kenetech by USA	Not stated	“Klettern für die Konkurrenz” SZ 13 October 2000
Enercon	Kene-tech Wind-power	Before 1996	Data concerning Enercon’s wind-powered electricity generating plant	Kenetech engineers photograph the plant	Kenetech copies the plant	Enercon vindicated: legal action brought against spy: estimated loss: several hundred million DM	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98.
Japanese Trade Ministry	CIA	1996	Negotiations on import quotas for US cars on the Japanese market	Hacking into computer system of the Japanese Trade Ministry	US negotiator Mickey Kantor should accept lowest offer	Kantor accepts lowest offer	“Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98
Japanese cars	US Govt	Not stated	Negotiations on the import of Japanese luxury cars. Info on the emissions standards of Japanese cars	COMINT, no detailed information	Obtaining information	No details	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA by Duncan Campbell

Case	Who	When	What	How	Aim	Consequence	Source
Lopez	NSA	Not stated	Videoconference involving VW and Lopez	Interception from Bad Aibling	Forwarding of info to General Motors and Opel	Interception Op allegedly provided the State Prosecutor's Office with "very detailed evidence" for its investigation	Bundeswehr Captain Erich Schmidt-Eenboom, quoted in "Wenn Freunde spionieren" <a href="http://www.zdf.msnbc.de/nes/54637.asp?cp1=1">www.zdf.msnbc.de/nes/54637.asp?cp1=1</a>
Lopez	Lopez and three of his staff	1992-1993	Papers and info concerning research, planning, manufacturing and purchasing (documents concerning a plant in Spain, cost info for various model ranges, project studies purchasing and saving strategies)	Collecting information	Use of General Motors documents by VW	In the wake of legal action, the firms settle out of court. In 1996, Lopex resigns as VW manager. In 1997 VW dismisses three further members of the Lopez teams, pays US \$100 m to General Motors/Opel (supposedly lawyers' fees) and over a seven-year period purchases spare parts from GM/Opel for a total of US\$ 1 billion	Industrial espionage. Firms as a target for foreign intelligence services, Baden-Wurttemberg Constitutional Protection Agency, Stuttgart as at 1998
Lopez	NSA	1993	Videoconference between Jose Ignacio Lopez and VW boss Ferdinand Piech	Videoconference recorded and forwarded to General Motors	Protection of commercial secrets held by GM in America, secrets which Lopez wished to pass on to VW (price lists, secret plans for a new car plant and a new small car)	Lopez's cover is blown, in 1998 criminal proceedings are halted in return for payment of fines. No consequences in respect of NSA	"Antennen gedreht," Wirtschafts-woche Nr 46 / 9 November 2000 "Abgehört," Berliner Zeitung, 22 January 1996 "Die Affare Lopez ist beendet." Wirtschafts-spiegel, 28 July 1998. "Wirtschafts-spionage: Was macht eigentlich die Konkurrenz? Von Arno Schutze, 1/98

Case	Who	When	What	How	Aim	Consequence	Source
Los Alamos	Israel	1988	Two employees of the Israel nuclear research program hack into the central computer of the Los Alamos nuclear weapons laboratory	Hacking	Obtaining information about new fuses for US atomic weapons	No specific consequences since the hackers fled to Israel. One is briefly held in custody in Israel, links with the Israeli Secret Service are not officially confirmed	“Maulwurfe in Nadelstreifen,” Andreas Foster, p. 137
Smuggling	FIS	1970s	Smuggling of computers into the GDR	Not stated	Uncovering of technology transfer to the Eastern Bloc	No particular consequences, deliveries not prevented	“Maulwurfe in Nadelstreifen,” Andreas Foster, p. 113
TGV	DGSE	1993	Cost calculation by Seimens Contract to supply high-speed trains to South Korea	Not stated	Lower price offer	Manufacturer of the ICE loses the contract to Alcatel-Alsthom	“Wirtschafts-spionage: Was macht eigentilch die Konkurrenz? Von Arno Schutze, 1/98
TGV	Not known	1993	Cost calculations by AEG and Seimens concerning a government contract to supply South Korea with high-speed trains	Seimens claims that the telephone and fax connections in its Seoul office are being tapped	Negotiating advantage for the Anglo-French competitor GEC Alsthom	South Korea decides in favor of GEC Alsthom, although the German offer was initially regarded as better	“Abgehört,” Berliner Zeitung, 22 January 1996
Thomson-Alcatel v Raytheon	CIA/ NSA	1994	Award to the French firm Thomson-Alcatel of a Brazilian contract for the satellite monitoring of the Amazon Basin (US\$ 1.4 bn)	Interception of communications to and from the successful tenderer Thomson-Alcatel	Uncovering corruption (payment of bribes)	Clinton complains to the Brazilian Government; under pressure from the USG, the contract is awarded to the US firm Raytheon	“Maulwurfe in Nadelstreifen,” Andreas Forster, p. 91
Thomson-Alcatel v Raytheon	US Dept of Commerce ‘made effort’	1994	Negotiations on a project worth billions of dollars concerning the radar monitoring of the Brazilian rainforest	Not stated	Win Contract	The French firms Thomson CSF and Alcatel lose the contract to the US firm Raytheon	“Antennen gedreht,” Wirtschafts-woche Nr 46 / 9 November 2000

Case	Who	When	What	How	Aim	Consequence	Source
Thomson-Alcatel v Raytheon	NSA Depart of Com- merce		Negotiations concerning a project worth US\$ 1.4 bn concerning the monitoring of Amazon Basin (SIVA) Discovery that the Brazilian selection panel had accepted bribes. Comment by Campbell: Raytheon supplies equipment for the Sugar grove interception station	Surveillance of the negotiations between Thomson-CSF and Brazil and forwarding of the findings to Raytheon Vcorp	Uncovering bribery Winning of the contract	Raytheon wins the contract	“Development of Surveillance Technology and Risk of Abuse of Economic Information,“ Vol 2/5 10 1999 STOA, von Duncan Campbell
Thyssen	BP	1990	Gas and oil drilling contract in the North Sea worth millions of dollars	Interception of faxes sent by the successful tendered (Thyssen)	Uncovering corruption	BP brings an action for damages against Thyssen	“Maulwurfe in Nadelstreifen,“ Andreas Forster, p. 92
VW	Not known	‘recent years’	Not stated	Inter alia, infrared camera, fixed in a mound of earth, which transmits images by radio	Obtaining information about new developments	VW admits losses of profits totalling hundreds of millions of deutschmarks	“Sicherheit muss kunftig zur Chefsache werden,“ HB / 29 August 1996
VW	Not known	1996	VW test circuit in Ehra-Lessien	Hidden camera	Information about new VW models	Not stated	“Auf Schritt und Tritt“ Wirtschaftswoche nr 25, 11 June 1998

---

The legal systems of all the industrialized countries define the theft of commercial secrets as a criminal offence. As in all other areas of the criminal law, the degree of protection varies from country to country. As a rule, however, the penalties for industrial espionage are much less severe than those for espionage in connection with military security. In many cases, competitive intelligence operations are banned only against firms from the same country, but not against foreign firms abroad. This is also the case in the USA.

In essence, the relevant laws prohibit only espionage by one industrial undertaking against another. It is doubtful whether they also restrict the activities of state intelligence services, since, on the basis of the laws establishing them, the latter are authorized to steal information. A gray area develops if intelligence services seek to pass on to individual firms' information gained by means of espionage. The laws, which endow intelligence services with special powers, would normally not cover such activities. In particular, in the EU this would represent a breach of the EEC Treaty.

Irrespective of this fact, however, in practice it would be very difficult for a firm to seek legal protection by bringing an action before the courts. Interception operations leave no trace and generate no evidence, which might be used in court.

States accept the fact that intelligence services, in keeping with their general objective of securing strategic information, are also active in the commercial sphere. However, this gentlemen's agreement is frequently breached in connection with competitive intelligence operations designed to benefit a country's own industry. Any state caught red-handed comes under massive political pressure. This applies in particular to a world power such as the USA, whose claim to global political leadership would be drastically undermined. Middle-ranking powers could probably afford to be singled out for such activities; a superpower certainly cannot.

Alongside the political problems, there is also the practical issue of which individual firm is

to be provided with the information gained by means of competitive intelligence operations. In the aerospace sector, the answer is a simple one, because only two major firms dominate the global market. In all other cases where a market is supplied by a number of firms, which are not state-controlled, it is extremely difficult to give preference only to one. In connection with international contract-award procedures, an intelligence service is more likely to forward detailed information concerning other competitors' offers to all the participating firms from its own country, rather than simply to one. This applies in particular when all the participating firms from one country can draw on the same level of government support, as is the case in the USA through the work of the Advocacy Center. In the case of the theft of technology, which should necessarily lead to the registration of a patent, it is only logical that such equal treatment would no longer be possible. Moreover, under the US political system in particular this would give rise to a serious problem. US politicians are massively dependent on contributions from firms in their constituencies to finance their election campaigns. If proof were to emerge of even one case of intelligence services favoring individual firms, the upheaval in the political system would be massive. As the former CIA Director James Woolsey put it in a discussion with representatives of the committee: "In that case the Hill—i.e. the US Congress—would go mad!" Quite!

Since 1990, the US Administration has increasingly come to equate national security with economic security. The annual White House report entitled, National Security Strategy repeatedly emphasizes that economic security is fundamental not only to our national interests, but also to national security. This development can be traced back to a number of sources. Essentially, three factors came together:

1. The interest of the intelligence services in taking on a task which would outlive the Cold War;
2. The US State Department's simple acknowledgement of the fact that, following the

- 
- Cold War, the USA's leading role in the world could not be based solely on military strength, but also made economic strength essential;
3. President Clinton's interest, from a domestic policy point of view, in strengthening the US economy and creating jobs.

This combination of interests had practical consequences.

As a logical response, since 1992, the FBI has focused its counterintelligence activities on industrial espionage and, in 1994, it set up an Economic Counterintelligence Program. Speaking to the US Congress, Louis J. Freeh, the Director of the FBI, described this as a defensive program designed to prevent the competitiveness of the US economy from being undermined by the theft of information.

As a logical response, at least from an American point of view, the Administration has used the CIA, and subsequently the NSA, to prevent distortions of competition by means of bribery. The former Director of the CIA, James Woolsey, made this explicitly clear at a press conference he gave on 7 March 2000 at the request of the US State Department.<sup>144</sup> As a logical response, the US Department of Commerce has focused its efforts to foster exports in such a way that a US firm wishing to export goods need only deal with one agency. Active use is made of all the weapons at the Administration's disposal.

Intelligence operations directed against the US economy are neither unusual nor new. For decades, both the USA and other leading industrialized countries have been targets for industrial espionage. During the Cold War, however, economic and technological intelligence gathering took second place to conventional espionage. Following the end of the Cold War, industrial espionage has come into its own.<sup>145</sup>

In 1996, speaking to the US Congress, the Director of the FBI, Louis J. Freeh, gave a detailed account of the way the US economy has become a target for industrial espionage by other countries'

intelligence agencies. As he put it, consequently foreign governments, through a variety of means, actively target US persons, firms, industries and the US Administration itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage. However, the theft of information by Americans was increasing just as much. The further remarks made by Mr. Freeh to the US Congress are summarized below.

At this point, your reporter would like to express regret at the fact that the US Administration did not allow a delegation from the Temporary Committee to discuss these issues with the FBI. Up-to-date information could then have been obtained. In the paragraphs, which follow, therefore, your reporter has assumed that the US Administration takes the view that the hearing before the House of Representatives held in 1996 gives an accurate picture of the threat currently posed to the US economy by industrial espionage. Accordingly, he has drawn extensively on that source.

At the time of the hearing, the FBI was investigating persons or organizations from 23 countries, which were suspected of industrial espionage against the USA. Some ideological or military opponents of the USA have merely continued their Cold War activities.<sup>146</sup> In contrast, other governments carry out industrial and technological espionage, even though they have long been the USA's military and political allies. In so doing, they often exploit their ease of access to US information. Some have developed agencies, which assess information concerning high-technology products and use that information in competition with US firms. No countries have actually been named, although the involvement of Russia, Israel and France has been hinted at.<sup>147</sup>

High-technology products and the defense industry are given as priority objectives. Interestingly enough, the FBI names information concerning bids, contracts, clients and strategic information in these areas as objectives of industrial espionage, which are pursued aggressively.<sup>148</sup>

---

In the context of the Economic Counterintelligence Program, the FBI has identified a series of espionage methods. A combination of methods is employed in most cases, a single method only rarely. According to the information obtained by the FBI, the best source is a person employed by a firm or organization, something, which is not only true for the USA. At the hearing, the FBI outlined how persons are used to carry out for espionage, but astonishingly gave no details of electronic methods.

At a press conference<sup>149</sup> and in a conversation with members of the committee in Washington, the former Director of the CIA, James Woolsey, briefly summarized the interception activities of the US Secret Service as follows:

1. The USA monitors international telecommunications in order to obtain general information about economic developments, shipments of dual-use goods and compliance with embargoes.
2. The USA monitors on a targeted basis communications by individual firms in connection with contract-award procedures in order to prevent corruption-related distortions of competition to the detriment of US firms. Questioned more closely, however, Woolsey gave no specific examples.

US firms are banned by law from paying bribes and accountants are required to report evidence of such payments. If a telecommunications surveillance operation reveals evidence of bribery in connection with public contracts, the US ambassador makes representations to the government of the country concerned. However, US firms competing for the contract are not directly informed. He categorically ruled out the possibility of espionage solely for the purposes of obtaining competitive intelligence.

At a hearing before the House Permanent Select Committee on Intelligence held on 12 April 2000, the current Director of the CIA, George J. Tenet, echoed Woolsey's comments: It is not the policy nor the practice of the United States to engage in espionage that would provide an unfair advantage

to US companies. At the same hearing, Tenet went on to say that information on the payment of bribes was forwarded to other government agencies so that they could help US firms.<sup>150</sup> In response to a supplementary question from Congressman Gibbons, Tenet admitted that there was no legal ban on the gathering of competitive intelligence; however, he saw no need for such a ban, given that the intelligence services were not involved in activities of that kind. In the course of a conversation held with him in Washington, the chairman of the House Permanent Select Committee on Intelligence, Porter Goss, painted a similar picture of US interception activities.

### **Legal Situation With Regard to the Payment of Bribes to Public Officials<sup>151</sup>**

The payment of bribes to secure contracts is a worldwide, and not simply European, phenomenon. According to the Bribe Payers Index (BPI) published by Transparency International in 1999, which ranks the 19 leading exporting countries on the basis of their willingness to offer bribes, Germany and the USA share ninth place. Sweden, Austria, The Netherlands, the United Kingdom and Belgium were identified as being less likely to offer bribes; only Spain, France and Italy have a higher rating.<sup>152</sup>

The Americans refer to the corrupt practices employed by European firms to justify industrial espionage. This is questionable, not only because wrongdoings by individual firms cannot justify the comprehensive use of espionage. Such heavy-handed practices could only be tolerated if there were a legal vacuum in this area.

However, the legal measures taken to combat corruption are just as stringent in Europe as they are in the USA. In 1997, these shared interests led to the adoption of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The Convention requires the signatory states to make the payment of bribes to a foreign public official a criminal offence and contains, alongside a definition of the offence of bribery, provisions concerning penalties, jurisdiction and enforcement.

---

The Convention, which came into force on 15 February 1999, has been transposed and ratified by all the EU Member States except Ireland. The USA transposed the Convention by adopting the 1998 International Anti-Bribery and Fair Competition Act amending the Foreign Corrupt Practices Act (FCPA) of 1977, which imposes on firms a requirement to keep accounts and prohibits the payment of bribes to foreign public officials.<sup>153</sup> Neither in the USA nor in the EU Member States are bribes accepted as tax-deductible operating expenditure.<sup>154</sup> Whereas the OECD Convention is designed only to combat the payment of bribes to foreign public officials, in 1999 the Council of Europe adopted two more far-reaching agreements, although neither has yet come into force.

The Criminal Law Convention on Corruption<sup>155</sup> also encompasses bribery in the private sector. It was signed by all the EU Member States except Spain and by the USA, but as yet has been ratified only by Denmark. The Civil Law Convention on Corruption<sup>156</sup> lays down rules governing liability and compensation, stipulating in particular those contracts and contract clauses, which require firms to pay bribes, will be deemed null and void. All the EU Member States except the Netherlands, Portugal and Spain have signed it; the USA has not signed.

The EU has adopted two further legal acts designed to combat bribery: the Convention on the fight against corruption involving officials and the Joint Action on corruption in the private sector. The Convention on the fight against corruption involving officials of the European Communities or officials of the EU Member States<sup>157</sup> is designed to ensure that corruption and the payment of bribes to officials are criminal offences throughout the EU. The Member States undertake to make both the payment of bribes to an official and corruption criminal offenses, regardless of whether one of their own officials, an official of another Member State or an EU official is involved.

The Joint Action on corruption in the private sector<sup>158</sup> is intended to ensure that corruption and the payment of bribes to firms are criminal offences.

In that connection, criminal law penalties are laid down for both natural and legal persons. However, the scope of the Joint Action is more restricted than that of the Convention on the fight against bribery involving officials in that it requires the Member States only to punish actions carried out at least in part on their territory. Member States are free to extend this jurisdiction to cover actions carried out abroad by their own nationals or to the benefit of domestic legal persons. Germany and Austria have made instances of corruption carried out abroad criminal offences provided that they are also punishable in the country concerned.

By means of Executive Order 12870, in 1993 President Clinton set up the Trade Promotion Coordinating Committee (TPCC).<sup>159</sup> Its role is to coordinate and develop a strategy for the US Administration's trade promotion policy. In accordance with the Executive Order, a representative of the National Security Council (NSC) also sits on the TPCC.<sup>160</sup> The NSC formulates the United States' national security policy with reference to domestic policy, foreign policy, military and intelligence issues. Each president alters the focus of the NSC's work. On 21 January 1993, by means of PDD2, President Clinton expanded the NSC and, at the same time, placed more emphasis on economic issues in connection with the formulation of security policy. Members of the NSC include the President, the Vice-President, the Secretary of State and the Secretary of Defense. The Director of the CIA is an advisory member.

The Advocacy Center, which is attached to the US Department of Commerce, is at the heart of the national export strategy employed by President Clinton and continued by President Bush. It acts as the interface between the TPCC and the US economy. By its own account, since its inception in 1993 the Center has helped hundreds of US firms to win public contracts abroad. The Advocacy Center helps US businesses by:<sup>161</sup>

- marshalling the resources of the US Administration - from the various financing, regulatory, country and sector experts, through

---

the worldwide network of commercial officers, to the White House;

- fighting to level the playing field and promote open competition in the international bidding arena—from the multibillion dollar infrastructure project to the strategic contract for a small business;
- pursuing deals on behalf of US companies from start to finish, through ‘hands-on’ support;
- supporting US jobs and boosting US exports through the successes of US companies who successfully bid for overseas projects and contracts;
- assisting US firms with stalled negotiations due to foreign government inaction or “red tape.”

Only the Director and a small staff complement of 12 people work at the Advocacy Center<sup>162</sup> itself—situation as at 6 February 2001. The project managers cover the following areas: Russia and the newly independent countries; Africa, East Asia and the Pacific; the Middle East and North Africa; South Asia—Bangladesh, India, Pakistan, Sri Lanka; Europe and Turkey; China, Hong Kong and Taiwan—Canada, the Caribbean and Latin America; the aerospace, automobile and defense industries worldwide; and the telecommunications, IT and computer industries worldwide.

The Center provides firms with a central contact point for their dealings with the various US authorities involved in promoting exports. It works on behalf of firms on a non-discriminatory basis, but, in line with the clear rules governing its work, supports only projects, which are in the US national interest. For example, projects manufactured in the USA must make up at least 50% of the value of the goods delivered under any given contract.

Duncan Campbell submitted to the members of the Temporary Committee a number of declassified documents, which provide evidence of CIA involvement in the work of the Advocacy Center. They include minutes of the Trade Promotion Coordinating Committee dealing with a meeting of the Indonesia Working Group held in July and August 1994.<sup>163</sup> According to the documents, a number of CIA staff members sit on the Working

Group, whose task is to draw up a trade strategy for Indonesia. The CIA staff members are named in the minutes. Moreover, the minutes show that one of the CIA staff members defines one objective of the Working Group as that of identifying main competitors and making this background information available to firms.<sup>164</sup>

The US Administration did not allow the discussion arranged between members of the Temporary Committee and representatives of the Center to take place. For that reason, two areas of doubt could not be cleared up:

- the Temporary Committee has in its possession documents which provide evidence of CIA involvement in the work of the TPCC;
- in its own information brochure (quoted above), the Advocacy Center acknowledges that it focuses the resources of 19 “US government agencies.” Elsewhere in the brochure, however, only 18 such agencies are listed, raising the issue of why the 19<sup>th</sup> cannot be named in public.

## Security of Computer Networks

Nowadays, alongside the use of spies, hacking into computer networks or the theft of data from laptop computers represents the second most effective method of industrial espionage. The information here has no direct bearing on the existence or otherwise of a global system for the interception of international communications. However, in view of the Temporary Committee’s aims, the chapter on industrial espionage must include brief details of one of its most powerful tools. This will certainly help readers to assess the significance of a system for the interception of international communications in connection with industrial espionage.

Modern electronic data-processing technologies have been in common use by firms for some time now. Data of all kinds is stored in highly compressed form on a variety of media. Data stored on computer has now become one of the key aspects of commercial know-how. This transition from an industrial to an information society is

---

opening up new opportunities, but, at the same time, creating substantial security risks.<sup>165</sup>

The new risks, which are emerging, can be summarized as follows:<sup>166</sup>

- More and more firms have computer networks and more and more information is being condensed in one place, with the result that it can be copied simply by hacking into the network. At the same time, other sensitive items of information are being decentralized and are thus not easily accessible in the context of a centralized security management strategy.
- The mobility of senior managers, who carry sensitive information with them on their laptop computers, is creating additional risks. The outsourcing of services is giving rise to new maintenance practices in the IT sphere as well which are highly questionable from a security point of view.
- A combination of the low status accorded to security staff in firms' management hierarchy and senior managers' ignorance of security issues is giving rise to misguided decisions.

Nowadays, firms' business secrets are stored in a physically very small area on compressed media. As a result, for example, the full plans for a new factory can be smuggled out of a firm on a substitute hard disk the size of a cigarette packet or copied electronically in minutes, without leaving any trace, by hacking into a computer network.

In the era of large-scale computers, it was easy to monitor access to secret information, since only one computer was involved. Today, each employee connected to the network is provided with substantial computing capacity at his or her workstation. This is of course a great advantage for the staff member concerned, but a disaster from a security point of view.

In the era of hand-drawn plans and mechanical typewriters it was very difficult to copy large numbers of documents without being detected. Today, in the electronic era, it is easy. Large volumes of digitized information can be copied

easily, quickly and without leaving any trace. As a result, in many cases only one intervention is needed to obtain the material in question and the risk of being detected are correspondingly much lower.

Often without being properly aware of the fact, senior managers often carry strategically important information about their firms with them on their laptop computers. The speed with which a copy of the hard disk can be made in the course of a "customs check" or a search of a hotel room offers intelligence services substantial opportunities for action. Alternatively, the Notebook in question is simply stolen. Moreover, in view of the decentralization involved it is difficult to incorporate into a central security management strategy the information stored on the hard disks of laptop computers used by a firm's senior managers.

Although outsourcing may serve to reduce a firm's costs, in the sphere of information technology and the maintenance of telephone networks it allows technicians from outside the firm virtually unrestricted access to information. The associated risks cannot be over-emphasized.

Alongside security loopholes in the software itself, which hackers repeatedly find, the most serious danger stems from network administrators who are not properly aware of the risks. In its basic form, Windows NT is configured in such a way that it reveals almost all the information required for a successful attack on the network.<sup>167</sup> If these configurations and standard passwords are not changed, accessing the network is child's play. Firms often make the mistake of investing considerable amounts of time and money in the security of the firewall, but fail to protect the network properly against attacks from within.<sup>168</sup>

The number of instances of computer networks being hacked into via the Internet is increasing every year.<sup>169</sup> In 1989, the Computer Emergency Response Team (CERT), an organization set up in the USA in 1988 with the aim of improving Internet security, received notification of 132 security problems. In 1994, the figure had already

---

risen to 2241 and in 1996 it reached 2573. The real figure is certainly much higher. This assumption was backed up by a large-scale simulation, which the US Department of Defense carried out using its own computers. Systematic efforts were made to hack into 8932 servers and mainframe computers from outside. In 7860 cases these attempts proved successful, only 390 attempts were detected and no more than 19 cases were reported.

A distinction must be drawn between attacks and security problems. An attack is a single attempt to gain unauthorized access to a system. A security problem consists of a number of related attacks. Extrapolating from their own long-term studies, the Pentagon and US universities have posited a figure of 20000 security problems and 2 million attacks on the Internet annually.

The aim of foreign intelligence services, which attack IT systems, is to secure the information they contain, if at all possible without being detected. In principle, a distinction can be drawn between three groups of perpetrators with three different *modi operandi*.

A spy who has been smuggled into a firm or whose services have been bought and who has risen to become a systems administrator or security administrator in a computer center need only make extensive use of the powers officially granted to him in order to steal virtually all his employer's know-how. The same applies to a senior development engineer with unrestricted access authorization to all a firm's databanks. A spy of this kind offers maximum espionage effectiveness. However, if suspicions arise, the risk of detection is high, since the investigations immediately focus on the small group of persons who have comprehensive access to information. Moreover, it is pure coincidence if a spy secures comprehensive access authorization.

A spy working within a firm has a clear advantage over a hacker attacking from the outside: he must overcome only the network security precautions, but no firewall. From an individual workstation, and provided that the person concerned has

the requisite knowledge, the architecture of the network can be established and substantial volumes of information can be obtained, using the same techniques employed by an outside hacker and other techniques available only to persons working from within.<sup>170</sup> In addition, the spy can converse with colleagues without raising suspicion and obtain passwords by means of "social engineering." The effectiveness of such a spy can be high, but is not as predictable as in the first case. The risk of detection is lower, particularly in the case of networks whose administrator pays little attention to the dangers of an attack from within. It is much easier to smuggle in a spy trained to hack into computer networks (trainees, guest researchers, etc.).

That hackers repeatedly gain unauthorized access to computer networks is well known and well documented. Intelligence services themselves now train specialists in the skills needed to hack into computer networks. The effectiveness of such an attack cannot be predicted or planned; it depends to a great extent on the effectiveness of the network defense mechanisms and on whether, for example, the network used by the research department is physically linked to the Internet. The level of risk involved for a professional spy is virtually zero; even if the attack is detected, the spy is somewhere else entirely.

As things stand, awareness of the risk of industrial espionage is not very well developed in individual firms. This is partly reflected in the fact that security officers often have middle- management rank and are not board members. However, security costs money and board members generally take an interest in security issues only when it is too late. Large firms do at least have their own security departments and employ security specialists in the IT sphere as well. In contrast, small and medium-sized firms vary rarely employ security experts and are generally happy enough if their data-processing equipment works properly. However, such firms as well may be targets for industrial espionage, since many of them are highly innovative. Moreover, in view of their integration in the production process medium-

---

sized component suppliers offer a suitable basis for industrial espionage operations against large firms.

As a rule, researchers are interested only in their area of expertise and can therefore sometimes be an easy target for intelligence services. Your reporter has noted with some amazement that research institutes whose work has obvious practical applications communicate with each other using unencrypted e-mails and the science network. This is quite simply reckless.

Information concerning preparations for decisions by the European Central Bank (ECB) could be of great value to intelligence services—and, it goes without saying, of course to the markets. At a meeting held in camera, the committee heard statements by representatives of the ECB concerning the security precautions taken to protect information. On that basis, your reporter has come to the conclusion that the ECB is aware of the risks and, as far as is feasible, is taking appropriate security measures. However, he has been supplied with information suggesting that risk-awareness is low in certain national central banks.

Prior to the appointment of the High Representative for the common foreign and security policy, the Council focused its efforts in the area of secrecy on measures to keep information concerning decision-making procedures and the stances adopted by the Member State governments from the public and the European Parliament. It would have had no defense against a professional intelligence operation.<sup>171</sup> For example, an Israeli firm apparently carried out technical maintenance in the interpreting booths. The Council has now adopted security regulations<sup>172</sup> consistent with the standard within NATO.

Up to now, the European Parliament has never dealt with classified documents and therefore has no experience in the area of the protection of secrecy and no security culture. The need for such a culture will only arise if Parliament gains access to classified documents in the future. Otherwise, a general policy of secrecy is anathema for a parliament whose actions must be as transparent

as possible. However, with a view to protecting informants and petitioners, provision should be made for the encryption of e-mails transmitted from one Member's office to another. At present, this is not possible.

The European Commission has directorates-general, which by virtue of the information they deal with have no need for secrecy rules or protection arrangements. Indeed, the reverse is true: complete transparency should be the norm in all areas, which have a bearing on legislation. The European Parliament must employ a vigilant approach in order to ensure that, in these areas, the influence exerted on legislative proposals by interested firms, etc. is not masked even more than it already is through the unnecessary introduction of inappropriate secrecy rules.

Admittedly, there are areas of the Commission's work, which involve the processing of sensitive information. Alongside Euratom, the most obvious areas are foreign relations, foreign trade and competition. On the basis of the information supplied by the directorates-general concerned to the committee at a meeting held in camera, and above all on the basis of other information, it is very doubtful as to whether the European Commission is properly aware of the risk of espionage and whether it takes a professional approach to the issue of security. Naturally enough, a public report is no place in which to outline security shortcomings. Nevertheless, there is a pressing need for the European Parliament to consider this issue in an appropriate manner.

However, it can be stated now that the encryption systems, which the Commission employs when communicating with some of its external offices, are outdated. This does not mean that the security standard is poor. However, the equipment currently in use is no longer manufactured and only roughly half of the external offices are equipped with encryption technology. The introduction of a new system working on the basis of encrypted e-mails is an urgent necessity.

---

## Cryptography as a Means of Self-Protection

Every time a message is transmitted, there is a risk of its falling into unauthorized hands. To prevent outsiders ascertaining its content in such cases, the message must be made impossible for them to read or intercept, i.e. encrypted. Consequently encryption techniques have been used since time immemorial for military and diplomatic purposes.<sup>173</sup>

In the past 20 years the importance of encryption has increased, since an ever greater proportion of communications has been sent abroad, where the confidentiality of post and telecommunications could not be guaranteed by the state of origin. Moreover, the expanded technical opportunities for the state legally to intercept/record communications on its own territory has led to concern among ordinary citizens and a greater need for their protection.

Finally, the increased interest among criminals in having illegal access to information, and the ability to falsify it, has also given rise to protection measures (e.g. in the banking sector). The invention of electrical and electronic communications (telegraph, telephone, radio, telex, fax and Internet) greatly simplified the transmission of intelligence communications and made them immeasurably quicker. The downside was that there was no technical protection against interception or recording, so that anyone with the right equipment could read the communication if he could gain access to the means of communication. If done professionally, interception leaves little or no trace. This imparted a new significance to encryption. It was the banking sector, which first regularly used encryption to protect communications in the new area of electronic money transfers. The growing internationalization of the economy led to communications in this field, too, being at least partly protected by cryptography. The widespread introduction of completely unprotected communications through the Internet also increased the need for private individuals to protect their messages from interception.

In the context of this report, then, the question arises as to whether there are cheap, legal, sufficiently secure and user-friendly methods of encrypting communications, which can protect the individual against interception.

The principle of encryption is to convert a plain text into an encrypted text in such a way that it has either no meaning or a different meaning from the original, but can be converted back to the original by those in the know. For example, a meaningful sequence of letters can be transformed into a meaningless sequence, which no outsider understands. This is done according to a given method (encryption algorithm) based on the transposition and/or the substitution of letters. The encryption method (algorithm) is not nowadays kept secret. On the contrary, a worldwide invitation to tender was recently issued for a new global encryption standard for use in industry.

The same was done for the creation of a specific encryption algorithm as hardware in a machine (e.g. an encrypted fax machine). What is really secret is the key to the code. This can be best explained by analogy. It is generally public knowledge how door locks work, not least because patents are held on them. Individual doors are protected by the fact that several different keys can exist for a particular type of lock. The same goes for the encryption of information: many different messages may be protected using individual keys, kept secret by those involved, on the basis of one publicly known encryption method (algorithm).

To explain these terms, we may use the example of the Caesarean encryption. Julius Caesar encrypted messages simply by replacing each letter with the letter three places further on in the alphabet (A became D, B became E, etc.). The word ECHELON would thus become HFKHORQ. The encryption algorithm thus consists of the shifting of letters within the alphabet, and the key in this particular case is the instruction to move the letters three places in the alphabet. Both encryption and decryption are done in the same way: by moving letters three places: a symmetrical process.

---

Nowadays this type of process would not provide protection for as much as a second!

A good encryption system may perfectly well be publicly known and still be regarded as secure. For this purpose, however, the number of possible keys needs to be so large that it is not possible to try all the keys (known as a brute force attack) in a reasonable time, even using computers. However, a large number of possible keys do not necessarily imply secure encryption if the method results in an encrypted text which gives clues to its decryption (e.g. the frequency of particular letters).<sup>174</sup> Caesar's encryption is thus an insecure system for both reasons. Because it uses simple substitution, the varying frequency of letters in a language means that the procedure can quickly be cracked; moreover, since there are only 26 letters in the alphabet, there are only 25 possible letter shifts and thus only 25 possible keys. In this case, then, the code breaker could very quickly find the key by trying all the possibilities and decipher the text. If an encryption system is required to be secure this may mean one of two things. Either it may be essential and susceptible of mathematical proof that the message is impossible to decipher without the key. Or it may be sufficient for the code to be unbreakable at the present state of technology and thus in all probability to meet the security requirement for far longer than the critical period during which the message needs to be kept secret.

At present the only absolutely secure method is the one-time pad. This system was developed towards the end of the First World War,<sup>175</sup> but was also used later for the telex hot line between Moscow and Washington. The concept consists of a key comprising a non-repeating row of completely random letters. Both sender and recipient encrypt using these rows, and destroy the key as soon as it has been used once. Since there is no internal order within the key, it is impossible for a cryptanalyst to break the code. This can be mathematically proven.<sup>176</sup>

The drawback to this process is that it is not easy to generate large numbers of these random keys,<sup>177</sup> and that it is difficult and impractical to find a secure

means of distributing the key. In normal business transactions, therefore, this method is not used.

Even before the invention of the one-time pad, cryptographic processes were developed, which could generate a large number of keys and thus produce coded texts which contained as few regularities in the text as possible and thus few starting-points for code breaking. In order to make these methods sufficiently fast for practical application, machines were developed for encryption and decryption. The most spectacular of these was probably Enigma,<sup>178</sup> used by Germany in the Second World War. The small army of decryption experts working at Bletchley Park in England succeeded in cracking the Enigma code by means of special machines known as bombs. Both the Enigma machine and the bombs were mechanical in operation.

The invention of the computer represented a breakthrough in cryptography, since its power made it possible to use increasingly complex systems. Even though it did not alter the basic principles of encryption, a number of changes took place. Firstly, the level of potential complexity of the encryption system was multiplied, since it was no longer subject to the constraints of what was mechanically feasible, and, secondly, the speed of the encryption process rose drastically. In computers, information is processed digitally using binary numbers. This means that the information is expressed by the sequence of two signals 0 and 1. In physical terms 1 corresponds to an electric current or magnetic field (light on), while 0 means the absence of current or magnetic field (light off).

ASCII<sup>179</sup> standardization now prevails, whereby each letter is represented by a seven-figure combination of 0 and 1.<sup>180</sup> A text therefore appears as a sheet of 0s and 1s, and instead of letters it is numbers that are encrypted. Both transposition and substitution can be used in this process. Substitution may, for example, take place by the addition of a key in the form of any row of numbers. According to the rules of binary mathematics the sum of two equal figures is zero ( $0+0=0$  and  $1+1=0$ ) while the sum of two different

---

figures is 1 (0+1=1). The new, encrypted row of figures arising from the addition of the key is thus a binary sequence, which can either be further digitally processed or made readable again by subtracting the added key.

The use of computers made it possible to generate coded texts, using powerful encryption algorithms, which offer practically no starting-points for code breakers. Decryption now entails trying all possible keys. The longer the key, the more likely it is that this attempt will be thwarted, even using very powerful computers, by the time it would take. There are therefore usable methods, which may be regarded as secure at the present state of technology.

As computers became more widely available in the 1970s, the need for the standardization of encryption systems grew ever more urgent, since only in this way could firms communicate securely with business partners without incurring disproportionate costs. The first moves were made in the USA. Powerful encryption systems can also be used for unlawful purposes or by potential military opponents; they may also make electronic espionage difficult or impossible. For that reason, the NSA urged that firms should be offered a sufficiently secure encryption standard, but one which the NSA itself could decrypt, by virtue of its exceptional technical capabilities. With that aim in mind, the length of the key was restricted to 56 bits. This reduces the number of possible keys to 100 000 000 000 000 000.<sup>181</sup> On 23 November 1976 Horst Feistel's so-called Lucifer key was officially adopted in its 56-bit version under the name Data Encryption Standard (DES) and for the next 25 years represented the official US encryption standard.<sup>182</sup>

This standard was also adopted in Europe and Japan, in particular in the banking sector. Media claims to the contrary, the DES algorithm has not yet been broken, but hardware now exists, which is powerful enough to try all possible keys (brute force attack). In contrast, Triple DES, which has a 112-bit key, is still regarded as secure. The successor to DES, the Advanced Encryption

Standard (AES), is a European process,<sup>183</sup> which was developed under the name Rijndael in Louvain, Belgium. It is fast and is regarded as secure, since it incorporates no key-length restriction. The reason for this lies in a change in US policy on cryptography. Standardization makes it much easier for firms to employ encryption. What remained, however, was the problem of key exchange.

As long as a system works with a key, which is employed both for encryption and decryption (symmetric encryption), it is difficult to use with large numbers of communication partners. The key must be handed over to every new communication partner in advance in such a way that no third party gains access to it. This is difficult for firms in practical terms, and feasible for private individuals only in rare cases.

Asymmetric encryption offers a solution to this problem: two different keys are used for encryption and decryption. The message is encrypted using a key, which may perfectly well be in the public domain, the so-called public key. However, the process works only in one direction, with the result that decryption is no longer possible using the public key. For that reason, anybody who wishes to receive an encrypted message may send a communication partner via an unsecured route the public key required to encrypt the message. The received message is then decrypted using a different key, the private key, which is kept secret and which is not forwarded to communication partners.<sup>184</sup> The process can best be understood on the basis of a comparison with a padlock: anyone can snap a padlock together and, by so doing, secure a trunk; the padlock can only be opened, however, by a person with the right key.<sup>185</sup> Although the public and private keys are linked, the private key cannot be calculated on the basis of the public key.

Ron Rivest, Adi Shamir and Leonard Adleman invented an asymmetric encryption process, which has been named after them (RSA process). In a one-way (trapdoor) function the result of the multiplication of two very large prime numbers

---

is used as a component of the public key. The text is then encrypted using that key. Decryption is dependent on knowledge of the two prime numbers employed. However, there is no known mathematical process by means of which the large integers resulting from the multiplication of two prime numbers can be factored in such a way as to determine what those prime numbers were. At present, all possible combinations must be tried systematically. Given the present state of mathematical knowledge, therefore, the process is secure, provided that sufficiently large prime numbers are chosen. The only risk is that at some stage a brilliant mathematician will discover a quicker factoring method. Thus far, however, even the best efforts have proved fruitless.<sup>186</sup> Many people even claim that the problem is insoluble, but this theory has not yet been proved.<sup>187</sup> By comparison with symmetric processes (e.g. DES), however, public-key encryption requires much more PC calculation time or the use of rapid, large-scale computers.

In order to make the public-key process generally accessible, Phil Zimmermann came up with the idea of linking the public-key process, which involves a great deal of calculation, with a faster symmetric process. The message itself should be encrypted using an asymmetric process, the IDEA [International Institute for Democracy and Electoral Assistance] process developed in Zurich, but the key to the symmetric encryption would be exchanged at the same time, as in the public-key process. Zimmermann developed a user-friendly program (Pretty Good Privacy), which created the requisite key and carried out the encryption at the push of a button (or the click of a mouse). The program was placed on the Internet, from where anyone could download it. PGP was ultimately bought by the US firm NAI, but is still made available to private individuals free of charge.<sup>188</sup>

The source text for the earlier versions has been published, so it can be assumed that no backdoors have been incorporated. Unfortunately, the source texts for the newest version, PGP 7, which is characterized by an exceptionally user-friendly graphic interface, are no longer published. There

is, however, a further implementation of the Open PGP Standard: GnuPG. GnuPG offers the same encryption methods as PGP, and is also compatible with PGP. However, it is freeware, its source code is known and any individual can use it and pass it on. The Federal German Ministry for Economic Affairs and Technology has promoted the porting of GnuPG on Windows and the development of a graphic interface; unfortunately, however, these functions have not yet been fully developed. There are also rival standards to OpenPGP, such as S/MIME, which are supported by many e-mail programs.

In the future quantum cryptography may open up new prospects for secure key exchange. It would ensure that the interception of a key exchange could not pass unnoticed. If polarized photons are transmitted, the fact of their polarization cannot be established without altering that polarization. Eavesdroppers on the line could thus be detected with 100% certainty. Only those keys, which had not been intercepted, would then be used. In experiments, transmission over 48 km via fiber optic cable and over 500 m through the air has already been achieved.<sup>189</sup>

In the discussion on the actual level of security of encryption processes the accusation has repeatedly been made that American products contain backdoors. For example, Excel made headlines here in Europe when it was suggested that in the European version of its program half the key is revealed in the file header. Microsoft also gained media attention when a hacker claimed to have discovered a NSA key hidden in the program, a claim that was of course strongly denied by Microsoft. Since Microsoft has not revealed its source code, any assessment amounts to pure speculation. At all events, the earlier versions of PGP and GnuPG can be said with a great degree of certainty not to contain such a backdoor, since their source text has been disclosed.

Many states initially ban the use of encryption software or cryptographic equipment and make exceptions only subject to prior authorization. The states concerned are not just dictatorships such as

---

China, Iran or Iraq. Democratic states have also imposed legal restrictions on the use or purchase of encryption programs or equipment. It would appear that communications are to be protected against being read by unauthorized private individuals, but that the state should retain the possibility of intercepting such communications, if necessary on the basis of specific legal provisions. The authorities' loss of technical superiority is thus made good by means of legal bans. For example, until recently France imposed a general ban on the use of cryptography, granting authorizations only in individual cases. A few years ago in Germany a debate arose concerning restrictions on encryption and the compulsory submission of a key to the authorities. In the past, the USA has taken a different course, imposing restrictions on key length.

By now, these attempts should have been shown, once and for all, to be futile. The state's interest in having access to encryption processes and thus to the plain texts does not only stand in opposition to the right to privacy, but also to entrenched economic interests. E-commerce and electronic banking are dependent on secure communications via the Internet. If this cannot be guaranteed, these techniques are doomed to failure, owing to a lack of customer confidence. This link explains the about-turn in US and French policy on cryptography.

It should be pointed out here that there are two reasons why e-commerce needs secure encryption processes: not only in order to encrypt messages, but also to prove beyond doubt the identity of business partners. The electronic signature procedure can be carried out using a reversal of the public-key process: the private key is used to encrypt the signature, and the public key to decrypt it. This form of encryption confirms the authenticity of the signature. Through the use of the public key, any individual can convince another of his or her genuineness, but he or she cannot imitate the signature itself. This function is also built into PGP as an additional user-friendly feature.

In some states business travelers are prohibited from using encryption programs on the laptop

computers they carry with them, ruling out any protection of communications with their own firm or the data stored on those computers.

When answering the question of what persons, and under what circumstances, should be advised to employ encryption, a distinction must be drawn between private individuals and firms. As far as private individuals are concerned, it must be clearly stated that the encryption of fax and telephone messages using a crypto-telephone or cipher-fax is not really a workable option, not only because the cost of purchasing such equipment is relatively high, but also because their use presupposes that the interlocutor also has such equipment available, which is doubtless only very rarely the case.

In contrast, e-mails can and should be encrypted by everyone. The oft-repeated claim that a person has no secrets and thus has no need to encrypt messages must be countered by pointing out that written messages are not normally sent on postcards. However, an unencrypted e-mail is nothing other than a letter without an envelope. The encryption of e-mails is secure and relatively straightforward and user-friendly systems, such as PGP/GnuPG, are already available, even free of charge, to private individuals on the Internet. Unfortunately, they are not yet sufficiently widely distributed. The public authorities should set a good example and employ encryption as a standard practice in order to demystify the process.

As far as firms are concerned, they should take strict measures to ensure that sensitive information is only transmitted via secure media. This may seem obvious, and no doubt is for large undertakings, but in small- and medium-sized firms in particular internal information is often transmitted via unencrypted e-mails, because awareness of the problem is not sufficiently well developed. In this connection, it can only be hoped that industry associations and chambers of commerce will step up their efforts to increase that awareness. Admittedly, the encryption of e-mails is only one security aspect amongst many, and serves no purpose if the information is made available to others prior to encryption.

---

The implication is that the entire working environment must be protected, thereby guaranteeing the security of a firm's premises, and checks must be carried out on persons entering offices and accessing computers. In addition, unauthorized access to information via the firm's network must be prevented by means of the introduction of corresponding firewalls. Here, particular dangers are posed by the linking of the firm's internal network and the Internet. If security is to be taken seriously, only those operating systems should be used whose source code has been published and checked, since only then can it be determined with certainty what happens to the data.

Firms are thus faced with a wide variety of tasks in the security sphere. Many businesses have already been set up to provide security advice and arrangements at affordable prices, and the supply of such services is expanding steadily in line with demand. In addition, however, it must be hoped that industry associations and chambers of commerce take up this issue, particularly in order to draw the attention of small firms to the problem of security and to support efforts to devise and implement comprehensive protection arrangements.

### **The EU's External Relations and Intelligence Gathering**

With the adoption of the Maastricht Treaty in 1991, the Common Foreign and Security Policy (CFSP) was established in its most elementary form as a new policy instrument for the European Union. Six years later the Amsterdam Treaty gave further structure to the CFSP and created the possibility for common defense initiatives within the European Union, whilst maintaining the existing alliances. On the basis of the Amsterdam Treaty and with the experiences in Kosovo in mind, the Helsinki European Council of December 1999 launched the European Security and Defense Initiative.

This initiative aims at the creation of a multinational force of between 50 000 and 60 000 troops by the second half of 2003. The existence of such a multinational force will make

the development of an autonomous intelligence capacity inevitable. The simple integration of the existing WEU [Western European Union] intelligence capacity will be insufficient for this purpose. Further cooperation between the intelligence agencies of the Member States, well beyond the existing forms of cooperation, cannot be avoided.

However, the further development of the CFSP is not the only factor leading to closer cooperation among the Union's intelligence services. Further economic integration within the European Union will likewise necessitate a more intensive cooperation in the field of intelligence collection. A united European economic policy implies a united perception of economic reality in the world outside the European Union. A united position in trade negotiations within the WTO [World Trade Organization] or with third countries calls for joint protection of the negotiating position. Strong European industries need joint protection against economic espionage from outside the European Union.

It must finally be emphasized that further development of the Union's second pillar and the Union's activities in the field of Justice and Home Affairs will inevitably also lead to further cooperation between intelligence services. In particular, the joint fight against terrorism, illegal trade in arms, trafficking of human beings, and money laundering cannot take place without intensive cooperation between intelligence services.

Although there is a long tradition within the intelligence services of only trusting the information they collect themselves and maybe even of distrust between the different intelligence services within the European Union, cooperation between services is already gradually increasing.<sup>190</sup> Frequent contacts do exist within the framework of NATO, the WEU and within the European Union. And whereas, within the framework of NATO, the intelligence services are still heavily dependent on the far more sophisticated contributions from the United States, the establishment of the WEU satellite center in Torrejon (Spain) and the creation

---

of an intelligence section attached to the WEU headquarters have contributed to more autonomous European action in this field.

In addition to these developments already taking place, it must be emphasized that there are objective advantages to a joint European intelligence policy. First of all there is simply too much classified and unclassified material available to be collected, analyzed, and evaluated by any single agency or under any single bilateral agreement in Western Europe. The demands on intelligence services range from defense intelligence, through intelligence on third states' internal and international economic policies, to intelligence in support of the fight against organized crime and drug trafficking. Even if cooperation existed only on the most basic level, i.e. as regards the collection of open-source intelligence (OSINT), the results of this cooperation would already be of great importance for the European Union's policies.

In the recent past budgets for intelligence collection have been cut and, in some cases, are still being reduced. At the same time, the demand for information and therefore intelligence has grown. These reduced budgets do not only make this cooperation desirable but, in the long run, also profitable. In particular, in the case of establishing and maintaining technical facilities, joint operations are of interest when money is scarce but also when it comes to evaluating the collected information. Further cooperation will increase the effectiveness of intelligence collection.

In principle, collected intelligence is used to give governments the possibility of better and better-founded decision-making. Further political and economic integration in the European Union demands that intelligence should be available at European level and should also be based on more than one single source.

These objective advantages merely illustrate the growing importance of cooperation within the European Union. In the past nation states used to guarantee their own external security, internal

order, national prosperity and cultural identity. Today, the European Union is in many fields in the process of taking up a role at least complementary to that of the nation state. It is inconceivable that the intelligence services will be the last and only area not affected by the process of European integration.

Following the Second World War cooperation in the field of intelligence collection did not at first take place at European level, but far more at transatlantic level. It has already been shown that very close relations in the field of intelligence gathering were established between the United Kingdom and the United States. But also in the field of defense intelligence within the framework of NATO and beyond, the United States was and still is the absolutely dominant partner. The major question therefore is this: will growing European cooperation in the field of intelligence gathering seriously disrupt relations with the United States, or might it lead to a strengthening of those relations? How will EU/US relations develop under the new Bush Administration? And, in particular, how will the special relationship between the United States and the United Kingdom be maintained in this framework?

Some take the view that there need not be a contradiction between the British/US special relationship and the further development of the CFSP. Others believe that intelligence gathering may be precisely the issue which forces the United Kingdom to decide whether its destiny is European or transatlantic. Britain's intimate links with the US (and with the other partners in the UKUSA Agreement) may make it more difficult for other EU states to share intelligence amongst themselves—because the United Kingdom may be less interested in intra-European sharing, and because its EU partners may trust the United Kingdom less.

Equally, if the US believes that the United Kingdom has developed special links with its EU partners, and that this is part of a European special agreement, the US may become reluctant to continue sharing its intelligence with the United

---

Kingdom. Closer EU cooperation in the field of intelligence may therefore constitute a serious test of the European ambitions of the United Kingdom and of the EU's capacity for integration.

In the present circumstances it is, however, highly unlikely that even extremely rapid progress in cooperation among the European partners can, in the short and even in the longer term, offset the technological advantage enjoyed by the United States. The European Union will not be able to establish a sophisticated network of SIGINT satellites, imaging satellites and ground stations. The European Union will not be able to develop, in the short term, the highly sophisticated network of computers required for the selection and evaluation of the collected material. The European Union will not be prepared to make available the budgetary resources needed to develop a true alternative to the intelligence efforts of the United States.

Purely from a technological and budgetary viewpoint, therefore, it will be in the interests of the European Union to maintain a close relationship with the United States in the field of intelligence collection. But also from a more political point of view, it will be important to maintain and, where necessary, strengthen relationships with the United States, in particular in the context of the joint fight against organized crime, terrorism, drugs and arms trafficking and money laundering. Joint intelligence operations are necessary to support a joint fight. Joint peacekeeping actions, such as in former Yugoslavia, demand a greater European contribution in all areas.

On the other hand, growing European awareness should be accompanied by greater European responsibility. The European Union should become a more equal partner, not only in the economic field, but also in the field of defense and therefore in the field of intelligence collection. A more autonomous European intelligence capacity should therefore not be seen as weakening transatlantic relations, but should be used to strengthen them by establishing the European Union as a more equal and more capable partner. At the same time, the European Union must make independent efforts to

protect its economy and its industry against illegal and unwanted threats such as economic espionage, cyber-crime, and terrorist attacks.

However, transatlantic understanding is necessary in the field of industrial espionage. The European Union and the United States should agree on a set of rules laying down what is and what is not allowed in this area. With a view to strengthening transatlantic cooperation in this field, a joint initiative could be undertaken at WTO level using that organization's mechanisms to safeguard fair economic development worldwide.

Although the issue of the protection of European citizens' privacy must remain fundamental, the further development of a joint European Union intelligence capacity should be considered necessary and inevitable. Cooperation with third countries, and in particular the United States, should be maintained and, very possibly, strengthened. This does not necessarily mean that European SIGINT activities should automatically be integrated in an independent European Union ECHELON system, or that the European Union should become a full partner in the present UKUSA Agreement. However, the development of proper European responsibility in the field of intelligence collection must be actively considered. An integrated European intelligence capacity demands, at the same time, a system of European political control over the activities of these agencies. Decisions will have to be taken on the procedure for assessing intelligence and for taking the political decisions, which result from an analysis of intelligence reports. The lack of such a system of political control, and therefore of political awareness and responsibility for the process of intelligence collection, would be detrimental to the process of European integration.

## **Conclusions and Recommendations**

That a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no

---

longer in doubt. It may be assumed, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organizations, including American sources, that the system or parts of it were, at least for some time, code-named ECHELON. What is important is that its purpose is to intercept private and commercial communications, and not military communications.

Analysis has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed. Nevertheless, it is worrying that many senior Community figures, in particular European Commissioners, who gave evidence to the Temporary Committee claimed to be unaware of this phenomenon.

The surveillance system depends, in particular, upon worldwide interception of satellite communications. However, in areas characterized by a high volume of traffic only a very small proportion of those communications is transmitted by satellite. This means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals. However, inquiries have shown that the UKUSA states have access to only a very limited proportion of cable and radio communications, and, owing to the large numbers of personnel required, can analyze only an even smaller proportion of those communications. However extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice.

Since intercepting communications is a method of spying commonly employed by intelligence services, other states might also operate similar systems, provided that they have the required funds and the right locations. France, thanks to its overseas territories, is the only EU Member State, which is geographically and technically capable of operating a global interception system by itself. There is ample evidence that Russia also operates such a system.

As regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios. If a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union, although at present that title lays down no provisions on the subject, so no criteria are available. If, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition. If a Member State participates in such a system, it violates EC law. At its meeting of 30 March 2000 the Council made clear that it cannot agree to the creation or existence of an interception system which does not comply with the rules laid down in the laws of the Member States and which breaches the fundamental principles designed to safeguard human dignity.

Any interception of communications represents serious interference with an individual's exercise of the right to privacy. Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference. Interference must be proportionate: thus competing interests need to be weighed up and it is not enough that the interference should merely be useful or desirable.

An intelligence system, which intercepted communications permanently and at random, would be in violation of the principle of proportionality and would therefore not be compatible with the ECHR. It would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable.

---

Since most of the rules governing the activities of US intelligence services abroad are classified, compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and predictability laid down by the European Court of Human Rights probably occur.

Although the USA is not itself an ECHR contracting party, the Member States must nevertheless act in a manner consistent with the ECHR. The Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and predictability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

In addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus. As the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinizing the secret services.

As the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and since in some cases parliamentary monitoring bodies do not even exist, the degree of protection can hardly be said to be adequate. It is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinizing the activities of the intelligence services. But even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it

is only the former which affect their own citizens. In the event of cooperation between intelligence services under the CFSP and between the security authorities in the spheres of justice and home affairs, the institutions must introduce adequate measures to protect European citizens.

Part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc. For these reasons, the firms concerned are often subject to surveillance. The US intelligence services do not merely gather general economic intelligence, but also intercept communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery.

Detailed interception poses the risk that information may be used as competitive intelligence, rather than combating corruption, even though the US and the United Kingdom state that they do not do so. However, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled. It should also be pointed out that an agreement on combating the bribery of officials, under which bribery is a crime at the international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications. At all events, it must be made clear that the situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country. Although it is frequently maintained that the global interception system considered in this report has been used in this way, no such case has been substantiated.

The fact is that sensitive commercial data are mostly kept inside individual firms, so that

---

competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more frequently, by hacking into internal computer networks. Only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence gathering. This applies systematically in the following three cases:

- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, the development of telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the company's head office.

Risk and security awareness in small and medium-sized firms is unfortunately often inadequate and the dangers of economic espionage and the interception of communications are often not recognized. Since security awareness is likewise not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations), immediate action is therefore necessary.

Firms must secure the whole working environment and protect all communications channels which, are used to send sensitive information. Sufficiently secure encryption systems exist at affordable prices on the European market. Private individuals should also be urged to encrypt e-mails: an unencrypted e-mail message is like a letter without an envelope. Relatively user-friendly systems exist on the Internet which are even made available for private use free of charge.

In December 1999 in Helsinki the European Council decided to develop more effective

European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP. In order to achieve this goal, by the year 2003 the Union was to be able to rapidly deploy units of about 50000—60000 troops which should be self-sustaining, including the necessary command, strategic reconnaissance and intelligence capabilities. The first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee.

Cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy, which did not involve the secret services, would not make sense and, secondly, it would have numerous professional, financial and political advantages. It would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR. The European Parliament would of course have to exercise appropriate monitoring. The European Parliament is in the process of implementing the Regulation (EC) No 1049/2001 on public access to European Parliament, Council and Commission documents by revising the provisions of its Rules of Procedure as regards access to sensitive documents.

## **Recommendations**

Conclusion and amendment of international agreements on the protection of citizens and firms.

1. The Secretary-General of the Council of Europe is called upon to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the

---

European Court of Human Rights nor reduce the flexibility, which is vital if future developments are to be taken into account.

2. The Member States of the European Union are called upon to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens rights in order to scrutinize the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR.
3. The member countries of the Council of Europe are called upon to adopt an additional protocol, which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities.
4. The Member States are called upon, at the next Intergovernmental Conference, to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy. The EU institutions are called upon to comply with the fundamental rights laid down in the Charter in their respective areas of responsibility and activity.
5. The European Union and the USA are called upon to conclude an agreement on the basis of which each party applies to the other the rules governing the protection of privacy and the confidentiality of business communications which are valid for its own citizens and firms.
6. The Member States are called upon to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions.
7. The UN Secretary-General is called upon to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations.
8. The USA is called upon to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant. The relevant US NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), are called upon to exert pressure on the US Administration to that end.
9. The Council and the Member States are strongly urged to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level. The European Parliament should play an important role in this monitoring and control system.
10. The Member States are strongly urged to review their own legislation on the operations of the intelligence services to ensure that it is consistent with the fundamental rights laid

- 
- down in the ECHR and in the case law of the European Court of Human Rights and, if necessary, to adopt appropriate legal provisions. They are called upon to afford all European citizens the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence. Any of their laws, which are discriminatory in terms of the surveillance powers granted to the secret services, must be repealed.
11. The Member States are called upon to aspire to a common level of protection against intelligence operations and, to that end, to draw up a code of conduct based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services. A similar code of conduct should be negotiated with the USA.
  12. The Member States are called upon to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission.
  13. The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void. The USA, Canada, Australia and New Zealand are called upon to join this initiative.
  14. The Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.
  15. The Member States and the US Administration are called upon to start an open US-EU dialogue on economic intelligence gathering.
  16. The authorities of the United Kingdom are called upon to explain their role in the UK/USA alliance in connection with the existence of a system of the ECHELON type and its use for the purposes of industrial espionage.
  17. The Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.
  18. The Member States are called upon to guarantee appropriate parliamentary and legal monitoring of their secret services. Those national parliaments, which have no monitoring body responsible for scrutinizing the activities of the intelligence services, are called upon to set up such a body.
  19. The monitoring bodies responsible for scrutinizing the activities of the secret services are called upon, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals.

- 
20. The Member States' intelligence services are called upon to accept data from other intelligence services only in cases where such data has been obtained in accordance with the conditions laid down by their own domestic law, as Member States cannot evade the obligations arising from the ECHR by using other intelligence services.
21. Germany and the United Kingdom are called upon to make the authorization of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorized or even merely tolerated on their territory respect human rights.
22. The Commission and Member States are called upon to inform their citizens and firms about the possibility of their international communications being intercepted. This information must be combined with practical assistance in developing and implementing comprehensive protection measures, not least as regards IT security.
23. The Commission, the Council and the Member States are called upon to develop and implement an effective and active policy for security in the information society. As part of that policy, specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information. A Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies must be established.
24. The Commission and Member States are urged to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software.
25. The Commission and Member States are called upon to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programs. The Commission is called upon to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the ,least reliable category.
26. The European institutions and the public administrations of the Member States are called upon systematically to encrypt e-mails, so that ultimately encryption becomes the norm.
27. The Community institutions and the public administrations of the Member States are called upon to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses.
28. The Commission is instructed to have a security analysis carried out, which will show what needs to be protected, and to have a protection strategy drawn up.
29. The Commission is called upon to update its encryption system in line with the latest developments, given that modernization is urgently needed, and calls on the budgetary authority (the Council together with Parliament) to provide the necessary funding.
30. The competent committee is requested to draw up an own-initiative report on security and the protection of secrecy in the European institutions.
31. The Commission is called upon to ensure that data is protected in its own IT systems and to

---

step up the protection of secrecy in relation to documents not accessible to the public.

32. The Commission and the Member States are called upon to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Program.
33. Firms are called upon to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency.
34. The Commission is called upon to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centers—in particular in those Member States where such centers do not yet exist—to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance.
35. The Commission is called upon to pay particular attention to the position of the applicant countries; if their lack of technological independence prevents them from implementing the requisite protective measures they should be given support.
36. The European Parliament is called upon to hold an international congress on the protection of privacy against telecommunications surveillance in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action.

***Minority Opinion by Giuseppe Di Lello, Pernille Frahm and Alain Krivine***

The report by the Temporary Committee confirms the existence of the Echelon interception system, which is administered by various countries, including the United Kingdom, a Member

State of the European Union, with the cooperation of Germany. An interception system of this nature, which does not differentiate between communications, data and documents, infringes the fundamental right to privacy guaranteed by Article 8 of the European Convention on Human Rights and Article 6 of the Treaty on European Union.

The system therefore flagrantly infringes the freedoms enjoyed by European citizens, the logic of the free market and the security of the Union. Whatever our support for or opposition to that logic and those treaties may be, such infringements are unacceptable. In its conclusions, the report ought to have called on the United Kingdom to dissociate itself from the Echelon system and on Germany to close the listening post located on its soil. It is a matter of regret that the European Union is more preoccupied with industrial espionage than with individual monitoring.

***Minority Opinion by Patricia McKenna and Ilka Schröder***

This report makes an important point in emphasizing that Echelon does exist, but it stops short of drawing political conclusions. It is hypocritical for the European Parliament to criticize the Echelon interception practice while taking part in plans to establish a European Secret Service.

No effective public control mechanism of secret services and their undemocratic practices exists globally. It is in the nature of secret services that they cannot be controlled. They must therefore be abolished. This report serves to legitimize a European Secret Service, which will infringe fundamental rights—just as Echelon does.

For the majority in Parliament, the focus is industry, where profit interests are supposedly threatened by industrial espionage. However, the vital issue is that no one can communicate in confidence over distances any more. Political espionage is a much greater threat than economic espionage.

---

This report constantly plays down these dangers of Echelon, while it remains silent about plans to introduce the ENFOPOL interception system in the EU. Every society must take a fundamental decision whether or not to live under permanent control. By adopting this report, the European Parliament shows that it is not concerned about protecting human rights and citizens' liberties.

### ***Minority Opinion by Jean-Charles Marchiani***

The UEN [Union for Europe of the Nations] Group was not surprised at the outcome of the vote on Mr. Schmid's report which, originally, was supposed to concern itself with the Echelon espionage system set up by certain English-speaking countries. From the outset, a majority within Parliament had clearly indicated its intentions, preferring to set up this temporary committee rather than a full-blown committee of inquiry. Accordingly, it had nothing else to fear from proceedings where the reporter's ability to create regular diversions was in no way threatened by a band of malcontents whose motives were too disparate.

Our message is crystal-clear: Mr. Schmid's efforts have been unable to conceal either the existence of the Echelon system or the active or passive involvement of several Member States. That has resulted in a serious breach of the principles underlying the treaties which ought to have led to sanctions being imposed or, at the very least, to measures being taken which might prevent intra-European solidarity from being subordinated to the imperatives of the solidarity of the English-speaking world. Mr. Schmid's weighty report is rich in information but does not properly address the central issue.

We therefore wish to distance ourselves from it and to reject a procedure, which enables this Parliament, on the one hand, to take preventive sanctions against a democratically elected government and, on the other, to refrain from so doing in instances such as this one.

### ***Minority Opinion by Maurizio Turco***

- A. Although the likely existence of an Anglo-American system for the systematic and generalized interception of communications using search engines has been demonstrated, no reference is made to the fact that this technological capacity is certainly being used by Germany and the Netherlands and, probably, by France as well. Accordingly, since the secret services are intercepting communications from abroad, without authorization and on the grounds of national security, some Member States will be intercepting communications from institutions, citizens or businesses of other Member States.
- B. Although more powerful encryption methods should help to protect privacy, their introduction will inevitably lead to the appearance of more powerful lawful means of decryption techniques, given the indissoluble link between the development of cryptographic, code-breaking and technical interception systems.
- C. Solutions must therefore be sought in the political field:
- via legal and parliamentary scrutiny of interception activities and monitoring of the police, security and intelligence services;
  - by preventing the proliferation of control bodies which operate to different data-protection standards and without any genuine democratic and legal scrutiny,
  - by regulating CE on the basis of the highest standard and the case-law of the ECHR—protection of the privacy of European citizens against preventive interference by government authorities and eliminating the discrimination existing within the European Union between citizens of various Member States.

---

## Endnotes

<sup>1</sup> Voice of America, 23 February 2000.

<sup>2</sup> Voice of America, 30 March 2000.

<sup>3</sup> STOA (Scientific and Technological Options Assessment) is a department of the Directorate General for Research of the European Parliament, which commissions research at the request of committees. However, the documents it produces are not subject to scientific review.

<sup>4</sup> Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in STOA (Ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information* (October 1999), PE 168.184.

<sup>5</sup> Steve Wright, An appraisal of technologies of political control, STOA interim study, PE 166.499/INT.ST. (1998).

<sup>6</sup> Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in STOA (Ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information* (October 1999), PE 168.184., PE 305.391 22/194 RR\445698EN.doc.

<sup>7</sup> Raytheon Corp Press release, <http://www.raytheon.com/sivam/contract.html>; Scott Shane, Tom Bowman, "America's Fortress of Spies," *Baltimore Sun*, 3 December 1995.

<sup>8</sup> European Parliament decision of 5 July 2000, B5-0593/2000, OJ C 121/131 of 24 April 2001.

<sup>9</sup> Decision of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry (95/167/EC), Article 3(3)-(5)..RR\445698EN.doc 23/194 PE 305.391.

<sup>10</sup> The Commission on the Roles and Capabilities of the US Intelligence Community has stated in its report, *Preparing for the 21st Century: An Appraisal of US Intelligence* (1996) that 95% of all economic intelligence is derived from open sources (Chapter 2, "The Role of Intelligence").

<sup>11</sup> Foreign communications is all incoming and outgoing civilian, military or diplomatic communications. If the intelligence service has access to the relevant cables, it can intercept both incoming and outgoing

communications. If the service targets satellite communications, it has access only to the downlink, but can intercept all the communications it carries, including those not intended for its own territory. Since as a rule the satellite footprints cover the whole of Europe or an even wider area, satellite communications throughout Europe can be intercepted using receiving stations in one European country. The + indicates that communications are intercepted. The – signifies that communications are not intercepted.

<sup>12</sup> With the aid of a demonstration version of Visual Route, a program, which reveals the route taken by an Internet link, it was shown that a link from Germany to England, Finland, or Greece passes via the USA and the UK. A link from Germany to France likewise passes via the UK. Links from Luxembourg to Belgium, Greece, Sweden, or Portugal pass via the USA and to Germany, Finland, France, Italy, the Netherlands or Austria via the switch in London. <http://visualroute.cgan.com.hk/>.

<sup>13</sup> Letter from the Minister of State in the German Federal Defense Ministry, Walter Kolbow, to the reporter, dated 14 February 2001.

<sup>14</sup> Süddeutsche Zeitung No 80, 5.4.2001, 6.

<sup>15</sup> Jeffrey T. Richelson, *The U.S. Intelligence Community* (1989), 188, 190.

<sup>16</sup> Letter from the Minister of State in the German Federal Defense Ministry, Walter Kolbow, to the reporter, dated 14 February 2001.

<sup>17</sup> Major A. *Andronov*, *Zarubezhnoye voyennoye obozreniye*, No 12, 1993, 37-43.

<sup>18</sup> Until May 2001 the FIS was not authorized to intercept foreign cable communications in Germany.

<sup>19</sup> Law on the restriction of the privacy of posts and telecommunications (law on Article 10 of the Basic Law) of 13 August 1968.

<sup>20</sup> Information drawn from the answers given to the Temporary Committee by telecommunications service providers from a number of Member States.

<sup>21</sup> Deutsche Telekom homepage: [www.detesat.com/deutsch/](http://www.detesat.com/deutsch/)

<sup>22</sup> Georg E. Thaller, *Satellites in Earth Orbit*, Franzisverlag (1999).

<sup>23</sup> Cf. Hans Dodel, *Satellite communications*, Huthig Verlag (1999).

<sup>24</sup> Homepage of the Federation of American Scientists, <http://www.geo-orbit.org>.

<sup>25</sup> Nicky Hager, *Exposing the Global Surveillance System* <http://www.ncoic.com/echelon1.htm>; *Secret Power. New Zealand's Role in the International Spy Network*, Craig Potton Publishing, 1996.

<sup>26</sup> Jeffrey T. Richelson, *Desperately Seeking Signals*, *The Bulletin of American Scientists*, Vol. 56, No. 2,

---

47-51; <http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html>. See also Richelson, T. Jeffrey, *The U.S. Intelligence Community*, Westview Press, 1999.

<sup>27</sup> Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition, Part 4/5, in STOA (Ed.). *Development of Surveillance Technology and Risk of Abuse of Economic Information*, October 1999, <http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf>. Inside Echelon, 25.7.2000, <http://www.heise.de/tp/deutsch/special/ech/6928/1.html>. Interception Capabilities Impact and exploitation: Echelon and its role in COMINT, submitted to the Temporary Committee on 22 January 2001.

<sup>28</sup> Jeffrey T. Richelson, Newly released documents on the restrictions NSA places on reporting the identities of US persons, Declassified. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>.

<sup>29</sup> Military.com; \*.mil-Homepages.

<sup>30</sup> Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, *Securing our Nation's Safety* (2000), <http://www.dpmc.govt.nz/dess/securingoursafety/index.html>.

<sup>31</sup> Abbreviations used: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

<sup>32</sup> It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations', from the home page of the 544<sup>th</sup> Intelligence Group <http://www.aia.af.mil>.

<sup>33</sup> Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; <http://www.aph.gov.au/hansard> 52 Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; <http://www.aph.gov.au/hansard>.

<sup>34</sup> Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety," December 2000, <http://www.dpmc.govt.nz/dess/securingoursafety/index.html>

<sup>35</sup> Ibid. In 1989, [...] the GCSB opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCSB not only intercepts the signals, it also processes, decrypts

or decodes and/or translates the information the signals contain before passing it on as a report to the appropriate Minister or government department.

<sup>36</sup> Nicky Hager, *Secret Power*. New Zealand's Role in the International Spy Network, op cit., p. 182.

<sup>37</sup> Announcement of 31 May 2001 on the INSCOM homepage, [http://www.vulcan.belvoir.army.mil/bas\\_to\\_close.asp](http://www.vulcan.belvoir.army.mil/bas_to_close.asp).

<sup>38</sup> Christopher Andrew, The making of the Anglo-American SIGINT Alliance in Hayden B. Peake, Samuel Halpern (Eds.), *In the Name of Intelligence*. Essays in Honor of Walter Pforzheimer, NIBC Press (1994), 95 -109.

<sup>39</sup> Christopher Andrew, The making of the Anglo-American SIGINT Alliance, op cit., p. 99 At a meeting in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that "it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable," and said that "the time had come or a free exchange of intelligence." (quoted from COS (40)289, CAB 79/6, PRO. Smith, *The Ultra Magic Deals*, 38, 43-4. Sir F.H. Hinsley, et al., *British Intelligence in the Second World War*, Vol. I, 312-13).

<sup>40</sup> Christopher Andrew, The making of the Anglo-American SIGINT Alliance, op cit., p.100. In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liaison officer to the British Joint Services Mission in Washington, Tim O'Connor, to advise him on cryptologic collaboration.

<sup>41</sup> Ibid, p.100. Sir F.H. Hinsley, et al., *British Intelligence in the Second World War*, Vol. II, 56.

<sup>42</sup> Christopher Andrew, op. Cit. P. 101. Sir F.H. Hinsley, et al., op. Cit. p. 48.

<sup>43</sup> Christopher Andrew, op. cit., p. 101-2. Interviews with Sir F.H. Hinsley, "Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW 63 Harry S. Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: "The Secretary of War and the Secretary of the Navy are hereby authorized to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States."

<sup>44</sup> Bradley F. Smith, *The Ultra-Magic Deals and the Most Secret Special Relationship*, Novato, Ca: Presidio,

---

1993.

<sup>45</sup> Christopher Andrew, The making of the Anglo-American SIGINT Alliance in Hayden, H. Peake and Samuel Halpern Eds, In the Name of Intelligence. Essays in Honor of Walter Pforzheimer (NIBC Press 1995) p. 95. Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.

<sup>46</sup> Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8, 14.

<sup>47</sup> Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

<sup>48</sup> Terms/Abbreviations/Acronyms' published by the US Navy and Marine Corps Intelligence Training Center (NMITC) at <http://www.cnet.navy.mil/nmitc/training/u.html>.

<sup>49</sup> Martin Brady, Head of the DSD, letter of 16.3.1999 to Ross Coulthart, Sunday Program Channel 9.

<sup>50</sup> Christopher Andrew, The growth of the Australian Intelligence Community and the Anglo-American Connection, pp. 223-4.

<sup>51</sup> Jeffrey T. Richelson, The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>.

<sup>52</sup> Jeffrey T. Richelson, The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html>.

<sup>53</sup> Statement for the Record of NSA Director Lt. Gen. Michael V. Hayden, USAF before the House Permanent Select Committee on Intelligence, April 12, 2000.

<sup>54</sup> Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8 1992.

<sup>55</sup> Document 7. United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures," July 27 1993.

<sup>56</sup> Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24 1952. Document 2b. National Security Council Intelligence Directive No. 9, Communications Intelligence, December 29 1952.

<sup>57</sup> Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security

Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3 1991.

<sup>58</sup> Document 12. 'Activation of Echelon Units,' from History of the Air Intelligence Agency, 1 January – 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

<sup>59</sup> Duncan Campbell, Inside ECHELON. The history, structure and function of the global surveillance system known as ECHELON, 1 97 Homepage of the Advocacy Center, <http://www.ita.doc.gov/td/advocacy/index.html>.

<sup>60</sup> Bo Elkjaer, Kenan Seeberg, ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Denmark, 8.3.2000, <http://cryptome.org/echelon>.

<sup>61</sup> Bo Elkjaer, Kenan Seeberg, ECHELON was my baby: Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

<sup>62</sup> NBC TV interview '60 Minutes', 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

<sup>63</sup> Communication Security Establishment, subordinate to the Canadian Ministry of Defense, engaged in SIGINT

<sup>64</sup> NBC TV interview '60 Minutes', 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

<sup>65</sup> Florian Rötzer, Die NSA geht wegen ECHELON an die Öffentlichkeit; [http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub\\_ordner=special](http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special).

<sup>66</sup> NBC TV interview '60 Minutes', 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

<sup>67</sup> Interview on the Australian Channel 9 on 23.3.1999; <http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm>.

<sup>68</sup> Jim Bronskill, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, <http://www.ottawacitizen.com/national/990522/2630510.html>.

<sup>69</sup> James Woolsey, Remarks at the Foreign Press Center, Transcript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>.

<sup>70</sup> Commons Written Answers, House of Commons Hansard Debates

<sup>71</sup> Ibid. 12.7.1995.

<sup>72</sup> Ibid. 25.10.1994.

<sup>73</sup> Ibid. 3.12.1997

<sup>74</sup> Ibid. 12.5.2000.

<sup>75</sup> Ibid. 12.7.1995.

<sup>76</sup> Ibid. 8.3.1999, 6.7.1999.

<sup>77</sup> Ibid. 3.12.1997.

<sup>78</sup> Intelligence and Security Committee (UK), Annual Report 1999-2000, para. 14, presented to the Commons by the Prime Minister in November 2000.

---

<sup>79</sup> Defense Signals Directorate, Australian intelligence service engaged in SIGINT.

<sup>80</sup> Letter of 16.3.1999 from Martin Brady, Director of the DSD, to Ross Coulthart, 'Sunday' program; see also: [http://sunday.ninemsn.com/01\\_cover\\_stories/transcript\\_335.asp](http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp); [http://sunday.ninemsn.com/01\\_cover\\_stories/article\\_335.asp](http://sunday.ninemsn.com/01_cover_stories/article_335.asp)

<sup>81</sup> Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

<sup>82</sup> Brief aan de Tweede Kamer betreffende 'Het grootschalige af luisteren van moderne telecommunicatie systemen', 19.1.2001.

<sup>83</sup> Francesco Sorti, Dossier esclusivo. Caso ECHELON. Parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998.

<sup>84</sup> Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per I servizi di informazione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 2000.

<sup>85</sup> Jean Guisnel, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998. Vincent Jauvert, Espionnage, comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, No 1900, 14 et seq.

<sup>86</sup> Erich Schmidt-Eenboom, in: Steng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg (1999), 180.

<sup>87</sup> Russian Federation Federal Law on Foreign Intelligence, adopted by the Duma on 8 December 1995, Sections 5 and 11 141 Quoted in Gordon Bennett, Conflict Studies and Research Centre, The Federal Agency of Government communications and Information, August 2000, <http://www.csrc.ac.uk/pdfs/c105.pdf>.

<sup>88</sup> Art. 3(1) and Recital 15 "Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union."

<sup>89</sup> See, for example, para 25 of the resolution on the draft action plan of the Council and Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice (13844/98 - C4- 0692/98 - 98/0923(CNS)), OJ C 219, 30.7.1999, p. 61 et seq.

<sup>90</sup> In the area of telecommunications surveillance there

are currently only two EU legislative acts, neither of which covers the question of admissibility: - Council resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11.1996), the annex to which sets out the technical requirements relating to the lawful interception of modern telecommunications systems, and - Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union.

<sup>91</sup> German Federal Constitutional Court (FCC), 1 BVR 226/94 of 14 July 1999, Rz 187: "The recording of data already represents a violation of that right in so far as it makes the content of the communications available to the Federal Intelligence Service and forms the basis of the ensuing analysis using search terms."

<sup>92</sup> Compare the report submitted to the US Congress in late February 2000, "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance," <http://www.fas.org/irp/nsa/standards.html>, which refers to the Foreign Intelligence Surveillance Act (FISA), printed in Title 50, Chapter 36, USC, § 1801 et seq, and Executive Order No 12333, 3 CFR 200 (1982), printed in Title 50, Chapter 15, USC, § 401 et seq, <http://www4.law.cornell.edu/uscode750/index.html>.

<sup>93</sup> Article 12 of the Universal Declaration of Human Rights; Article 17 of the UN Covenant on Civil and Political Rights; Article 7 of the EU Charter of Fundamental Rights; Article 8 of the ECHR; Recommendation of the OECD Council on guidelines for the security of information systems, adopted on 26/27 November 1993, C(1992) 188/final; Article 7 of the Council of Europe Convention on the Protection of Persons with regard to the automatic processing of personal data; compare the study commissioned by STOA entitled "Development of Surveillance Technology and Risk of Abuse of Economic Information;" Part. 4/5: the legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), October 1999, 2.

<sup>94</sup> Adopted by the UN General Assembly on 16 December 1966.

<sup>95</sup> Optional Protocol to the International Covenant on Civil and Political Rights, adopted by the UN General Assembly on 16 December 1966.

<sup>96</sup> "Everyone has the right to respect for his or her private family life, home and communications."

<sup>97</sup> Judgment of the European Court of Human Rights, Loizidou/Turkey, 23.3.1995, line 62, with further references: '– the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties [–] responsibility can be

---

involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory’, with reference to the European Court of Human Rights, Drozd and Janousek, 26.6.1992, line 91. See also the comprehensive details in Francis G. Jacobs, Robin C. A. White, *The European Convention on Human Rights*, Clarendon Press (1996), pp. 21 et seq. Jochen Abr. Frowein, Wolfgang Peukert, *European Convention on Human Rights*, N.P. Engel Verlag (1996), Rz 4 et seq.

<sup>98</sup> See European Court of Human Rights, Klass et al, 9.1978, line 41.

<sup>99</sup> See European Court of Human Rights, Malone, 2.8.1984, line 83 et seq; also B. Davy/U.Davy, *Aspects of state information collection and Article 8 of the ECHR*, JBl 1985, 656.

<sup>100</sup> Under the case law of the European Court of Human Rights (in particular Sunday Times, 26.4.1979, line 47 et.

<sup>101</sup> Silver et al, 25.3. 1983, line 87 et seq. seq, Silver et al, 25.3.1983, line 85 et seq, the term ‘the law’ in Article 8(2) embraces not only laws in the formal sense, but also legal provisions below the level of a law and, in certain circumstances, even unwritten law. It is essential, however, that it is clear to the legal subject under what circumstances interference is possible. For more details see Wolfgang Wesseley, *Telecommunications Privacy; an unknown basic right?*, ÖJZ 1999, pp. 491 et seq, 495.

<sup>102</sup> The justification of ‘economic well-being’ was accepted by the European Court of Human Rights in a case involving the transmission of medical data relevant to the award of public compensation, M.S./Sweden, 27.8.1997, line 38; and in a case involving the expulsion from the Netherlands of a person who had been living on welfare payments after the grounds for the award of a residence permit had ceased to apply, Ciliz/Netherlands, 11.7.2000, line 65.

<sup>103</sup> European Court of Human Rights, Leander, 26.3.1987, line 51.

<sup>104</sup> European Court of Human Rights, Malone, 2.8.1984, line 67.

<sup>105</sup> European Court of Human Rights, Leander, 26.3.1987, line 59, Sunday Times, 26.4.1979, line 46 et seq.

<sup>106</sup> European Court of Human Rights, Silver et al, 24.10.1983, line 97.

<sup>107</sup> European Court of Human Rights, Leander, 26.3.1987, line 60.

<sup>108</sup> Your reporter is aware that neither Luxembourg nor Ireland has a foreign intelligence service and does not carry out SIGINT operations. The need for a

specific supervisory body relates here only to domestic intelligence activities.

<sup>109</sup> For details of the situation regarding the supervision of intelligence services in the Member States, see Chapter 9.

<sup>110</sup> Bill entitled ‘Proposition de loi tendant à la création de délégations parlementaires pour le renseignement, and the related report by Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d’une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l’assemblée nationale le 23. novembre 1999.

<sup>111</sup> See also Dimitri Yernault, ‘ECHELON and Europe. The protection of privacy against communications espionage’, *Journal of the Courts, European Law*, 2000, 187 et seq.

<sup>112</sup> European Court of Human Rights, Abdulaziz, Cabales and Balkandali, 28.5.1985, line 67; X and Y/Netherlands, 26.3.1985, line 23; Gaskin v United Kingdom, 7.7.1989, line 38; Powell and Rayner, 21.2.1990, line 41.

<sup>113</sup> This is also necessary for compliance with Article 13 of the ECHR, which grants the person whose privacy has been invaded the right to submit a complaint to national courts.

<sup>114</sup> James Woolsey (former CIA Director), *Why America Spies on its Allies*, *The Wall Street Journal Europe*, 22 March 2000, 31, and Remarks at the Foreign Press Centre, transcript, 7 March 2000, <http://cryptome.org/echelon-cia.htm>.

<sup>115</sup> Article 8(2) of the ECHR lays down these issues as grounds justifying interference in an individual’s exercise of the right to privacy.

<sup>116</sup> British law is an exception, giving the Home Secretary the power to issue authorisations (Regulation of Investigatory Powers Act 2000, Section 5(1) and (3)(b)).

<sup>117</sup> For example, in Austria and Belgium.

<sup>118</sup> For example, in Germany, law on the restriction of post and telecommunications secrecy (Law on Article 10 of the Basic Law). Pursuant to paragraph 9, except in cases where there is a risk that delay would frustrate the operation, the commission must be informed before the surveillance is carried out.

<sup>119</sup> For example in the United Kingdom (Regulation of Investigatory Powers Act, Section 1), and in France for cable communications (Law 91/646 of 10 July 1991 *Loi relative au secret des correspondances émises par la voie de télécommunications*).

<sup>120</sup> For example cable communications in France (Article 20 of Law 91/646 of 10 July 1991 - *loi relative*

---

au secret des correspondances émises par la voie de télécommunications).

<sup>121</sup> For full details see ‘The Parliamentary Supervision of the Intelligence Services in Germany, as at 9.9.2000’, published by the German Bundestag, Secretariat of the Parliamentary Control Body.

<sup>122</sup> Law on the supervision of federal intelligence activities (PKGrG) of 17 June 1999, BGBI I 1334 idgF.

<sup>123</sup> Law 91-646 of 10 July 1991; loi relative au secret des correspondances émises par la voie de télécommunications.

<sup>124</sup> See the Bill entitled ‘Proposition de loi tendant à la création de délégations parlementaires pour le renseignement’, and the related report by *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N o 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d’une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de L’Assemblée nationale le 23 novembre 1999.

<sup>125</sup> Intelligence Services Act 1994, Section 10

<sup>126</sup> Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 / IV, organique du contrôle des services de police et de renseignements.

<sup>127</sup> Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningsjenester, lov 378 af 6.7.88.

<sup>128</sup> Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 17 Juni 1999 BGBI I 1334 idgF.

<sup>129</sup> Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento de servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

<sup>130</sup> Tweede-Kamercommissie voor de Inlichtingen-en Veiligheidsdiensten, 17. Reglement van order van de Tweede Kamer der Staten-General, Art. 22.

<sup>131</sup> Conselho de Fiscalização dos Serviços de Informações (CFSI), Law 30/84 of 5.9.1984, amended by Law 4/95 of 21.2.1995, Law 15/96 of 30.4.1996 and Law 75-A/97 of 22.7.1997.

<sup>132</sup> Intelligence and Security Committee (ISC), Intelligence Services Act 1994, Section 10.

<sup>133</sup> Standing Subcommittee of the National Defence Committee responsible for monitoring intelligence measures to safeguard military security and the Standing Subcommittee of the Committee on Internal Affairs responsible for monitoring measures to protect constitutional bodies and their ability to act, Article 52a B-VG, §§ 32b et seq., Law on the Rules of Procedure,

1975.

<sup>134</sup> Ombudsman, legal basis for supervision of the police (SUPO): Poliisilaki 493/1995 § 33 and Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 § 15, for the military: Poliisilaki 493/1995 § 33 and Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 § 5.

<sup>135</sup> Rikspolisstyrelsens ledning, Förordning (1998: 773) med instruktion för Rikspolisstyrelsen (Regulation (1989: 773) on the national police authority).

<sup>136</sup> Information for firms provided with security protection, Federal Ministry of Economic Affairs, 1997.

<sup>137</sup> Michael E. Porter, *Competitive Strategy*, Simon & Schuster (1998). 206 *Roman Hummelt*, *Industrial espionage on the data highway*, Hanser Verlag (1997). 207 Details and names confidential.

<sup>138</sup> *Impulse*, 3/97, 13 et seq.

<sup>139</sup> Louis J. Freeh, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996.

<sup>140</sup> Robert Lyle, Radio Liberty/Radio Free Europe, 10.2.1999.

<sup>141</sup> *Computerzeitung*, 30.11.1995, 2.

<sup>142</sup> Roman Hummelt, *Spionage auf dem Datenhighway*, Hanser Verlag (1997), 49 et seq

<sup>143</sup> Confidential statement to the reporter by a counterintelligence service, source protected.

<sup>144</sup> State Department Foreign Press Center briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000.

<sup>145</sup> Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996.

<sup>146</sup> The end of the Cold War has not resulted in a peace dividend regarding economic espionage, Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996.

<sup>147</sup> Interpretation by your reporter of the cryptic remarks made by *Louis J. Freeh* to the committee.

<sup>148</sup> In these areas the interception of communications is a promising method!

<sup>149</sup> James Woolsey, Remarks at the Foreign Press Center, Transcript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>.

<sup>150</sup> As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate

agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defense, we never play offense, and we never will play offense.

<sup>151</sup> Albin Eser, Michael Überhofer, Barbara Huber (Eds), *Using the criminal law to combat corruption. A comparative survey of offences involving bribery*, drawn up on behalf of the Bavarian Ministry of Justice, edition iuscrim (1997).

<sup>152</sup> The scale runs from 10 (low incidence of bribery) to 0 (high incidence of bribery): Sweden (8.3), Australia (8.1), Canada (8.1), Austria (7.8), Switzerland (7.7), Netherlands (7.4), United Kingdom (7.2), Belgium (6.8), Germany (6.2), USA (6.2), Singapore (5.7), Spain (5.3), France (5.2), Japan (5.1), Malaysia (3.9), Italy (3.7), Taiwan (3.5), South Korea (3.4) and China (3.1). <http://www.transparency.org/documents/cpi/index.html#bpi>.

<sup>153</sup> OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, *Legal Aspects of International Trade and Investment*, <http://www.ita.doc.gov/legal/>

<sup>154</sup> <http://www.oecd.org/daf/nocorruption/annex3.htm>.

<sup>155</sup> Criminal Law Convention on Corruption <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01>

<sup>156</sup> Civil Law Convention on Corruption ETS no.: 174, <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01>

<sup>157</sup> Convention, drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union, on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, OJ C 195, 25.6.1997, 2.

<sup>158</sup> Joint Action of 22 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on corruption in the private sector (98/742/JHA), OJ L 358, 31.12.1998, 2.

<sup>159</sup> White House Archive, <http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html>.

<sup>160</sup> Homepage of the National Security Council (NSC), <http://www.whitehouse.gov/nsc>.

<sup>161</sup> TPCC brochure on the Advocacy Center, October 1996.

<sup>162</sup> Homepage of the Advocacy Center, <http://www.ita.doc.gov/td/advocacy/>

<sup>163</sup> TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, and Minutes of the meeting of 17.8.1994, from a letter from the US and Foreign Commercial Service of 25.8.1994.

<sup>164</sup> *ibidem*: 'Bob Beamer suggested that any primary

competitors known to the group for these projects should be included as background information', Bob Beamer is one of the CIA representatives.

<sup>165</sup> Computer espionage, Document 44, Federal Ministry for Economic Affairs, July 1998.

<sup>166</sup> Roman Hummelt, *Industrial Espionage on the Data Highway*, Hanser Verlag (1997).

<sup>167</sup> George Kurtz, Stuart McClure, Joel Scambray, *Hacking exposed*, Osborne/McGraw-Hill (2000), 94.

<sup>168</sup> Martin Kuppinger, *Internet and Internet Security*, Microsoft Press Deutschland (1998), 60.

<sup>169</sup> Othmar Kyas, *Security on the Internet*, International Thomson Publishing (1998), 23.

<sup>170</sup> Anonymous, *Hacker's guide*, Markt & Technik-Verlag (1999).

<sup>171</sup> Information supplied by members of COREPER [The Committee of Permanent Representatives of the Member States of the European Union] and Council officials; sources protected.

<sup>172</sup> Council Decision of 19 March 2001 adopting the Council's security regulations, OJ L 101, 11.4.2001, 1.

<sup>173</sup> There is evidence of this even in antiquity, e.g. the use of the *skytale* or cipher rod by the Spartans in the 5<sup>th</sup> century BC.

<sup>174</sup> Otto Leiberich, , *Vom diplomatischen Code zur Falltürfunktion*  $\text{\textcircled{E}}$  *Hundert Jahre Kryptographie in Deutschland*<sup>TM</sup> [From diplomatic code to trap-door function  $\text{\textcircled{E}}$  a hundred years of cryptography in Germany], *Spektrum der Wissenschaft* June 1999, 26 et seq.

<sup>175</sup> It was introduced by Major Joseph Mauborgne, head of the cryptographic research division of the American army; Simon Singh, *The Code Book* (1999), Carl Hanser Verlag 151.

<sup>176</sup> Simon Singh, *The Code Book* (1999), Carl Hanser Verlag 151 et seq.

<sup>177</sup> Reinhard Wobst, *Abenteuer Kryptologie 2*, Adison-Wesley (1998), 60.

<sup>178</sup> Enigma was developed by Arthur Scherbius and patented in 1928. It was a little like a typewriter, as it had a keyboard on which the plain text was keyed in. By means of a peg-board and rotating drums the text was encoded in accordance with given rules and decoded at the other end on the same machine using code books.

<sup>179</sup> American Standard Code for Information Exchange.

<sup>180</sup> A= 1000001, B= 1000010, C=1000011, D=1000100, E= 1000101, etc.

<sup>181</sup> In binary terms, this number consists of 56 zeros and ones. See Singh, *The Code Book*, Carl Hanser Verlag (1999), 303.

<sup>182</sup> Simon Singh, *The Code Book*, Carl Hanser Verlag (1999), 302 et seq.

<sup>183</sup> It was created by two Belgian cryptographers working

at the Catholic University of Louvain, Joan Daemen and Vincent Rijmen.

<sup>184</sup> The idea of asymmetric encryption using the public-key process was devised by Whitfield Diffie and Martin Hellmann.

<sup>185</sup> Simon Singh, *The Code Book*, Carl Hanser Verlag (1999), 327.

<sup>186</sup> Johannes Buchmann, *Factoring large integers*, *Spektrum der Wissenschaft* 2, 1999, 6 et seq.

<sup>187</sup> Simon Singh, *The Code Book*, Carl Hanser Verlag (1999), 335 et seq.

<sup>188</sup> Information on the software can be found at [www.pgpi.com](http://www.pgpi.com).

<sup>189</sup> On quantum cryptology, see Reinhard Wobst, *Abenteuer Kryptographie 2*, Adison-Wesley (1998), 224 et seq.

<sup>190</sup> Charles Grant, *Intimate relations. Can Britain play a leading role in European defense - and keep its special links to US intelligence?* 4.2000, Centre for European Reform.

## George and Marisol Gari

The FBI arrested two additional members of the Cuban “La Red Avispa”—the Wasp Network—on 31 August 2001. Taken into custody by the FBI in Orlando, Fla., were George Gari and his wife, Marisol, for trying to infiltrate Cuban exile and US military installations. George was born in Brooklyn, N.Y., but moved to Cuba as a child.

In the three-count indictment, George, 40, and his wife, 42, were charged with conspiracy to act as agents of a foreign government without proper identification or notice to the attorney general. The FBI said that the espionage by the Garis occurred between 1991 and 1998 and that Marisol used her US Postal Service job to gain access to mail sent by and intended for Cuban Americans. She also compiled a report on various US mail systems for her Cuban bosses.

The Garis also are suspected of conducting surveillance on the Cuban American National Foundation, including surveying the interior layout and the security measures in place at the Foundation’s Miami headquarters. According to the FBI, George, who worked for Lockheed Martin, was ordered by his Cuban handlers to apply for work at the Southern Command but was unsuccessful.

Known by the codenames “Luis” and “Margot,” authorities said the Garis received training by the Cuban Directorate of Intelligence (DI) before their 1990 arrival in the United States and, together, used advanced encryption technology to transmit information about anti-Castro exile organizations between the Cuban Government and other agents.

A federal grand jury sitting in Miami, Florida, returned a three-count Indictment charging George and Marisol with spying for the Government of Cuba.

As set forth in the indictment, the object of the conspiracy was that the defendants and their co-conspirators would function as covert spies serving the interests of the government of the Republic

---

of Cuba within the United States. Their task was to gather and transmit information to the Cuban Government concerning US Government functions and installations by informing on anti-Castro Cuban political groups in Miami-Dade County and by carrying out other operational directives of the Cuban Government.

As set forth in the indictment, trained officers of the Cuban DI, known as illegal officers, would take up residence in South Florida and carry out clandestine activities on behalf of the Cuban Government. These officers would manage and oversee the activities of agents, transmitting to the agents instructions received by the illegal officers from the Republic of Cuba. The illegal officers also would receive oral and recorded reports from the agents and cause these reports to be communicated to the Republic of Cuba.

The network of Miami-based illegal officers and agents was known as La Red Avispa and their activities were overseen, directed, analyzed, and reviewed by the DI in Cuba. The illegal officers would and did receive and transmit to the agents instructions, which the agents would and did carry out, to conduct covert and clandestine activities on behalf of the Republic of Cuba.

On 20 September 2001, the Garis pleaded guilty to spying for Cuba, but Marisol's plea occurred behind closed doors. Her plea agreement, which was sealed by the US District Judge, called for her to cooperate with federal prosecutors in their continuing investigation. Marisol's lawyer confirmed that she pleaded guilty to one count of conspiracy to act as an unregistered agent for Cuba. She faces a maximum of five years in prison and could be deported afterward because she is not a US citizen. In turn, prosecutors dropped a second charge of acting as an unregistered Cuban agent, which carried a 10-year sentence.

After Marisol made her plea, the courtroom was reopened for George's guilty plea to one count of acting as an unregistered agent for Cuba. He faces a maximum of 10 years. In return, prosecutors agreed to recommend a reduction in his sentence

and dropped a second charge of conspiracy. His plea agreement does not call for him to cooperate.

Many of the lawyers for the high-ranking Cuban La Red Avispa spies said that the Garis were relatively low-level functionaries in the network and did not believe that they would have any important information to provide to US authorities. However, because they reported to several of the higher-ranking Cuban DI illegal agents and had started "handling" other spies, according to the plea agreements, they may be able to shed additional light on the Cuban network and possibly other members still at large.

On 4 January 2002, George and Marisol Gari received prison sentences of seven years and three and a half years, respectively.

## Japan

Japan is cited as a good example of a country whose government has played a key role in collecting, analyzing, and disseminating foreign technology information to both its industry and government. In the early part of the 20<sup>th</sup> century, Japan's foreign technical collection was done by some of its corporations, which had worldwide intelligence networks. However, the real boom came after the allied occupation in 1945, when former military intelligence officers found new homes for their skills in Japan's consolidated trading companies. After World War II, Japan also solidified its technology base by importing foreign technology to supplement its own research and development efforts.

Japan's primary industrial technology agency is the Ministry of International Trade and Industry (MITI). MITI's mission is to further industrial research and development in Japan, and it has been the engine of Japan's economic miracle since its founding in 1949.

Japanese research and development capabilities have grown, and Japanese Government industrial policies continue to target knowledge-intensive technologies as well as substantially increasing government and industry investments in new technologies.<sup>2</sup> Many Japanese technological capabilities now match those of the United States and in some cases have surpassed US capabilities.

The Japanese Government has an extensive, centrally coordinated process and uses considerable resources to collect and disseminate foreign technology information primarily for commercial purposes. This process is characterized by extensive networks between officials and researchers in government, industry, and academia that provide information and a methodical process of consensus building regarding what technologies should be monitored within a competitive, commercial framework. Experts collect information in specific areas of interest, which is targeted to the needs of the users, and then use extensive and multiple channels to disseminate the

data. MITI facilitates and coordinates government, industry, and academic activities, including research and development programs and foreign technology information collection efforts, by providing technology information and significant funding for these activities.

Japanese Government and private-sector officials stressed the importance of determining and providing the foreign technology information that customers want and need. Other elements of a successful system that they identified include maintaining a cooperative government-industry relationship, treating technology monitoring as an integral part of an organization's operations, and locating operations in the target country.

The Japanese Government plays a more significant and intense role in guiding the national research and development effort for economic competitiveness. In addition, Japan spends a lot of money to collect, analyze, and disseminate foreign technology information to its government, industry, and academia.

MITI retains its reputation abroad as being the headquarters of "Japan Incorporated." With its 15,000 employees, MITI has no counterpart in the United States or in most other industrialized nations. MITI's role as a government ministry is to work closely with private industry to identify strategic markets and products.

MITI establishes organizations that carry out specific research and development programs. It provides funds (subsidies) and/or information, such as data on foreign technology policy and research capabilities, to government and private-sector organizations for research and development projects. It also coordinates government-industry policies, for example, by routing information toward those who will benefit from it and facilitates technology diffusion and transfer.

One organization that has changed its mission is the Asian Office of Aerospace Research and Development. The mission of the Asian Office, which was reestablished in Tokyo, was changed

---

to include monitoring more applied technology, which may be useful to industry, as well as the basic technology on which they have traditionally focused.

Despite its industry orientation, MITI has been likened to a military intelligence service, choosing targets based on the basis of national interest and coordinating collection. For example, in 1976 MITI set up a Committee on Information and Acquisitions in its Electrotechnical Laboratory to monitor developments in the US computer industry. Funds were available to purchase information from individuals in the United States who were willing to sell it, whether legally or illegally, through front companies set up by MITI or by way of consulting contracts with employees of US computer firms.

This information was instrumental in Japan's subsequent ability to dominate the field of microelectronics. Since the 1980s, MITI has been running the same type of operation against the US biotech and aerospace industries.

The Japanese Government primarily collects foreign technology information through MITI-sponsored organizations. In response to requests from government organizations, industry, and academia, the Japan External Trade Organization (JETRO), MITI's primary information collection organization, collects foreign technology information through its extensive network of offices in Japan and overseas and disseminates it to requesters.

Because of the cozy relationship between MITI and industrialists, Japan established an impressive collection system. JETRO is its key organization, but all Japan's services abroad and all individuals on foreign travel, whether for professional purposes or not, were part of it. The system's strength is in the "symbiosis between state and industry and in the overall consensus on the pooling of information."<sup>3</sup>

The role of JETRO in collecting foreign intelligence is legendary. Created in 1958 as part of MITI's International Trade Administrative

Bureau to support foreign trade, JETRO's unofficial major task has been to collect intelligence on foreign business strategies, trade secrets—now illegal under the Economic Espionage Act of 1997—and new technologies. Overall, JETRO has 1,300 staff in a total of 79 offices worldwide, seven of which are in the United States—Atlanta, Chicago, Denver, Houston, Los Angeles, New York, and San Francisco.

Despite these government efforts, many Japanese Government officials and industry representatives said that Japanese companies are the primary collectors of specific information on foreign technologies.<sup>4</sup> This is true particularly for large firms, such as Nippon Electronics Corporation, that have extensive, in-house capabilities to monitor and disseminate foreign technology information within the company. Japanese businessmen are voracious consumers of technical information. In addition, the Japanese Government and private sector have relatively easy access to US technology information because many Japanese, including scientists and engineers, speak and read English, and much of the US research and development is done in an open university system.

A typical trading company collects about 100,000 pieces of information from its 10,000 plus employees in about 180 offices worldwide and spends over \$60 million annually to maintain its collection infrastructure. Many overseas branches of Japanese companies are located near high-technology centers, which in the United States include Silicon Valley, the Route 128 corridor in Massachusetts, the Rockville area of Maryland, and Northern Virginia.

Besides helping Japan keep up with the latest developments in technology, their strategic locations facilitate negotiation of joint ventures with high-tech and capital-starved US startups as a means of acquiring promising new technology. It also allows direct recruitment of local scientists, technical experts, and employees of competing firms with inside knowledge of that firm's technology.

---

Japan does recruit human sources but unlike Western intelligence services that recruit individuals to spy against their organization, Japan uses two other methods. The first is a vigorous hiring campaign conducted by Japanese companies in sectors judged by MITI and the companies themselves to be of importance. For example, in one issue of an industry magazine, Toshiba America Electronics Components, Inc., a Silicon Valley subsidiary of the Japanese electronics manufacturers, ran an advertisement asking US semiconductor engineers with three or more years experience to become part of “the new wave of VLSI technology.” A few pages later, Fujitsu Microelectronics in San Jose, California, invited experienced computer engineers to “imagine a world without any boundaries.” The ad promised that, “We’re not about to put limits on your creativity either.” In the same issue, HAL Computer Systems, another Fujitsu subsidiary in Silicon Valley, tried to interest US software engineers in joining “The Dawn of a New Era.”

The second technique used is where Japanese employees of local subsidiaries seek personal relationships with specialists at nearby US companies who are in a position to provide technical information. Occasionally, these efforts to suborn US employees are detected. An example of this occurred when Hitachi and Mitsubishi Electric tried to obtain proprietary technology illegally from an IBM employee through a Silicon Valley-based consulting company. In another exposed operation, Japanese agents in San Francisco recruited a mid-level engineer at Fairchild, who between 1977 and 1986 passed some 160,000 pages of research results to the consultants of Japanese companies.

An effective addition to the above methods is Japan’s extensive use of travelers to collect information. Japanese companies have a history of sending individual businessmen abroad on technology-gathering missions. The effort began in the 1950s with government-subsidized expeditions primarily to the United States to scout out and obtain new technologies. It continues today with as many as 10,000 trips annually reported. Collection

goals can be generic or technology specific. Also important are the 15,000 plus Japanese scientists and engineers staying in the United States at high-tech companies or US Government-funded laboratories under exchange programs or “co-development” projects.

Representatives of Japanese organizations attend symposiums and international conferences, collect technical literature, and visit laboratories and individual scientists. Japanese officials emphasized that it was useful to establish and maintain informal networks with other Japanese and foreign scientists. Japanese officials use journals, reports, newsletters, databases, facsimiles, the Internet, and workshops to disseminate information.

Japanese Government and private-sector officials cited four elements that they believe contribute to a successful system for collecting and disseminating foreign technology information. They are targeted data collection, a cooperative government-industry relationship, treatment of foreign technology monitoring as an integral part of their operations, and establishment of operations in the target country.

One important element of an effective information collection and dissemination effort cited by the Japanese is that it be demand driven. In other words, the needs of the users of the information must be identified and met for the collection to be successful. For example, JETRO regularly uses inquiries to survey its customers’ needs and determine the best dissemination method. JETRO, among other activities, gathers information for private companies on technologies and markets based on specific requests for information, in much the same way that a consulting company would tailor information to a client’s strategic and operational needs.

According to Japanese officials, the Japanese Government and industry have a very effective government-industry relationship that contributes to the flow of foreign technology information among various organizations. In addition, Japanese company officials said that one of their most useful

---

methods of obtaining information is participating in government-sponsored research and development projects where several Japanese companies are involved.<sup>5</sup>

A State Department official said that there is a more cooperative government-industry relationship in Japan than in the United States because the Japanese Government does not restrict the flow of information to the private sector. He said that the Japanese Government has fewer security and copyright restrictions on information due to its more informal process of disseminating information. For example, the Japanese Government provides information to Japanese industry associations that condense and repackage the information.

Another effective element cited by the Japanese is that those organizations treat foreign technology monitoring as an integral part of their operations. Rather than having separate, specific offices for this activity, researchers, scientists, and others throughout the organizations monitor foreign technology information. For example, the Japanese research and development consortium for superconductor technology expects all its researchers to stay abreast of foreign technology developments in their field as part of their work

## Endnotes

<sup>1</sup> Much of the information in this article comes from a Government Accounting Office report, "Foreign Technology: Collection and Dissemination of Japanese Information Can Be Improved," GOA/NSIAD-93-251, 30 September 1993. It has been updated with additional information.

<sup>2</sup> *Japan-U.S. Economic Issues: Investment, Saving, Technology, and Attitudes*, Congressional Research Office, 2 February 1990.

<sup>3</sup> Jean-Francois Daguzan, "From Intelligence to Lobbying," *Paris Le Nouvel Economiste*, 18-31 May 2001.

<sup>4</sup> Japan also has networks of related companies and financial institutions called *keiretsu* that provide means for information exchange as well as risk sharing and mutual problem solving. See *Competitiveness Issues: The Business Environment in the United States, Japan, and Germany* (GAO/GGD-93-124, August 9, 1993).

<sup>5</sup> Officials from a US company said that foreign technology information is also obtained from negotiating a coproduction agreement, even when the company decides not to do the project. Coproduction is overseas production based on government-to-government agreement that permits a foreign government or producer to acquire the technical information to manufacture all or part of a US-origin defense article.

## The South Korean National Intelligence Service<sup>1</sup>

### Background

The South Korean National Assembly easily elected Syngman Rhee president in 1948, but almost immediately, Rhee ran into difficulties. Most of Rhee's efforts during his time in office (1948-60) involved his own personal struggle to stay in power against his opponents trying to unseat him. Constitutional provisions concerning the presidency became the focal point.

The South Korean constitution called for a four-year term limit on the presidency. Because Rhee had little prospect of being reelected by the National Assembly, he tried to get a constitutional amendment passed in the National Assembly in November 1951 to elect the president by popular vote. This proposal was resoundingly defeated by a vote of 143 to 19, prompting Rhee to marshal his supporters in the Liberal Party. Four months later, in April 1952, the opposition introduced another motion calling for a parliamentary form of government. In response, Rhee declared marshal law in May, rounded up the assembly members by force, and called for another vote. His constitutional amendment to elect the president by popular vote was railroaded through, passing with 163 votes of the 166 assembly members present. In the subsequent popular election in August 1952, Rhee was reelected by 72 percent of the voters.

The constitution, however, limited the president to only two terms. Hence, when the end of Rhee's second term of office approached, the constitution again was amended in November 1954 by the use of fraudulent tactics that allowed Rhee to succeed himself indefinitely.

In the meantime, South Koreans—particularly the urban masses—had become more politically astute. The press frequently exposed government ineptitude and corruption and attacked Rhee's authoritarian rule. The Democratic Party capitalized on these issues, and in the presidential election of May 1956, Rhee won only 55 percent of

the votes, even though his principal opponent—Sin Ik-hui—had died of a heart attack ten days before the election. Rhee's running mate, Yi Ki-bung, fared much worse, losing to the Democratic Party candidate, Chang Myon (John M. Chang). Since Rhee was already 81 years old in 1956, Chang's victory caused a major tremor among Rhee's supporters.

Thereafter, the issue of Rhee's age and the goal of electing Yi Ki-bung became an obsession. The administration became increasingly repressive as Liberal Party leaders came to dominate the political arena, including government operations, around 1958. Formerly Rhee's personal secretary, Yi and his wife (Mrs. Rhee's confidant and a power behind the scenes) had convinced the childless Rhee to adopt their son as his legal heir. For fear that Rhee's health might be impaired, he was carefully shielded from all information that might upset him. Thus, the aged and secluded president became a captive of the system he had built, rather than its master.

In March 1960, the Liberal Party managed to reelect Rhee and to elect Yi Ki-bung vice president by the blatant use of force. Rhee was reelected by default because his principal opponent had died while receiving medical treatment in the United States just before the election. As for Yi, he was largely confined to his sickbed—a cause of public anger—but won 8.3 million votes as compared to 1.8 million votes for Chang Myon. The fraudulent election touched off civil disorders, known and celebrated as the April 19 Student Revolution, during which the police killed 142 students. As a result, Rhee resigned on 26 April 1960. The next day, all four members of Yi's family died in a suicide pact. This account has been challenged by some who believe Yi's bodyguards killed the family in hopes of enabling Rhee to stay on.

Rhee's resignation left a political void subsequently filled by Ho Chong, whom Rhee had appointed foreign minister the day before he resigned. Although Ho was a lifelong friend of Rhee, he had maintained amicable relations with Democratic Party leaders and was acceptable to all concerned.

---

Between April and July 1960, Ho's transitional government maintained order, exiled Rhee and his wife to Hawaii, and prepared for a new general election of the National Assembly in July. The transitional government revised the constitution on 15 June, instituting a parliamentary form of government with a bicameral legislature. In the election of July 1960, the Democratic Party won 175 of the 233 seats in the lower house of the National Assembly. The second-largest group, the independents, won 49 seats. The Liberal Party won only two seats. In the upper house, the Democratic Party won 31 of the 58 seats.

The Democratic Party had been a coalition of two divergent elements that had merged in 1955 to oppose Rhee. When the common enemy—Rhee and his Liberal Party—had been removed from the scene and opportunities for power were presented, each group sought to obtain the spoils for itself.

The Democratic Party candidate for the presidency in the March 1960 election, Cho Pyong-ok, died of illness shortly before the election, just as his predecessor, Sin Ik-hui, had in 1956. The two divergent Democratic Party groups openly struggled against each other during the elections in July for the National Assembly. Although they agreed on Yun Po-son as presidential candidate and Chang Myon as their choice for premier, neither had strong leadership qualities nor commanded the respect of the majority of the party elite. During its brief eight-month term—beginning October 1960—a parliamentary-cabinet system was introduced similar to that which exists in the United Kingdom, and efforts were made to decentralize and curb the powers of the executive. Yun and Chang could not agree on the composition of the cabinet. Chang attempted to hold the coalition together by reshuffling cabinet positions three times within a five-month period. In November 1960, the group led by Yun left the Democratic Party and formed the New Democratic Party.

In the meantime, the tasks confronting the Chang's new government were daunting. The economy suffered from mismanagement and corruption. The army and police needed to be purged of

the political appointees who had buttressed the dictatorship. The students, to whom the Democratic Party owed its power, filled the streets almost daily, making numerous wide-ranging demands for political and economic reforms, but the Democratic Party had no ready-made programs. Law and order could not be maintained because the police, long an instrument of the Rhee government, were demoralized and totally discredited by the public. Continued factional wrangling caused the public to turn away from the party.

This situation provided a fertile ground for a military coup. Rhee had been able to control the military because of his personal prestige, his skill in manipulating the generals, and the control mechanisms he had instituted; Chang lacked all these advantages. When the demands of the young army officers under Maj. Gen. Park Chung Hee were rebuffed, and as political power appeared to be increasingly hanging in the balance with no one clearly in charge, the army carried out a coup d'état on 16 May 1961. Chang's own army chief of staff, Chang To-yong, joined the junta, and Chang Myon's fragile government was toppled. (The junta subsequently tried and convicted General Chang for attempting to take over the junta.) The young officers' initial complaint had been that Chang Myon had not kept a campaign pledge to weed out corrupt generals from the South Korean army, and some Korean sources attributed this failure to the intervention of high-ranking US military officers, who feared the weakening of South Korea's national security.

Yun Po-son, leader of the New Democratic Party, sided with the junta and persuaded the US Eighth Army and the commanders of various South Korean army units not to interfere with him and his party. Yun stayed on as president for ten months after the military junta seized power, thereby legitimizing the coup. A small number of young officers commanding 3,600 men had succeeded in toppling a government with authority over an army of 600,000.

The junta under Maj. Gen. Park Chung Hee quickly consolidated its power, removed those it considered

---

corrupt and unqualified from government and army positions, and laid plans for the future. The 32-member Supreme Council for National Reconstruction became all powerful.

### **The Creation of the Korean Central Intelligence Agency**

The Korean Central Intelligence Agency (KCIA) was originally established on 19 June 1961 to prevent a countercoup and to suppress all potential enemies. Its duties were to “supervise and coordinate both international and domestic intelligence activities and criminal investigation by all government intelligence agencies, including that of the military.” The KCIA had the power to arrest and detain anyone suspected of wrongdoing or harboring antijunta sentiments. Its mission was akin to that of a combined US Central Intelligence Agency and Federal Bureau of Investigation.

The first head of the KCIA was Kim Chong-p’il. Kim utilized the existing Army Counterintelligence Corps to build a 3,000-member organization—the most powerful intelligence and investigative agency in the republic. The KCIA maintained a complex set of interlocking institutional links to almost all of the government’s key decisionmaking bodies. The KCIA had a near monopoly over crucial information concerning national security under the charter of the Act Concerning Protection of Military Secrets and, more important, possessed considerable veto power over other agencies through its supervisory and coordination functions.

The KCIA’s practically unlimited power to investigate and to detain any person accused of antistate behavior severely restricted the right to dissent or to criticize the regime. The frequent questioning, detention, or even prosecution of dissidents, opposition figures, and reporters seriously jeopardized basic freedoms and created an atmosphere of political repression.

Under Park, the lack of advancement in civil liberties continued to be justified by referring to the threat from North Korea. The political influence

of the Ministry of Home Affairs and the police declined in the face of the KCIA’s power. The relationship between the police and general public, however, was not significantly altered. As Se-Jin Kim wrote in 1971: “The former still act with arbitrary arrogance; the latter respond with fear but not respect.”

The government often used martial law or garrison decree in response to political unrest. From 1961 to 1979, martial law or a variant was evoked eight times. The garrison decree of 15 October 1971, for example, was triggered by student protests and resulted in the arrest of almost 2,000 students. A year later, on 17 October 1972, Park proclaimed martial law, disbanded the National Assembly, and placed many opposition leaders under arrest. In November, the *yusin* constitution (*yusin* means revitalization), which greatly increased presidential power, was ratified by referendum under martial law.

The government grew even more authoritarian, governing by presidential emergency decrees in the immediate aftermath of the establishment of the *yusin* constitution; nine emergency decrees were declared between January 1974 and May 1975. The Park regime strengthened the originally draconian National Security Act of 1960 and added an even more prohibitive Anticommunism Law. Under those two laws and Emergency Measure Number Nine, any kind of antigovernment activity—including critical speeches and writings—was open to interpretation as a criminal act of “sympathizing with communism or communists” or “aiding antigovernment organizations.” Political intimidation, arbitrary arrests, preventive detention, and brutal treatment of prisoners were not uncommon.

Opposition to the government and its harsh measures increased as the economy worsened in 1979. Scattered labor unrest and the government’s repressive reactions sparked widespread public dissent resulting in mass resignation of the opposition membership in the National Assembly and student and labor riots in Pusan, Masan, and Ch’angwon. The government declared martial law

---

in the cities. In this charged atmosphere and under circumstances that appeared related to dissatisfaction with Park's handling of the unrest, on 26 October 1979, KCIA chief Kim Chae-gyu killed Park and the chief of the Presidential Security Force—Ch'a Chich'ol—and then was himself arrested. [The nominal Prime Minister Ch'oe Kyo-ha became president.] Emergency martial law was immediately declared to deal with the crisis, placing the head of the Defense Security Command—Maj. Gen. Chun Doo Hwan—in a position of considerable military and political power.

After the assassination in 1979 of President Park by the KCIA director, the KCIA was purged and temporarily lost much of its power. Chun Doo Hwan used his tenure as acting director of the KCIA from April to July 1980 to expand his power base beyond the military. The slow pace of reform led to growing popular unrest. In early May 1980, student demonstrators protested a variety of political and social issues, including the government's failure to lift emergency martial law imposed following Park's assassination. The student protests spilled into the streets, reaching their peak during the period 13 to 16 May, at which time the student leaders obtained a promise that the government would attempt to speed up reform. The military's response, however, was political intervention led by Lt. Gen. Chun Doo Hwan, then KCIA chief and army chief of staff. Chun had forced the resignation of Ch'oe's cabinet; banned political activities, assemblies, and rallies; and arrested many ruling and opposition politicians. In Kwangju, demonstrations to protest the extension of martial law and the arrest of Kim Dae Jung—the leading opposition candidate who later became president on 18 December 1997—turned into rebellion as demonstrators reacted to the brutal tactics of the Special Forces sent to the city. The government did not regain control of the city for nine days, after some 200 deaths.

### **Agency for National Security Planning**

The KCIA was renamed the Agency for National Security Planning (NSP), and its powers were

redefined in presidential orders and legislation. The NSP, like its predecessor, was a cabinet-level agency directly accountable to the president. The director of the NSP continued to have direct presidential access. In March 1981, the NSP was redesignated as the principal agency for collecting and processing all intelligence. The requirement for all other agencies with intelligence-gathering and analysis functions in their charters to coordinate their activities with the NSP was reaffirmed.

Legislation passed at the end of 1981 further redefined the NSP's legally mandated functions to include the collection, compilation, and distribution of foreign and domestic information regarding public safety against communists and plots to overthrow the government. The maintenance of public safety with regard to documents, materials, facilities, and districts designated as secrets of the state was the purview of the NSP. Also under NSP's authority was the investigation of crimes of insurrection and foreign aggression, crimes of rebellion, aiding and abetting the enemy, disclosure of military secrets, and crimes provided for in the Act Concerning Protection of Military Secrets and the National Security Act. The investigation of crimes related to duties of intelligence personnel, the supervision of information collection, and the compilation and distribution of information on other agencies' activities designed to maintain public safety also were undertaken by the NSP. By 1983, the NSP had rebounded and again was the preeminent foreign and domestic intelligence organization.

Public discontent was kept under control until 1987 by the regime's extensive security services—particularly the Agency for National Security Planning, the Defense Security Command (DSC), and the Combat Police of the Korean National Police (KNP). Both the civilian NSP and the military DSC not only collected domestic intelligence but also continued “intelligence politics.” The Act Concerning Assembly and Demonstration was used to limit the expression of political opposition by prohibiting assemblies likely to “undermine” public order. Advanced

---

police notification of all demonstrations was required. Violation of the act carried a maximum sentence of seven years' imprisonment or a fine. Most peaceful nonpolitical assemblies took place without government interference. However, the act was the most-frequently-used tool to control political activity in the Fifth Republic, and the Chun regime was responsible for more than 84 percent of the 6,701 investigations pursued under the act.

The security presence in city centers, near university campuses, government and party offices, and media centers was heavy. Citizens, particularly students and young people, were subject to being stopped, questioned, and searched without due process. The typical response to demonstrations was disruption by large numbers of Combat Police, short-term mass detention of demonstrators, and selective prosecution of the organizers. Arrest warrants—required by law—were not always produced at the time of arrest in political cases.

The National Security Act increasingly was used after 1985 to suppress domestic dissent. Intended to restrict “anti-state activities endangering the safety of the state and the lives and freedom of the citizenry,” the act also was used to control and punish nonviolent domestic dissent. Its broad definition of offenses allowed enforcement over the widest range, wider than that of any other politically relevant law in South Korea. Along with other politically relevant laws such as the Social Safety Act and the Act Concerning Crimes Against the State, the National Security Act weakened or removed procedural protection available to defendants in nonpolitical cases.

Questioning by the security services often involved not only psychological or physical abuse but also outright torture. The torture and death of Pak Chong-ch'ol in 1987, a student at Seoul National University being questioned as to the whereabouts of a classmate, played a decisive role in galvanizing public opposition to the government's repressive tactics.

The security services not only detained those accused of violating laws governing political

dissent but also put under various lesser forms of detention—including house arrest—those people, including opposition politicians, who they thought intended to violate the laws. Government agents subjected many political, religious, and other dissidents to surveillance. Opposition assembly members later charged in the National Assembly that telephone tapping and the interception of correspondence were prevalent. Ruling party assembly members, government officials, and senior military officials probably also were subjected to this interference although they did not openly complain.

Use of tear gas by the police (more than 260,000 tear gas shells were used in 1987 to quell demonstrations) increasingly was criticized. The criticism eventually resulted in legal restrictions on tear gas use in 1989. The government continued, however, to block many “illegal” gatherings organized by dissidents that were judged to incite “social unrest.” In 1988, government statistics noted 6,552 rallies involving 1.7 million people. There were 2.2 million people who had participated in 6,791 demonstrations in 1989.

Listening to North Korean radio stations remained illegal in 1990 if it were judged to be for the purpose of “benefiting the anti-state organization” (North Korea). Similarly, books or other literature considered subversive, procommunist, or pro-North Korean were illegal; authors, publishers, printers, and distributors of such material were subject to arrest.

As of 1990, the organizational structure of the NSP was considered classified by Seoul, although earlier organizational information was public knowledge. Despite the social and political changes that came with the Sixth Republic, the NSP apparently still considered the support and maintenance of the president in power to be one of its most important roles. In April 1990, for example, ruling Democratic Liberal Party (DLP) coleader Kim Young Sam complained that he and members of his faction within the DLP had been subjected to “intelligence maneuvering in politics” that

---

included wiretapping, surveillance, and financial investigations.

Nevertheless, the NSP's domestic powers were indeed curtailed under the Sixth Republic. Prior to the change, the NSP had free access to all government offices and files. The NSP, Defense Security Command, Office of the Prosecutor General, Korean National Police, and the Ministry of Justice had stationed their agents in the National Assembly to collect information on the activities of politicians. In May 1988, however, overt NSP agents, along with agents of other intelligence agencies, were withdrawn from the National Assembly building. The NSP's budget was not made public nor apparently was it made available in any useful manner to the National Assembly in closed sessions. In July 1989, pressured by opposition parties and public opinion, the NSP was subjected to inspection and audit by the National Assembly for the first time in 18 years. The NSP removed its agents from the chambers of the Seoul Criminal Court and the Supreme Court in 1988.

As of 1990, however, the NSP remained deeply involved in domestic politics and was not prepared to relinquish the power to prevent radical South Korean ideas—much less North Korean ideas—from circulating in South Korean society. Despite an agreement in September 1989 by the chief policymakers of the ruling and opposition parties to strip the NSP of its power to investigate pro-North Korean activity (a crime under the National Security Act), the NSP continued enforcing this aspect of the law rather than limiting itself to countering internal and external attempts to overthrow the government. The NSP continued to pick up radical student and dissident leaders for questioning without explanation.

In another move to limit the potential for the NSP to engage in “intelligence politics,” the NSP Information Coordination Committee was disbanded because of its history of unduly influencing other investigating authorities, such as the Office of the Prosecutor General. In addition, the NSP, responding to widespread criticism of its alleged human rights violations, set up

a “watchdog” office to supervise its domestic investigations and to prevent agents from abusing their powers while interrogating suspects.

Aside from its controversial internal security mission, the NSP also was known for its foreign intelligence gathering and analysis and for its investigation of offenses involving external subversion and military secrets. The National Unification Board and the NSP (and the KCIA before it) were the primary sources of government analysis and policy direction for South Korea's reunification strategy and contacts with North Korea. The intelligence service's reputation in pursuing counterespionage cases also was excellent.

The NSP monitored visitors, particularly from communist and East European countries, to prevent industrial and military espionage. Following the diplomatic successes of the late 1980s—the establishment of diplomatic relations with the Soviet Union and the countries of Eastern Europe and the increased informal contacts with China, Mongolia, and Vietnam—this mission grew in importance. The security watch list contained 162 out of 3,808 visitors from communist nations in 1988 and 226 out of 6,444 visitors in 1989.

In 1995, by relocating to a new intelligence building equipped with up-to-date facilities in Naegok-dong (southern Seoul) from its 34-year-old site in Mt. Nam in downtown Seoul and Imundong (eastern Seoul), the NSP laid the cornerstone to become a 21st century, advanced intelligence agency. With the inauguration of the People's Government on 22 January 1999, the agency was renamed the National Intelligence Service (NIS). The former Minister of Defense Chun Yong-taek took office as the 23rd Director General of the National Intelligence Service on 26 May 1999. He had served as National Assemblyman, Party member of the Government of the People, Minister of Defense, and Lieutenant General in the armed forces reserve.

National Intelligence Service missions and functions include:

- Collection, coordination, and distribution of information on the nation's strategy and security.
- Investigation of crimes affecting national security, including crimes that violate the Military Secrecy Protection Law and the National Security Law that prohibit the incitement of civil war, foreign troubles, and insurrection.
- Investigation of crimes related to the missions of NIS staff.
- Maintenance of documents, materials, and facilities related to the nation's classified information.
- Planning and coordination of information and classified information.

### **Government and Private-Sector Efforts To Steal US Technological Secrets**

In the mid-1990s, South Korean media began reporting that, over the past two years, the Republic of Korea (ROK) Government and South Korean companies were engaging in systematic efforts to obtain foreign proprietary technology through indirect methods. Faced with a decline in the competitiveness of its products, the high cost of buying foreign technology, and the difficulty of developing new technology through its own resources, South Korea reportedly contrived a host of oblique means to access the technological secrets of advanced countries.

According to these ROK press reports, these techniques ranged from the use of academic exchange programs to the use of the country's intelligence service for industrial espionage. Several of these technical acquisition programs reportedly targeted US citizens through databases and through recruitment programs focused on expatriate Koreans. Many such initiatives reportedly were designed and managed by the ROK Government itself. The press described South Korea's methods to obtain foreign technology, particularly from US companies. Of note, the press reported that ROK firms were losing interest in

Japan, traditionally South Korea's main technology source, because the Japanese demanded high royalties for technology transfers.

The most-wanted technologies sought from the United States by South Korean companies and government research institutes were aerospace, automobiles, bioengineering, computers, communications, electronics, environmental, machinery and metals, medical equipment, nuclear power, and semiconductors. Within these areas, the South Koreans frequently targeted electronics, data communications and processing, and semiconductor technology—South Korea's major high-tech export fields. These data were based on reported cases of attempted technology transfer and press reports of the targeted fields. Within the frequently targeted group, the highest priorities included high-speed CD-ROM, ultra-high-resolution monitor design, traffic-control systems, flash memory, digital signal processors, application-specific integrated circuits of all types, cable television converters, digital communications, image-data processing, asynchronous transmission-mode technology, fiber optics, and audio-video compression technology.<sup>2</sup>

South Korea's eagerness to assimilate foreign technology without paying royalties is reflected in the variety of indirect transfer techniques:

- Academic cooperation:
  - *Centers of excellence.* Setting up "centers" staffed by leading foreign institutes provides ROK researchers with opportunities to "come into contact" with high-level scientists and advanced equipment.<sup>3</sup>
  - *Academic exchanges.* Under this strategy, the South Korean Government sends ROK researchers abroad to acquire advanced technology through their studies.<sup>4</sup>
  - *Technical links to foreign universities.* Large South Korean manufacturers form "international industrial-academic cooperative associations" with foreign universities to do "joint research" in advanced technology.<sup>5</sup>

- 
- International cooperation:
    - *International research projects.* Because the initial focus of this research is noncommercial, foreign companies reportedly are more willing to share their technology than they would through conventional channels.<sup>6</sup>
    - *International forums and foundations.* The South Korean Government has sanctioned the establishment of “S&T forums” to act as a corridor between the ROK’s commercial science and technology (S&T) establishment or state-subsidized “foundations” and US high-tech companies to facilitate the transfer of US technology.<sup>7</sup>
  - Cooperation between South Korea and foreign companies:
    - *Strategic cooperation.* This process involves identifying gaps in indigenous technology, finding a foreign company that has the technology, and engaging the latter in some kind of cooperative relationship that results in the transfer of the technology to South Korea.<sup>8</sup>
    - *Joint “research” and development.* When South Korean technicians obtain foreign technology through the development process as part of a transfer agreement, which the South Korean press described as “joint development”.<sup>9</sup>
  - Obtaining foreign patents:
    - *Bargain basement patents.* A large number of ROK firms and research institutes have been obtaining needed technology through cheap patents acquired in Russia.<sup>10</sup>
    - *Buyouts of foreign firms.* ROK press reports reveal that buyouts of high-tech foreign companies are another popular way to obtain patented technology.<sup>11</sup>
  - Employing foreign talent:
    - *Hiring overseas specialists.* Hiring foreign experts is another favored, low-cost means used by South Korea to transfer technology indirectly; it is recommended by government experts, facilitated by official and semiofficial ROK organizations, and widely practiced in ROK industries.<sup>12</sup>
    - *“Brain pools.”* South Korea’s government and industry also operate systems to identify potential recruits who are in a position to transfer high-level technology and, because of their ethnicity, are predisposed to accept offers to “contribute” their knowledge to South Korea.<sup>13</sup>
  - Direct overseas involvement:
    - *Overseas technical training.* On-site training at overseas companies allows South Korea to obtain technology at a fraction of its market cost.<sup>14</sup>
    - *Establishing overseas subsidiaries.* Judging by press reports, South Korean firms have also discovered that overseas branches provide another shortcut to technology transfer.<sup>15</sup>
    - *Overseas “research centers.”* In addition to obtaining technology through overseas subsidiaries, South Korean companies acquire foreign technology by establishing “research” facilities abroad and staffing them with host-country scientists who transfer knowledge of technological processes to their employers, according to ROK press reports.<sup>16</sup>
  - Collection networks:
    - *International trade organizations.* The Korea Trade Promotion Corporation—an ROK Government–run organization that is officially chartered to facilitate the export of South Korean products and that has 81 overseas trade offices—also promotes technology transfer.<sup>17</sup>
    - *Employees as intelligence collectors.* ROK firms also have discovered that ordinary employees can yield a wealth of information on competitors’ technologies and plans. Although this does not necessarily lead to technology transfer, it does allow corporations to get a pulse on worldwide research and development (R&D) activities and to use this information in its own policies.<sup>18</sup>

---

— *Ethnic and personal relationships.* Substantial media documentation exists on South Korea’s interest in exploiting the ethnicity of overseas Koreans to obtain commercial and technological information.<sup>19</sup>

— *Foreign databases.* ROK Government institutes have also helped facilitate the transfer of technology by providing South Korean companies access to foreign databases with industrial, scientific, and technological data from foreign and domestic sources.<sup>20</sup>

- Commercial espionage:
  - *National intelligence service.* South Korea’s NSP is also involved in the indirect transfer of foreign technology.<sup>21</sup>
  - *Corporate spying.* In addition to government-sanctioned efforts to collect technological information, Seoul media report widespread industrial espionage by South Korean companies against each other to obtain a competitor’s proprietary technology.<sup>22</sup>

### South Korea’s Informal Technology Acquisitions

Despite its efforts, South Korea continued to suffer economic difficulties during the mid-1990s. As part of its uphill struggle to break out of its economic doldrums, South Korea increased its efforts to obtain foreign proprietary technology, according to Seoul media reports. Mechanisms through which enhanced collection activity was reported included “joint research,” recruitment of foreign nationals, outposts located in high-tech regions abroad, expatriate scientists, and the National Intelligence Service’s apparatus. In addition, the South Korean Government reportedly formed a new committee to systematize foreign technology collection and expand the number of overseas collectors.

The South Korean press reported an intensification of the country’s efforts to obtain foreign technology through informal channels that was attributed, in part, to strains in the ROK economy. While

earlier collection efforts were motivated by what the media described as a shortage of “wellspring technology,” other factors such as “snowballing” royalty payments<sup>23</sup> and the then–financial crisis were cited as causes for renewed emphasis on this practice.

South Korea’s national laboratories were tasked by the government to “help domestic industry overcome the economic crisis” by rendering “practical” support for new product development and by “Internationalizing their research activities.”<sup>24</sup> Examples of the latter included the Korea Institute of Science and Technology’s (part of the Ministry of Science and Technology—MOST) program to “conduct personnel exchanges, information interchange, and joint research with 57 institutions in 19 countries.” The Korean Institute of Machinery and Metals’ (another MOST affiliate) planned to set up joint R&D centers at Stanford University and MIT to “acquire leading future technologies.” South Korea also sought US Government backing to expand these “cooperative exchanges” across a wide range of “state-of-the-art technologies.”<sup>25</sup>

European countries also were increasingly targeted as sources of new technology. South Korean science officers stationed at 10 ROK Government–funded research centers in Europe and Russia met in Paris to discuss ways to boost their research activity, described by one officer as the “systematic gathering of information on [host country] research institutes, technologies, and personnel.”<sup>26</sup>

Direct exploitation of overseas scientists by ROK Government institutions was being stepped up by expanding the “brainpool” project according to an Internet posting by the Korea-American Scientists and Engineers Association (KSEA), read on 2 February 1998 through a mirror site in Seoul. Administered by MOST and executed through eight national chapters (United States, Canada, United Kingdom, France, Germany, Japan, China, and Australia) of the Seoul-based General Federation of Korean Science and Technology Organizations, the project offers salaries and expenses to “outstanding scientists and engineers

---

from overseas” to share their knowledge in “all fields of science and technology” with their counterparts at ROK national and corporate laboratories. In previous years, the notices capped the number of positions to a few dozen, whereas in 1998, the solicitation appeared to be open-ended.

ROK companies likewise were increasingly eager to tap the expertise of foreign scientists. The major groups’ electronic subsidiaries “launched an aggressive ‘head hunting’ operations” overseas aimed at scientists and engineers in electronics and information science.<sup>27</sup> Samsung Electronics reportedly held briefing sessions and recruitment exhibitions “at major universities and research institutes in the United States and Europe.” LG Electronics, Hyundai Electronics (through the use of an Internet-based “manpower management program”) and Daewoo Electronics matched Samsung’s efforts. It was noted that Daewoo, in particular, was “securing competent employees overseas by using Korean students studying abroad on company scholarships, its overseas branches, and its own research institutes established in the United States, Japan, and Europe as an information network. The overseas recruitment of scientific talent was being pursued at the group level and focused not only on established scientists but also on new graduates of prestigious US technical universities.<sup>28</sup>

Besides these company-led efforts, South Koreans were establishing independent “consulting firms” overseas whose function is to “scout out technical manpower for Korean companies” and broker the transfer of “core technologies” to ROK producers.<sup>29</sup> One such company reportedly was established in Moscow by “specialists engaged in technology transfers from Russia on behalf of large Korean businesses.” Another Korean consulting firm opened offices in Moscow and Los Angeles to “recruit high-tech personnel in data communications.” A personnel officer from an ROK company stated to the effect that fees of \$100,000 are not considered excessive for the services of a top foreign scientist and speculated that “hiring advanced specialists from foreign countries” would increase.<sup>30</sup>

The United States’ Silicon Valley is a favorite venue for informal technology transfers through ROK Government-backed outposts for marketing and “information exchange.” According to a Ministry of Information and Communications (MIC) press release of 17 November 1997, South Korea was funding the creation of “incubators” in Silicon Valley designed both to promote the sale of ROK software products and conduct “technology exchange activities.”

Korea Telecom, a public corporation, was to create a capital fund with ROK communications equipment manufacturers to support Silicon Valley-based American venture enterprises in advanced data communications.<sup>31</sup> The Korea Advanced Institute of Science and Technology (a MOST subsidiary) funded the establishment of a semiconductor equipment-manufacturing firm in Silicon Valley, which is run by expatriate Koreans. The firm reportedly is designed to allow ROK graduate students “to acquire technology at the same time they earn dollars” by performing research with world-class engineers.<sup>32</sup>

Coordinating S&T collection efforts and integrating collection targets with the needs of ROK manufacturers—long a “bottleneck” in South Korea’s informal technology-transfer programs—entered a “new dimension” as a result of programs undertaken by MOST’s Science and Technology Policy Institute (STEPI).<sup>33</sup> According to a report released by STEPI on 9 December 1998 cited by the Korean press, the separate collection programs run by the Ministries of Foreign Affairs, Trade and Industry, National Defense, and Science are to be brought together under a “Science and Technology Foreign Cooperation Committee” meant to systematize collection strategy, integrate local operations, and avoid duplication of effort. The committee reportedly would be divided into groups of specialists by geographical region who would interact with a council composed of working-level personnel from organizations such as the Korea Trade Promotion Agency (KOTRA) and STEPI on the one hand, and national labs, universities, and ROK companies on the other.

---

Reportedly formed to counter the “increasing reluctance of advanced countries to transfer their science and technology,” the program entails establishing local “Korea Centers” to collect foreign S&T information and to set up overseas branches of government bodies, national labs, and companies “to provide information on foreign S&T.”<sup>34</sup> Moreover, to “strengthen overseas S&T collection” and build an information system that would link ROK organizations to overseas sources of technology, STEPI was to create an “Overseas Science and Technology Information Center” that integrates the S&T information collected by “overseas Korean scientists and engineers associations, Korean diplomatic and consular offices in foreign countries, large Korean trading companies, and the overseas offices of national labs.”

In this connection, the Korean-US Science Cooperation Center, an ROK Government-funded S&T collection facility and host to the KSEA, is now five years old. Items posted on its Internet Web site included a comprehensive directory (with hotlinks to major US Government technology centers, national laboratories, and professional scientific organizations), along with an invitation for proposals to create new programs designed to promote S&T cooperation and to help “Korean and American scientists develop and maintain permanent S&T networks.” KSEA, for its part, promoted on its Web site STEPI’s “Creative Research Initiative Program” that sought to fill some 45 South Korean research associate positions with foreign or expatriate scientists in 1998.

In 1997, the president-elect, Kim Dae-jung, drafted reforms for the NSP that entailed an “intensive buildup of economic information-collecting capabilities” against overseas targets.<sup>35</sup>

### **Cooperation Centers To Acquire Technologies**

In March 2001, South Korea’s Small and Medium Business Administration began to screen applicants for admission to a newly established Korea Venture

Center (KVC) in Fairfax County, Virginia. Of the 35 South Korean venture companies that applied for entry into the US-based high-tech “incubator,” 10 were to be selected to receive support at the Center. This support reportedly included subsidized rent and guidance in finding local firms for technical cooperation.<sup>36</sup>

The KVC is the first South Korean center in the eastern United States. Its formation was announced by South Korea’s Ministry of Commerce, Industry, and Energy (MOCIE) as part of that country’s effort to promote “strategic cooperation” with US firms in high-tech corridors of the United States.<sup>37</sup> At its formal opening in late November 2000, KVC Director U Chong-sik reiterated that the Center’s goal is to assist Korean companies in arranging joint R&D with foreign institutions.<sup>38</sup>

The KVC was South Korea’s third information technology (IT) incubator in the United States; the other two being the Overseas Software Support Center (KSI) and the Information and Communications Venture Support Center (I-park) in Silicon Valley, both under the MIC. The 14 companies at KSI were to relocate to I-park at the end of 2001, in connection with a merger of the two facilities that was driven by the need to directly support their clients’ interaction with local high-tech firms.<sup>39</sup>

I-park is involved in technology transfer by “facilitating strategic cooperation with local US companies,” a phrase used in the Korean press to describe programs aimed at acquiring foreign technology.<sup>40</sup> I-park serves as a base of operations for a network of ethnic Korean IT specialists in Silicon Valley, which suggests that the South Korean venture companies are encouraged to pursue technical ties to émigré IT companies already operating in the valley.<sup>41</sup>

I-park’s role as a technology-transfer installation was stated on its Web site, which listed facilitating technology exchanges as a main function. The site acknowledged support from the Institute of Information Technology Assessment (IITA),

---

whose primary Web site identified technology transfer as one of its main projects. The IITA was founded in 1992 as an affiliate of the Electronics and Telecommunications Research Institute (ETRI), now part of MIC, South Korea's state-run telecommunications research facility chartered to disseminate innovative technology to Korean manufacturers.

The link between tech transfer and the KVC/I-park operations is further underscored by IITA's association since October 1999 with Seoul's IT Technology Transfer Center, also referred to as a cyber technomart, which is designed to facilitate the early acquisition of state-of-the-art technology and its commercialization by South Korean manufacturers, according to the Center's Web site. I-park itself is referred to in some Seoul press reports<sup>42</sup> and IITA's "History" pages as the Overseas IT technology cooperation center.

In a related event, MOCIE planned to establish a similar Japan IT venture center in Tokyo at the end of February 2001 to support South Korean venture firms' strategic cooperation with high-tech Japanese telecommunications companies. The new center, based on a Korean-Japan IT cooperation initiative signed in September 2000, reportedly would maintain contact with the KVC in Fairfax County.<sup>43</sup>

### **Science Ministry Continues Foreign Recruitment Drive**

The South Korean Government is continuing its efforts to recruit ethnic Korean scientists abroad to support state and corporate-defined research programs, as evidenced by a Science Ministry posting that called for a transnational "brainpool." The pragmatic nature of these efforts was brought out in the posting, which emphasized the importance of making concrete contributions to the country's S&T agenda.

According to a notice posted in April 2001 on the South Korean Science Ministry's Web site, the ministry, in conjunction with liaison organizations,

renewed its sponsorship of a "brainpool" project to recruit foreign technical specialists willing to share their accumulated expertise with Seoul. The notice read in part:

*The General Federation of Korean S&T Organizations, in accordance with the government's (Ministry of Science and Technology) plan to recruit and make use of high-level overseas scientists (brainpool), is seeking world-class superior overseas scientists and engineers willing to contribute to raising our country's international competitiveness for on-site work at colleges, companies, and South Korean R&D facilities. We hope for your wide participation.*

The notice invited overseas scientists with recognized skills in areas "targeted for national strategic development" to apply. Some 30 different fields were listed, ranging from basic science to applied technology. Employment reportedly involved working with an existing R&D team or one formed around the scientist's area of expertise. Lecturing at seminars and before "scholarly associations" is also an option. Appointments ranged from three months to two years.

The ministry advised that applicants should be "overseas Korean or foreign scientists and engineers" with more than five years postdoctoral experience in a foreign country. However, exceptions would be made for those who demonstrated outstanding research ability or who "possess know-how." Scientists who have worked five years in a foreign firm's research lab need not hold a doctorate.

### **Technology-Transfer Facility in San Diego**

A quasi-official ROK industrial organization was to work with South Korean biotechnology companies to establish a technology-transfer facility in San Diego. The South Korean Government would subsidize the new center, which would facilitate "networking" with local researchers.

---

The Federation of Korean Industries (FKI), which is South Korea's largest industrial organization and serves as an intermediary between ROK companies and government policy makers, proposed in late October 2001 that a "Korea Bio Valley" be set up near San Diego to serve as a focal point for entry of ROK products into the US market and to facilitate acquisition of US biotechnology. FKI's plan called for joint participation by large ROK companies, pharmaceutical makers, and biotech startups in establishing this "bridgehead" into the US "hub" of the life sciences industry.<sup>44</sup>

Bio Valley would support 10 to 15 ROK companies in the Carlsbad district of San Diego. The ROK Government reportedly would buy buildings and other infrastructure and lease them to Korean companies or make them available at no cost. Ten billion won of the 15-billion won budget would be covered by public subscriptions with the remainder provided as a government subsidy.<sup>45</sup> FKI would work with the Korea Bioventure Association, South Korea's major biotech industrial group, to complete the complex by 2001. However, the plans to establish the "Korea Bio-Park" have been hit by delays over budget problems. The Ministry of Commerce, Industry and Energy has yet to set aside a budget for the project. Also, Korean companies and bio-venture firms, which are to help finance the project, are suffering financial difficulties. The plan is currently in limbo.

Bio Valley is part of a larger FKI proposal titled "A Plan for Developing the Biotech Industry (October 2001)" aimed at raising the technology level of domestic biotech firms. According to a copy of the plan posted to FKI's Web site, the main purpose of the US complex is "to grasp in real time the latest advances in biotechnology and trends in the biotech industry." The plan states that Korea's "R&D capability will be improved by making use of top-notch overseas research personnel and networking with them." A secondary goal is noted as promoting "with a minimum investment, the introduction of ROK biotech products into the United States and adjacent countries."

Seoul's move to establish a high-tech "liaison center" in the heartland of the US biotech industry parallels its successful efforts noted above to comb Silicon Valley for information technology, a field where South Korea now enjoys some commanding leads. An example of this approach is the so-called "Information and Communications Venture Support Center" in San Jose, identified recently in South Korean press reports as an information technology-transfer facility sponsored by the ROK Government.

---

## Endnotes

- <sup>1</sup> This article is based on Library of Congress information and articles written by the National Counterintelligence Center and its successor, the National Counterintelligence Executive.
- <sup>2</sup> *Hanguk Kyongje Sinmun*, *Maeil Kyongje Sinmun*, various dates in 1994 and 1995.
- <sup>3</sup> *Maeil Kyongje Sinmun*, 29 January 1995.
- <sup>4</sup> *Korea Herald*, 14 January 1995.
- <sup>5</sup> *Hanguk Kyongje Sinmun*, 23 January 1995.
- <sup>6</sup> *Hanguk Kyongje Sinmun*, 25 June 1994.
- <sup>7</sup> *Maeil Kyongje Sinmun*, 25 May 1994.
- <sup>8</sup> *Maeil Kyongje Sinmun*, 24 January 1994.
- <sup>9</sup> *Maeil Kyongje Sinmun*, 10 January 1995.
- <sup>10</sup> *Hanguk Kyongje Sinmun*, 31 January 1994.
- <sup>11</sup> *Maeil Kyongje Sinmun*, 3 February 1995.
- <sup>12</sup> *Hanguk Kyongje Sinmun*, 13 July 1994.
- <sup>13</sup> *Maeil Kyongje Sinmun*, 19 May 1993.
- <sup>14</sup> *Hanguk Kyongje Sinmun*, 25 March 1993.
- <sup>15</sup> *Hanguk Kyongje Sinmun*, 17 May 1993.
- <sup>16</sup> *Hanguk Kyongje Sinmun*, 16 January 1995.
- <sup>17</sup> *Hanguk Kyongje Sinmun*, 25 July 1994.
- <sup>18</sup> *Hanguk Kyongje Sinmun*, 25 June 1994.
- <sup>19</sup> *Hanguk Kyongje Sinmun*, 14 February 1994.
- <sup>20</sup> *Chonja Sinmun*, 19 March 1994.
- <sup>21</sup> *Changang Ilbo*, 6 May 1993.
- <sup>22</sup> *Hangyore Sinmun*, 29 July 1993.
- <sup>23</sup> Reported in the 5 August 1997 and 30 September 1997 issues of *Chonja Sinmun*.
- <sup>24</sup> *Chonja Sinmun*, 10 January 1998.
- <sup>25</sup> *Yonhap*, 14 January 1998.
- <sup>26</sup> *Chonja Sinmun*, 9 October 1997.
- <sup>27</sup> *Chonja Sinmun*, 30 September 1997.
- <sup>28</sup> *Hanguk Kyongje*, 27 September 1997.
- <sup>29</sup> *Maeil Kyongje Sinmun*, 9 September 1997.
- <sup>30</sup> *Maeil Kyongje Sinmun*, 5 December 1997.
- <sup>31</sup> *Maeil Kyongje Sinmun*, 14 November 1997.
- <sup>32</sup> *Maeil Kyongje Sinmun*, 14 January 1998.
- <sup>33</sup> *Chonja Sinmun*, 10 December 1997.
- <sup>34</sup> *Ibid.*
- <sup>35</sup> *Yonhap*, 26 and 29 December 1997.
- <sup>36</sup> *Chonja Sinmun*, 8 February 2001.
- <sup>37</sup> *Chonja Sinmun*, 20 October 2000.
- <sup>38</sup> *Hanguk Kyongje Sinmun*, 21 November 2000.
- <sup>39</sup> *Chonja Sinmun*, 21 December 2000.
- <sup>40</sup> *Maeil Kyongje Sinmun*, 29 May 2000.
- <sup>41</sup> *Hanguk Ilbo*, 3 September 2000.
- <sup>42</sup> See *Hanguk Kyongje Sinmun*, 7 October 2000.
- <sup>43</sup> *Naewoe Kyongje Sinmun*, 7 December 2000.
- <sup>44</sup> *Chonja Sinmun*, 31 October 2000.
- <sup>45</sup> *Hanguk Kyongje Sinmun*, 31 October 2000.