ONLINE JOURNAL™
www.onlinejournal.com

Special Report

The demise of global communications security

The neocons' unfettered access to America's secrets

By Wayne Madsen
Online Journal Contributing Writer

September 21, 2005—During the Cold War, if the United States suffered a massive compromise of its own cryptographic security and, at the same, time experienced a thorough penetration of its communications intelligence yielding the sensitive sources and methods whereby the U.S. intelligence community tapped and decrypted the communications of its adversaries, the Soviet Union would have been able to dictate surrender terms for America and its allies.

For years, the National Security Agency (NSA) maintained highly classified back doors into the encrypted communications of worldwide foreign ministries, military commands, banks, international organizations, and even the Vatican, the International Committee of the Red Cross, and the United Nations. In addition, the United States spent billions of dollars to develop highly secure cryptographic systems to protect its military, intelligence, and diplomatic communications from the prying ears and eyes of its enemies.

However, according to U.S. intelligence sources with connections to both the Reagan and Clinton administrations, America's most sensitive communications security and cryptologic secrets have been totally compromised by a Fifth Column embedded within the recent past and current administrations—the group generally identified as "neoconservatives," political ideologues rooted in a peculiar blend of Trotskyism and fascism—ideologues who are neither "new" nor "conservative" in ideology but whose intentions are to weaken America's national security to a degree that ruins the very foundations on which the nation was built.

One of the major NSA success stories since its establishment on October 24, 1952, was the rigging of the encryption machines of the Swiss company Crypto AG in a secret deal cut between NSA's William Friedman and Boris Hagelin, the developer of the Hagelin cipher machine used by the Allies in World War II. In 1958, Hagelin, who founded Crypto AG in 1950, agreed to the deal with NSA. It was the height of the Cold War.

For U.S. intelligence, the Hagelin-NSA deal was an intelligence coup on the level of the U.S. breaking of Germany's Enigma code and Japan's Purple code in World War II. Neutral nations trusted a Swiss company to sell encryption machines as highly reliable as Swiss watches and as trusted as Swiss bank accounts. Non-aligned nations like Egypt, Indonesia, Algeria, Afghanistan, Iraq, Mexico, Yemen, Venezuela, Yugoslavia, and Argentina became contented Crypto AG users. Upon independence, Britain's Commonwealth Office offered the British Empire's newly-independent states a sweetheart deal. They could protect their sensitive diplomatic communications with free surplus Hagelin cryptographic machines like the C-52 cipher machine once used by Britain. Nations like India, Pakistan, Ghana, Burma, Ceylon, Nigeria, Kenya, Kuwait, and Jordan enthusiastically accepted the offer along with mechanical modifications to handle non-Latin alphabets like Arabic, Burmese, Thai, and Farsi. The users were unaware that all their coded traffic was an open book to NSA and Britain's Government Communications Headquarters (GCHQ), NSA's British signals intelligence partner in a secret intelligence-sharing pact known as the UK-USA Agreement. French-speaking Crypto AG salesmen had tremendous success in francophone former French and Belgian African colonies to use their ciphering machines after independence. Soon, governments in the Central African Republic, Morocco, Tunisia, Gabon, Upper

Volta, Dahomey, Cameroon, Togo, Congo (Brazzaville), Congo (Kinshasa), Senegal, Malagasy Republic, and Chad were encrypting their communications not aware that everything was being decoded and read by NSA.

Eventually, Crypto AG's encryption machines went digital. The encryption mechanisms, according to a U.S. intelligence source, were contained in an electronically programmable read-only memory (EPROM) unit known as HC6800 (the "HC" standing for "Hagelin Cipher"). As Crypto AG sold more and more of its units to some 120 countries around the world, the NSA's ability to read encrypted traffic was a virtual gold mine of intelligence. Convinced the Swiss firm was an honest broker, the Iranian Islamic regime, Libya's Muammar el Qaddafi, Iraq's Saddam Hussein, the Philippine's Ferdinand Marcos, Ethiopia's Mengistu Haile Mariam, Equatorial Guinea's brutal dictator Francisco Macias Nguema, and Uganda's Idi Amin all scrambled their secret money movements, assassination orders, and clandestine arms deals with Crypto's machines. And everything was known to Washington.

That was until 1983, when the Soviets became aware of the Crypto AG secret project courtesy of the classified information passed to Israel by convicted Israeli spy Jonathan Pollard. The Naval Intelligence Field Operational Intelligence Office employee, in the course of passing a garage-full of classified documents and computer disks to Israeli intelligence, compromised one of NSA's most important sources and methods of intelligence gathering. Included among the classified NSA documents passed to Israel was RASIN (Radio-Signal Notations), the multi-volume TOP SECRET UMBRA encyclopedia of how the NSA collected signals around the world. However, the Crypto AG disclosures were contained in an even higher classified set of documents compromised by Pollard.

Pollard's Scientific Liaison Unit (LAKAM) handler Rafael ("Rafi") Eitan spirited Pollard's intelligence take off to Israel where some of it was traded to the Soviet Union in return for an increase in the number of Soviet Jews permitted to emigrate to Israel. America's ability to read the encrypted traffic of all of Israel's neighbors (Jordan, Egypt, Syria, Lebanon, and Saudi Arabia) was immediately compromised to the detriment of United States interests in the Middle East. Pollard's intelligence also included details of the Pakistani atomic bomb project and the A. Q. Khan nuclear proliferation network. According to a 1999 *New Yorker* article by Seymour Hersh, Pollard had also been involved in trying to broker arms sales to the Afghan rebels in 1985—an activity that would have put the Israeli spy in direct contact with the Mujahideen, which was then bankrolled by the Saudis and included Osama Bin Laden and his nascent future "al Qaeda" terrorists.

Thanks to Pollard's disclosures to the Soviets, NSA's prized collection project was immediately compromised to the KGB and GRU military intelligence. The KGB and GRU found out about the "seed key" used by NSA as a master key" to unlock encoded communications transmitted by Crypto AG machines.

For a while NSA's secret was only known to the Soviets and Israelis. However, in March 1992, after Hans Buehler, Crypto AG's marketing representative in Iran was arrested by Iranian counter-intelligence for spying for the "intelligence services of the Federal Republic of Germany and the United States of America," NSA's operations were truly out of the bag and thrust into the public limelight. Buehler was jailed in Tehran's infamous Evin prison for nine months. Eventually, Crypto AG paid a $1 million bail for Buehler's release. After returning to Switzerland, Buehler documented his experience and the NSA rigging program in a book, titled *Verschluesselt.*

Although it is undetermined who tipped off the Iranians about the NSA Trojan horse embedded in their Crypto AG machines, U.S. intelligence sources have revealed that Israel gained the most from the disclosure of the Crypto operation, originally compromised by their American spy Pollard. Ex-CIA agents report that the Russian intelligence successors to the former KGB were actually tipped off about the Crypto AG project by CIA spy Aldrich Ames. While still acting as a spy for the Russians after the Soviet collapse, Ames reportedly told the Russians about the Crypto machines. The Russians, in turn, tipped off the Iranians that their Crypto AG units were rigged by the NSA. The Russians may have received additional information on the Crypto units from longtime Soviet and Russian FBI spy Robert Hanssen.

CIA sources claim Hanssen could not have gotten his job without high-level support from more senior FBI officials, including his Opus Dei co-religionist and personal friend Louis Freeh, Jr., the FBI director.

Although Crypto AG (and its secret partner Siemens of Germany) paid Buehler's bail and tried to bury the story, the effect of Crypto AG's sales was immediate. Country after country and bank after bank began to have reservations about the equipment despite Crypto's assurances. Spain and Japan reportedly canceled sales. A number of longtime customers switched to high grade Russian encryption gear.

According to U.S. intelligence sources, shortly after the revelations by Buehler and other Crypto engineers about the NSA project, Switzerland-based international billionaire fugitive and suspected Mossad asset Marc Rich stepped in and invested heavily in Crypto AG's to boost its deflated stock values. Rich was pardoned by President Clinton in January 2001 in an eleventh hour deal partly negotiated by Rich's attorney (and current Vice President Dick Cheney's chief of staff and CIA "Leakgate" suspect) I. Lewis "Scooter" Libby.

The deal with Rich was a Faustian one for Crypto AG. NSA was forced to abandon its prized signals intelligence operation. Communications currently encoded by Crypto AG machines are now, according to U.S. intelligence sources, routinely read by Rich and his Israeli intelligence contacts. Although the encryption technology graduated from computerized central processing units to surface mounted encryption boards, the security trap doors still exist, according to intelligence sources.

Encrypted cables between oil companies and buyers, including spot market dealers, allegedly allow Rich and his friends to underbid lucrative oil contracts. In addition, compromised "secure" bank networks have permitted fake wire transfers to loot numbered bank accounts, including those held by Saudi and Vatican officials. These revelations apparently resulted in the mysterious murder three years ago of the Crypto AG salesman in Saudi Arabia. Moreover, the ability by the Israelis to monitor diplomatic, intelligence, and financial traffic prior to the 9–11 terrorist attacks permitted international speculators to place "put" options on the stocks of American and United Airlines just prior to September 11, 2001—an operation that yielded hundreds of millions in profits.

In the early 1990s, a transfer of five KY-78 encryption devices by Canada to a NATO base in Germany resulted in a disastrous compromise of U.S. communications security (COMSEC) secrets to the Israelis. According to U.S. intelligence sources, the Canadians transferred five of the machines to their CANLOG (Canadian Logistics) United Nations Truce Supervision Organization (UNTSO) post at Camp Ziounai (nicknamed by the Canadians "Camp Roofless") on the Golan Heights in the Separation Zone between Israeli and Syrian forces. During a rotation of Canadian personnel, two of the encryption machines went missing. After a COMSEC audit was conducted, the Canadian communications supervisor reported he had "at least four" of the KY-78s on the books but could only account for two. Since only one was required for communications, he shipped one back to Germany. However, three of the highly classified units remained missing. Two of the units ended up in the hands of Israeli intelligence and were taken apart and fully examined by Mossad crypto experts. Israeli human intelligence agents procured the machine's key codes from other sources.

The results were disastrous for U.S. and NATO secure communications. During Operation Desert Storm, the Israelis were able to read all of the encrypted traffic in and out of the U.S. Embassy in Tel Aviv. U.S. intelligence sources report the only secured communications to and from the embassy was by diplomatic pouch. To cover the fact that they had obtained the codes from the Canadian Golan post, Israeli intelligence began setting up U.S. Marine guards at the Tel Aviv embassy with local prostitutes as a feint to divert attention away from the KY-78 compromise on the Golan to the unwitting Marines as possible crypto thieves in the eyes of U.S. counter-intelligence agents.

Ironically, after the compromise the Canadian peacekeepers replaced their KY-78s with similarly compromised Crypto AG equipment. As for the U.S. Embassy in Tel Aviv, after its coded communications were compromised and this became known to NSA, the embassy's encryption devices were rewired and the codes were changed.

The Israelis were then forced to rely on human intelligence assets within the embassy to feed them classified information. Enter Air Force Reserve officer Larry Franklin—a Defense Intelligence Agency analyst who was first detailed in 1993 to perform his reserve active duty at the U.S. Embassy in Tel Aviv. Franklin would serve repeated tours of duty at the embassy. Earlier this year, Franklin and two officials of the American Israel Public Affairs Committee (AIPAC) were indicted for mishandling highly classified U.S. intelligence. Franklin was discovered to have stashed 83 classified documents, including Sensitive Compartmented Information (SCI) files at his West Virginia home. Franklin was accused of passing classified documents to the AIPAC officials who had maintained a liaison with an Israeli intelligence official at the Israeli embassy in Washington.

Soon, Franklin would have some intelligence assistance at the Tel Aviv embassy. Enter U.S. Ambassador Martin Indyk, a naturalized U.S. citizen from Australia. Strangely, Indyk had two tours of duty as U.S. ambassador to Israel–from 1995 to 1997 and from 2000 to 2001. According to U.S. intelligence sources, Indyk was a valued supplier of classified U.S. intelligence to Israel. In 2000, Indyk had his security clearance yanked. Although Secretary of State Madeleine Albright denied that Indyk was suspected of espionage, U.S. intelligence sources tell an entirely different story. State Department Bureau of Diplomatic Security agents discovered that Indyk routinely took home classified materials where they were left to be photocopied by his maid who doubled as a Mossad operative. Indyk also reportedly allowed his Israeli dinner guests to read other classified documents. Knowing this, State Diplomatic Security agents planted some “classified” documents on Indyk and waited for them to appear. After they turned up through the suspected channels, Indyk’s security clearance was lifted.

CIA sources have confirmed that the neocon penetration of NSA’s raw telecommunications intercept data by John Bolton was part of a multi-pronged attempt by Israeli intelligence to access the “Fort Knox” of America’s cryptologic secrets: the massive repository database of global intercepts of phone calls, email, faxes, and telexes now known as “ANCHORY” but will soon be expanded into a super database code named “OCEANARIUM.” As a result of former NSA Director Michael Hayden’s outsourcing contracts, named “Groundbreaker” and “Trailblazer,” companies with ties to Israeli intelligence are gaining increased access to NSA’s operations and its massive archives of secrets.

The FBI also had severe problems with communications compromises during the lead up to 9–11. FBI agents tailing Israeli agents in the United States (who, in turn, were living and working in close proximity to the alleged al Qaeda hijackers) were stymied by the compromise of secure FBI and Justice Department communications systems by Israeli contractor telecommunications companies such as AMDOCS and Comverse Infosys. In addition, Israeli software companies had permitted Mossad unfettered access to credit card and telephone records of U.S. counter-intelligence agents. America’s counter-intelligence community was trying to do its job with one hand tied behind its back.

The Mossad operatives, the FBI’s New York Joint Terrorism Task Force (JTTF) was tailing in the New York and New Jersey areas, covered their communications by using untraceable Verizon pre-paid cellular phones and Nextel two-way walkie-talkie devices. Mossad agents were also trailing and harassing CIA agents assigned to track people like alleged lead hijacker Mohammed Atta, especially in Fort Lee, New Jersey, where Atta lived for a while. An attempt by the FBI to penetrate New York and New Jersey Israeli intelligence-connected office moving companies, such as Urban Moving Systems, which was discovered to have conducted an emergency move of the Israeli Zim-American Israeli Shipping Company from the World Trade Center’s North Tower just weeks prior to 9–11, were disrupted by communications compromises and pressure from FBI and Justice Department headquarters in Washington, DC. Much of that pressure reportedly originated from then-U.S. Attorney for Northern New Jersey Michael Chertoff, the current secretary of Homeland Security.

U.S. intelligence sources report that the late FBI agent John O’Neill was well aware of the suspicious Israeli activity in the lead up to 9–11. One FBI agent was taken off the Israeli surveillance operations and sent to Pakistan to investigate the kidnapping and murder of *Wall Street Journal* reporter Daniel Pearl. According to U.S. intelligence sources, Pearl was killed not by al Qaeda but by paid foreign hit men hired to get rid of someone who was getting “too close” to the actual money sources that paid for the 9–11 attack.

U.S. intelligence sources report that the one Israeli who is considered an extreme threat to U.S. national security is former prime minister and current prime minister hopeful Binyamin Netanyahu. Not only has Netanyahu visited convicted Israeli spy Jonathan Pollard in his North Carolina prison cell and advocated strenuously for his release, but he was once overheard by an ex-CIA agent as saying to a group of his supporters, “Once we squeeze all we can out of the United States, it can dry up and blow away.” Considering the damage the neocons and their Israeli facilitators are causing for U.S. national security, Netanyahu may soon have his wish.

Wayne Madsen is a Washington, DC-based investigative journalist and nationally-distributed columnist. He is author of the forthcoming book, “Jaded Tasks: Big Oil, Black Ops & Brass Plates.” He is the editor and publisher of the Wayne Madsen Report