Volume 14 | Issue 6 | Number 6 | Article ID 4868 | Mar 15, 2016

US Signals Intelligence (SIGINT) Activities in Japan 1945 – 2015: A Visual Guide

Desmond Ball, Richard Tanter

Introduction

'Due to government secrecy, our citizens are often ignorant of the fact that our garrisons encircle the planet. This vast network of American bases on every continent except Antarctica actually constitutes a new form of empire -- an empire of bases.'

Chalmers Johnson, America's Empire of Bases

Nobody, probably not even the Pentagon, knows exactly how many military bases the United States maintains in foreign countries, or how many have come and gone in the past. Today, there are certainly more than a thousand, and still increasing, and expanding into new fronts, especially in Central Africa. A 'base' can mean many different things, but the ones that usually receive most attention are those where the mechanics of American power projection are most evident – US Marines on the ground or large weapons platforms in place or coming and going: warships, aircraft, submarines, and major ground force equipment. Important to scrutinise as these are, other, less conspicuous types of US foreign military facilities are arguably even more important in the US empire of bases. Before a missile can be launched, the target – and its role, characteristics, and defences - has to be known and found. There are different types and layers of intelligence that feed into such targeting matrices, ranging from flash time-sensitive observations through to the longterm maintenance of adversary electronic order of battle documents recording, for example, the location and capacities of opposition armed forces, air and missile defence radars, and their precise role in the event of combat. But all of this means that for those concerned to assess the consequences of US bases in foreign countries need to attend to signals intelligence bases whose constant and efficient functioning is a necessary prerequisite for power projection.

'Signals intelligence' or SIGINT is then one of the highest priorities for any military, and critical to US global operations. Signals intelligence bases range from huge Circularly-disposed Antenna Arrays or 'elephant cages' more than 400 metres in diameter picking up military transmissions from more than 7,000 kms away, to farms of parabolic antennas downlinking transmissions collected from the ground by SIGINT satellites in geosynchronous orbit, through to small antennas in embassies and consulates picking up local cell phone transmissions between towers. Signals intelligence interceptions are mainly classified as either communication intelligence (COMINT) made up of transmissions between people and electronic intelligence (ELINT) made up of other kinds of transmissions besides communication – such as radar emissions.

A key factor in the location and design of signals intelligence facilities is the type of signals they are attempting to intercept – especially their strength and frequency. Signal strength, for example, declines with the square of the distance from the transmitter to the receiver. Different frequencies behave differently as they pass through the earth's atmosphere and its changing conditions. Some are impeded by rain; others are reflected to a

greater or lesser degree by layers in the ionosphere, enabling short-wave (High Frequency 3-30 MHz) radio signals to bounce around the world. 'Line of sight' (LOS) radio at VHF frequencies (30-300 MHz) and higher generally follow a straight line from the point of transmission until at a certain distance the curvature of the earth makes it impossible for the receiving station to pick up the signal. At a little above sea-level this is a matter of tens of kilometres. For a transmitter at an altitude of 1,500 metres, line of site range is more than 150 kms, depending on weather conditions.

The higher the frequency, the smaller the antenna diameter required to receive and transmit. On the other hand, the higher the frequency, the shorter the wavelength, and the greater demands for antenna precision and stability, especially from transmitters and receivers in motion.

As the military and commercial demand for bandwidth has grown rapidly, satellite communications, which are now critical for all advanced militaries, have moved progressively up the radio frequency spectrum to shorter and shorter wavelengths, from the Very High Frequency Range (VHF; 30 - 300 MHz) through Ultra High Frequency (UHF), Super High Frequency (SHF) and Extremely High Frequency (EHF; 30 – 300 GHz) range.

The US maintained signals intelligence (SIGINT) activities at about 100 sites in Japan during the Cold War, probably more than in any other country. In Japan today, about 1,000 US personnel are engaged in SIGINT, Information Operations, Internet surveillance and Network Warfare activities, mainly at Yokusuka, Misawa, Yokota Air Base in Tokyo, Camp Hansen and Kadena Air Base in Okinawa, and the US Embassy in Tokyo. The US SIGINT activities in Japan have directly supported US nuclear war planning, Korean War and Vietnam operations, and since September 2011, the 'Global War on Terror'. The technological developments over these seven decades have been stupendous. The end of the Cold War coincided with the beginning of the World Wide Web and the Internet age. Surveillance of the Internet and computer network systems became the highest priority. Intelligence became conflated with operations, with a proliferation of Information Operations (IO) and Cyber-warfare units. There has been no Japanese involvement in the US SIGINT activities, and no direct cooperation between US and Japanese SIGINT stations, apart from limited cooperation with respect to particular crises, and with the partial exception of Camelus at Camp Hansen since 2007. Japan is a Third Party to the UKUSA Agreements under which the US and Japan exchange certain designated intercept materials, including HF/VHF DF bearings, but excluding higher level cryptologic material.

The full version of this report provides accounts and photographs of more than 90 SIGINT bases operated by the US military in Japan since 1945. It draws on declassified official US documents, memoirs of former service personnel, Japanese reports, photographic interpretation, and extensive site visits for ground-truthing.

The US now conducts signals intelligence (SIGINT) and cyber-warfare activities at six places in Japan. Yokosuka Naval Base in Tokyo Bay, which was first opened as a US Navy SIGINT station in April 1946, now hosts the Navy Information Operations Command (NIOC), which provides SIGINT, Information Operations and Cyber-warfare support to the 7th Fleet HQ at Yokosuka. The SIGINT station at Misawa in Aomori Prefecture, which was established by the US Air Force in March 1951, became by the 1990s one of the largest in the world, hosting a huge AN/FLR-9 Circularly-disposed Antenna Array (CDAA), a large satellite communications (SATCOM) interception field, and the Misawa Cryptologic Operations Center (MCOC), involving large

elements from the cryptological agencies of each Service, although the AN/FLR-9 elephant cage has recently been dismantled and the Service elements have departed. Yokota Air Base in metropolitan Tokyo, once the main base in Japan for US airborne SIGINT operations in the Far East, now hosts the office of the Department of Defense (DoD) Special Representative Japan (DSRJ), the senior representative of the National Security Agency (NSA) in Japan, and has become a major internet surveillance and Network Warfare centre. An enormous CDAA was constructed at Camp Hansen, in Okinawa, in 2002-06; it replaced the US Navy's giant AN/FRD-10 CDAA at Camp Hanza, which was built in 1962 and dismantled in 2007. Kadena Air Base in Okinawa is now the main base in Japan for US Air Force RC-135 and US Navy EP-3E SIGINT aircraft operating in the western Pacific. The NSA reportedly also maintains a special collection unit at the US Embassy in Tokyo.

The US maintained SIGINT activities at about 100 sites in Japan at various times over the period from 1945 to the mid-1990s, notwithstanding several rounds of rationalisation and consolidation. It probably had more SIGINT-related sites in Japan than in any other country during the Cold War. There were more US SIGINT sites in Western Europe than in the East Asian/western Pacific theatre during the course of that half century, but Japan hosted by far the most in the latter region.

As an NSA history of US cryptological activities during the Cold War noted in 1967, Japan was 'close to the enemy, an ideal SIGINT platform, and in a quasi-subordinate diplomatic status resulting from the American occupation'. Okinawa, still under US military administration until 1972, 'had become a virtual aircraft carrier for American SIGINT collection, with stations at Sobe, [deleted], Hanza and Kadena'.[1]

The US facilities varied enormously with respect to their sizes, capabilities, functions and productivity. Many of them were small and short-lived, especially during the early postwar period. Many minor direction-finding (DF) sites, in particular, were located in remote and isolated places, and maintained by only a few people. On the other hand, some stations were very large and involved major investments, such as the AN/FLR-9 CDAA and the Project *Ladylove* SATCOM (satellite communications) interception facilities at Misawa, the Navy's station at Kami Seya, and the AN/FRD-10 facility at Camp Hanza in Okinawa. Some became quite famous, such as Wakkanai, which intercepted the Soviet Air Force signals relating to the shoot-down of KAL Flight 007 over Sakhalin Island on 1 September 1983, portions of the tape recordings of which were played by President Ronald Reagan in a special address to the nation several days later, attracting world-wide attention to the facility. Camp Hanza was embroiled in local political controversy for more than three decades until the so-called 'elephant cage' was dismantled. The *Ladylove* SATCOM interception site at Misawa is featured on innumerable websites about NSA's *Echelon* civilian telecommunications monitoring program.

From fragmentary beginnings in 1945, within a couple of decades thousands of people were maintaining large antenna farms at more than 20 places, with many more minor sites. Among the larger sites, about 1,500 personnel were assigned to Kami Seya in 1960, Camp Hanza had about 500 personnel at its peak in the late 1960s and the 1970s, about 500 were stationed at Wakkanai in the late 1950s and the 1960s, some 865 personnel were at Onna Point in Okinawa in 1965, and more than 700 personnel were at the Joint Sobe Processing Station (JSPS) at Torii Station in Okinawa in 1968. There were more than 1,900 personnel at Misawa in 1983. A total of around 6,000 would have been engaged in SIGINT activities throughout Japan at the numerical peak in the

late 1960s, with perhaps around 4,000 in the 1970s and 1980s. Many tens of thousands of US SIGINT personnel have served in Japan during the decades since 1945. As in the realm of information technology more generally, SIGINT establishments and operations have been transformed in both capacities and levels of efficiency. There are probably only about 1,000 US personnel engaged in SIGINT, Information Operations, Internet surveillance and Network Warfare activities in Japan today.

These include personnel from all three Services as well as civilian contractors. For example, the DSRJ facility at Yokota there are Army Information Technology Specialists, Navy communications technicians (CTs) and Communications Watch Officers, USAF

Special Collection Systems Senior Engineers (which 'provide RF and computer systems field engineering support'), and civilian Computer Information Security Managers from NSA at Fort Meade.

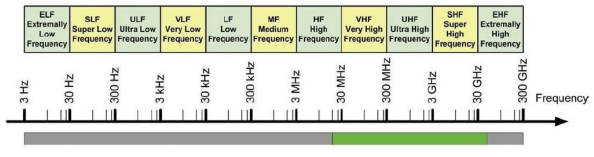
In the past the larger bases employed a number of Japanese nationals – Camp Zama, for example, employed more than a hundred in 1964, but the numbers are smaller today. However, none of these were engaged in operational matters. Rather, they provided

perimeter security, maintained the utilities such as power, water and sewage, and worked as grounds-keepers, cleaners, drivers, waste removalists, etc. Since the 1990s, as US communications and communications interception activities have increasingly moved to the Internet, the Japanese work-force has increased at many US

facilities, where they are increasingly employed in providing IT support, including maintaining connectivity with Japanese Internet service providers (ISPs) and telecommunications carriers.

US SIGINT activities in Japan have undergone enormous changes over the course of these seven decades, of which the personnel movements are a manifestation. They have been generated by short-term budgetary considerations, changes in US-Japan political relations, the exigencies of the Cold War and changes in the regional security environment, the demands of the US involvement in the Korean War, the Vietnam War, and the 'global war on terrorism', technological developments, and organisational changes within the US intelligence community.

With regard to budgetary factors, defence cuts by the Eisenhower Administration in 1957-58 forced major contractions and rationalisations, including the movement of the Army Security Agency's HQ ASAPAC from Camp Oji in Tokyo to Hawaii and the deactivation of its SIGINT station at Fukakusa near Kyoto. HQ ASAPAC returned to Tokyo, at Camp Zama, in 1960, but was moved back to Hawaii in 1965, evidently for balance of payments reasons. According to an official history of the US Air Force Security Service (USAFSS), budget cuts forced the closure of its stations at Wakkanai, Hakata and Yokota in 1972.[2] The deactivation of all Service SIGINT units at Misawa, announced in February 2014, was attributed to fiscal austerity measures by the Pentagon.[3]



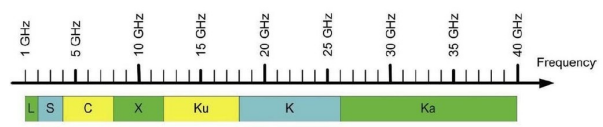
Radio frequency spectrum. Source: Peter Miller, "Ka-Band – the future of satellite communication?", TELE-satellite & Broadband, 9 August 2007, pp. 12-14.

With respect to the impact of changes in the status and temperament of US-Japan political relations, the growth of Japanese political

autonomy after the signing of the 1951 San Francisco Peace Treaty and requests for the return of some of the relevant bases, especially remnants of the Korean War build-up, led to a round of contractions which coincided with the Eisenhower budget cuts. In the case of the USAFSS, for example, 'by 1958, Japan's growing autonomy called for the USAFSS to withdraw all facilities from the Japanese mainland except an augmented effort in the Misawa-Wakkanai complex'.[4] The reversion of Okinawa to Japan in 1972 was accompanied by the transfer of some stations in Hokkaido to other parts of Japan, most importantly Wakkanai and Chitose, but also by the transfer of substantial activities to Okinawa.

The technological developments over these seven decades, with respect to both the means of communication and the techniques for interception of them, have been stupendous. They have generally involved a movement up the radio frequency (RF) spectrum to increasingly shorter wave-lengths but wider band-widths.

The means of communication moved up the spectrum from the High Frequency (HF) range (3 to 30 MHz), used for both Morse Code telegraphy and voice telephony, to Very High Frequency (VHF, 30 to 300 MHz), used for communications over shorter distances but increasingly used also by radars and air defence systems, to satellite communications, mainly operating in the Ultra High Frequency (UHF, 300 MHz to 3 GHz) and Super High Frequency (SHF, 3 to 30 GHz) bands, to the Internet.



Satellite communications bands. Source: Peter Miller, "Ka-Band - the future of satellite communication?", TELE-satellite & Broadband, 9 August 2007, pp. 12-14.

Correspondingly, all of the US SIGINT stations established in Japan in the immediate post-Second World War period were concerned with HF radio interception, using very large antenna systems to capture the HF signals, such as the large rhombic arrays installed at Kami Seya and Torii Station and, in the early 1960s, the CDAAs at Camp Hanza and Misawa.

Band name	Abbreviation	ITU band	Frequency and wavelength in air	Example uses
Extremely low frequency	ELF	1	3–30Hz 100,000km – 10,000km	Communication with submarines
Super low frequency	SLF	2	30–300Hz 10,000km – 1000km	Communication with submarines
Ultra low frequency	ULF	3	300–3000Hz 1000km – 100km	Submarine communication,communication within mines
Very low frequency	VLF	4	3–30kHz 100km – 10km	Navigation,time signals, submarine communication, wirelessheart rate monitors,geophysics
Low frequency	LF	5	30–300kHz 10km – 1km	Navigation,clock time signals, AMlongwavebroadcasting (Europe and parts of Asia),RFID,amateur radio
Medium frequency	MF	6	300–3000kHz 1km – 100 m	AM(medium-wave) broadcasts, amateur radio,avalanche beacons
High frequency	HF	7	3–30MHz 100 m – 10 m	Shortwavebroadcasts,citizens' band radio, amateur radio andover-the-horizonaviation communications, RFID,over-the-horizon radar,automatic link establishment(ALE) /near-vertical incidence skywave(NVIS) radio communications,marine and mobile radio telephony
Very high frequency	VHF	8	30–300MHz 10 m – 1 m	FM,televisionbroadcasts and line-of-sight ground-to-aircraft and aircraft-to-aircraft communications, land mobile and maritime mobile communications, amateur radio,weather radio
Ultra high frequency	UHF	9	300–3000MHz 1 m – 100mm	Television broadcasts,microwave oven,microwavedevices/communications,radio astronomy,mobile phones,wireless LAN,Bluetooth,ZigBee,GPSand two-way radios such as land mobile,FRSandGMRS radios, amateur radio
Super high frequency	SHF	10	3–30GHz 100mm – 10mm	Radio astronomy, microwave devices/communications, wireless LAN, most modernradars, communications satellites, cable and satellite television broadcasting,DBS, amateur radio
Extremely high frequency	EHF	11	30–300GHz 10mm – 1mm	Radio astronomy, high-frequencymicrowave radio relay, microwaveremote sensing, amateur radio, directed-energy weapon,millimeter wave scanner
Terahertzor Tremendously high frequency	THz or THF	12	300–3000GHz 1mm – 100 µm	Terahertz imaging – a potential replacement for X-rays in some medical applications, ultrafast molecular dynamics,condensed-matter physics,terahertz time-domain spectroscopy, terahertz computing/communications, sub-mm remote sensing, amateur radio

Source: Wikipedia

The Soviet Armed Forces began to use the VHF band in 1952, initially for air-to-air and air-to-ground communications. There were fewer places in Japan able to collect VHF traffic, although these few were very good. For operational reasons, the US Services were

especially interested in electronic intelligence (ELINT) associated with Soviet air defences. The USAFSS installed VHF interception systems at Wakkanai in 1952, obtaining superb coverage of VHF communications around the La Perouse (or Soya) Strait and Sakhalin Island. Small VHF interception units were located at Okushiri Island, off Hokkaido's southwest coast, in 1953-57, and at Henashi Saki in northwest Honshu in 1955. The US Navy maintained a station for ELINT collection at Sakata, also facing the Sea of Japan, from 1956 to 1962. The most sophisticated ground-based system VHF/UHF intercept system was the USAFSS's AN/FLR-12, installed at Wakkanai in 1965-66. Because of line-of-sight limitations, VHF communications and ELINT are best collected by airborne systems, with SIGINT-equipped aircraft operating from such bases as Yokota, Misawa, Atsugi, and Kadena at different periods from the early 1950s through to the present day.

Sputnik 1, the first Soviet satellite (or Earth Space Vehicle), launched on 4 October 1957, transmitted telemetry on two frequencies, 20.005 and 40.002MHz. The first Soviet communications satellites, the highly-elliptical *Molniya* series, transmitted in the high part of the UHF band and bottom of the SHF band. Most international communications satellites transmit in the higher part of the SHF band. In the early 1960s, Wakkanai was equipped with a *Trackmaster* system for monitoring Soviet ESV (earth satellite vehicle) telemetry and voice communications from Soviet manned space flights. A more advanced system, code-named *Bankhead II*, was installed at Chitose in 1963. The *Ladylove* SATCOM interception system at Misawa was established in 1980 to monitor Soviet *Raduga* and *Gorizont* geosynchronous communications satellites, as well as the *Molniyas*, used for both civilian and military communications. In the early 1990s, with the end of the Cold War, the focus of the *Ladylove* operation shifted to international communications satellites, primarily carrying civilian telephony, facsimile ('fax') and e-mail traffic.

The end of the Cold War coincided with the beginning of the World Wide Web and the Internet age. Surveillance of the Internet and computer network systems became the highest priority. NSA broadened its collection activities from concentrating almost entirely on interception of information 'in motion', as electromagnetic waves travel through the ether, to also undertaking the collection and manipulation of information 'at rest', stored on computer databases, disks and hard drives.[5] Intelligence became conflated with operations, with a proliferation of Information Operations (IO) and Cyber-warfare units – including the Navy's IO and Cyber-warfare units at Misawa and Yokosuka, and the DSRJ centre and the associated 315th Network Warfare Squadron at Yokota.

There have been a mind-boggling number of organisational changes involving US SIGINT activities during the post-War period. Overall, they have involved a fitful but indubitable trend toward greater centralisation and civilianisation, beginning with separate activities by the military SIGINT organisations, later called the Service Cryptologic Agencies (SCAs), progressing to multi-Service operations in the 1960s and increasing control and participation by the NSA at Fort Meade in Maryland.

The US had two Service SIGINT organisations at the end of the Second World War, the Army's Signal Security Agency, headquartered in Arlington, Virginia, and the Navy's OP-20-G, based in the Navy Department Building in Washington, D.C. The Signal Security Agency was replaced by the Army Security Agency (ASA) on 15 September 1945. The Navy's COMINT elements were collectively designated Communications Supplementary Activities (OP-20-2) on 10 July 1946; they became the Naval Security Group (NSG) on 28 January

1950. The US Air Force was established as a separate Service on 18 September 1947 and established its own SIGINT organisation, the Air Force Security Group on 23 June 1948, renamed the US Air Force Security Service (USAFSS), at Arlington Hall on 20 October 1948.

The Armed Forces Security Agency (AFSA) was established by a directive from the Secretary of Defense on 20 May 1949, which placed it 'under the direction and control of the Joint Chiefs of Staff', to provide some coordination of the Service SIGINT activities. However, the AFSA was frustrated by poor Service cooperation, and, after it failed to provide any warning of the North Korean attack on South Korea on 25 June 1950 and the massive Chinese intervention on 25 October 1950, President Harry S. Truman directed on 13 December 1951 that its performance be reviewed and recommendations made to improve the effectiveness of US COMINT activities.[6] The review team, chaired by George A. Brownell and known as the Brownell Committee, found that the AFSA was founded and functioned as 'a compromise', promoting some cooperation between the Service agencies but allowing them to operate as independent, vertically-organised agencies subject to the command and control of their respective Services.[7]

The report of the Brownell Committee led directly to the establishment of the NSA by Presidential directive on 24 October 1952. The NSA was placed organisationally within the Department of Defense, directly subordinate to the Secretary of Defense, and responsible for COMINT activities at the 'national' level, with Service prerogatives relegated to secondary status.[8] However, the Services retained primary responsibility for operational and tactical COMINT activities, as well as for ELINT collection and processing, which they regarded as indispensible for operational planning.

It took several more years before the mechanics of Service support for NSA COMINT collection and processing activities could be agreed. This was effected in a major reorganisation in 1956, in which a dozen or so COMINT Communications Relay Centers (CCRCs) were established around the world, each providing relay services with from seven to more than 30 COMINT collection sites and command HQs. Later called CRITICOMM Relay Centers, two were located in Japan and Okinawa, providing connectivity with 11 major COMINT collection stations elsewhere in Japan/Okinawa.[9]

Among the SCAs, the USAFSS quickly grew to be the largest. It was renamed the Electronic Security Command (ESC) on 1 August 1979, the Air Force Intelligence Command on 1 October 1991, the Air Intelligence Agency (AIA) on 1 October 1993, and the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) on 8 June 2007. The Army Security Agency (ASA) was reorganised into a new Army Intelligence and Security Command (INSCOM) in 1977. The NSG became the Navy Information Operations Command (NIOC) on 1 October 2005; it provides the components of the Navy's Tenth Fleet or Cyber Command, activated on 29 January 2010.

At the unit level, nomenclature changes have been frequent. In the case of the Air Force, units have been elevated from Flight to Squadron to Group to Wing, or reduced in backwards sequence. In the case of the Army, they have grown from Detachment to Company to Battalion to Brigade, or have shrunken vice versa. Wakkanai had nine designations from 1951 to 1972. Misawa had 20 from 1951 to 1978, and Kadena had 15 from 1955 to 1976.[10] The units at Misawa and Kadena have since had many further name changes.

The US SIGINT units in Japan have performed a multitude of missions, from national through strategic, operational and even tactical levels,

in conflict areas sometimes far from Japan. At the national level, the SIGINT stations at Wakkanai and Chitose were used to intercept the telemetry of Soviet ICBM test flights into the Pacific, as well as the telemetry transmitted by Soviet satellites. Airborne systems, beginning with RB-50s based at Yokota in the late 1950s and a special USASA unit based at Atsugi from 1963 to 1972, through to RC-135S *Cobra Bell* aircraft which use Kadena today, have intercepted telemetry transmitted from Russian, Chinese and North Korean missile tests. The large HF DF systems were able to precisely locate the sources of transmissions thousands of kilometers deep inside the Eurasian land mass, and track Soviet Naval flotillas and missile-carrying submarines in the broad expanses of the Pacific Ocean.

The US SIGINT activities in Japan have directly supported US nuclear war planning. Traffic analysis together with HF DF triangulations identified and provided the locations of enemy command and control centres and major military operating bases for targeting purposes. Precise and up-to-date Electronic Order of Battle (EOB) data concerning adversary air defences, collected by ELINT activities, is essential for planning bomber penetration routes. The Korean War and the Vietnam War generated requirements for operational and tactical SIGINT. During the Korean War, all US SIGINT stations in Japan were involved in support activities to a greater or lesser extent, but especially those at Johnson Air Base, Ashiya, Hakata and Fushimi Momoyama (Kyoto), each of which deployed contingents to Korea. As the war in Vietnam escalated in the early 1960s, it became the principal preoccupation of the activities at Kadena, Torii Station, Camp Hanza and Onna Point in Okinawa, as well as the Pacific Command (PACOM) ELINT Center at Fuchu near Tokyo. SIGINT units based at Kami Seya and Atsugi played direct roles in support of US/Coalition forces during Operations *Desert Shield* and *Desert Storm* in Kuwait and Iraq 1990-91.[11]

Since September 2011, all relevant US activities have been engaged in the 'Global War on Terror', especially the Network surveillance facilities at Misawa and Yokota. For example, units at the *Ladylove* facility at Misawa (the 373rd Intelligence Group in 2004 and NIOC Misawa in 2012) have been commended for their contributions, while a civilian sub-contractor at *Ladylove* stated in September 2013 that its activities there also helped 'to defeat global terrorism'.[12]

Throughout this whole period, the US SIGINT agencies were also responsible for a parallel mission, that of ensuring the security of US communications at all levels against interception and exploitation by potential adversaries. The first communications security (COMSEC) units were established in Japan in 1946, at Nagoya and Naha in Okinawa. The USASA sent the 50th Signal Service Detachment, a COMSEC unit, from Tokyo to Korea soon after US forces entered the Korean War.[13] During the Vietnam War, the Navy maintained major COMSEC centres at Kami Seya (COMSEC 702) and Camp Hanza (COMSEC 704). More recently, as US forces have moved to the Internet for their own communications, including the Voice over Secure Internet Protocol (VoSIP) system for voice communications, NSA and the SCAs have established major centres in Japan for assuring the security of the Internet against hostile penetration. In Okinawa, for example, Network Operations and Security Centers have been located at Fort Buckner and Torii Station.

The Soviet military and intelligence organisations sought to determine the capabilities and purposes of the US SIGINT activities from the outset. Overflights of Wakkanai and Misawa by Soviet Air Force reconnaissance aircraft and MiG fighters were regular occurrences in the 1950s and 1960s. Japanese agents, from local Communists to bar-girls ('josans') were recruited as spies. Veterans have produced numerous novelized

accounts of Soviet espionage activities involving local Japanese nationals at Wakkanai, Camp Oji, Shiroi, Yokota, Chitose and Misawa in the 1950s and 1960s.[14] Two NSA employees, William H. Martin and Bernon F. Mitchell, who had served together at the NSG stations at Yokosuka and Kami Seya in 1951-54, defected to the Soviet Union in 1960, providing Moscow with first-hand accounts of the activities at those places.[15] The capture of the USS *Pueblo* SIGINT collection ship by the North Koreans in January 1968 was a windfall, providing the Soviet agencies with current cryptologic materials as well as information about the roles of Kami Seya and the PACOM ELINT Center at Fuchu.[16] Similarly, after a Kadena-based EP-3E SIGINT collection aircraft made an emergency landing on Hainan Island on 1 April 2001, its state-of-the-art equipment was disassembled and studied by Chinese technicians before it was returned to the US six months later.

There have been many tragedies. Twelve men died in a terrible fire which engulfed the Operations Complex at Kami Seya in September 1965. The airborne SIGINT collection missions could be especially dangerous. Eighty crew members died in just five incidents in the 1950s and 1960s – 33 aboard three aircraft based at Yokota were killed in deliberate shoot-downs by Soviet fighters (on 19 June 1952, 7 October 1952 and 29 July 1953), 16 others met an unknown fate somewhere over the Sea of Japan while on a flight from Yokota on 10 September 1956. A US Navy EC-121M SIGINT aircraft based at Atsugi was shot down by North Korean fighters, killing all 31 men aboard, on 15 April 1969. Several others died in other incidents in which the aircraft managed to land safely back in Japan.[17] One crew member was killed when the North Koreans seized the *Pueblo* was seized in January 1968; all of the remaining 82 were brutally tortured while held in captivity over the next 11 months.[18]

Many major figures in the history of US SIGINT activities served in Japan at one time or another. Edward J. Snowden, the famous NSA 'whistle-blower', was stationed at the NSA post at Yokota from 2009 to 2012; he says that it was while he was at Yokota that he first appreciated the scale of NSA's global civilian Internet monitoring and data-mining activities and decided to expose them.[27]

The full report is available here [6MB].

Recommended citation: *Desmond Ball and Richard Tanter, "US Signals Intelligence (SIGINT) Activities in Japan 1945 – 2015: A Visual Guide",* The Asia-Pacific Journal*, Vol. 14, Issue 6, No. 8, March 15, 2016.*

Related articles

- Richard Tanter, Australia in America's Third Iraq War http://apjjf.org/2014/12/51/Richard-Tanter/4238.html
- Vince Scappatura, The US 'Pivot to Asia', the China Spectre and the Australian-American Alliance
- Richard Tanter, The US Military Presence in Australia: Asymmetrical Alliance Cooperation and its Alternatives
- Richard Tanter, An Australian Role in Reducing the Prospects of China-Japan War over the Senkakus/Diaoyutai?

Desmond Ball is Emeritus Professor at the Australian National University (ANU). He was a Special Professor at the ANU's Strategic and Defence Studies Centre from 1987 to 2013, and he served as Head of the Centre from 1984 to 1991.

Richard Tanter is Senior Research Associate at Nautilus Institute for Security and Sustainability and Director of the Nautilus Institute at the Royal Melbourne Institute of Technology. A Japan Focus associate, he has written widely on Japanese security policy, including 'With Eyes Wide Shut: Japan, Heisei Militarization and the Bush Doctrine' in Melvin Gurtov and Peter Van Ness (eds.), *Confronting the Bush Doctrine: Critical Views from the Asia-Pacific*, (New York: Routledge, 2005). He co-edited, with Gerry Van Klinken and Desmond Ball, *Masters of Terror: Indonesia's Military and Violence in East Timor*.

Notes

[1] Thomas R. Johnson, American Cryptology During the Cold War, 1945-1989. Book II: Centralization Wins, 1960-1972, (Center for Cryptologic History, National Security Agency, 1995), p. 306.
[2] James E. Pierson, *A Historical Study of the Organizational Development of United States Air Force Security Service, 1970-1974*, (United States Air Force Security Service, Kelly AFB, San Antonio, Texas, 15 September 1974), p. 11.
[3] Travis J. Tritten, 'Pentagon Budget Cuts Take First Toll in Japan', *Stars and Stripes*, 26 February 2014.
[4] Josh Chapman, *A Special Historical Study of the Organizational Development of the United States Air Force Security Service, 1948-1966*, (HQ United States Air Force Security Service, San Antonio, Texas, 1 February 1967), pp. 35-36.
[5] James Bamford, *Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World*, (Century, London, 2001), p. 480.
[6] George A. Brownell, *The Origin and Development of the National Security Agency*, (Aegean Park Press, Laguna Hills, California, 1981), pp. 30, 81.
[7] Ibid., p. 64.
[8] George F. Howe, 'The Early History of NSA', *Cryptologic Spectrum*, (Vol. 4, No. 2), Spring 1974, p. 17.
[9] 'Notes by the Secretaries to the Joint Communications-Electronics Committee', *Revision of Interim Outline Plan for Telecommunications Support of National Security Agency*, (JCRC 1371/1, 19 July 1956), Appendix C to Enclosure A.
[10] Larry Tart, *Freedom Through Vigilance: History of U.S. Air Force Security Service (USAFSS). Volume III: USAFSS Ground Sites in Alaska and the Far East*, (Infinity Publishing, West Conshoshocken, Pennsylvania, 2010), pp. 1602-1604.
[11] Douglas Easton, 'Gulf War Diary', *NCVA Cryptolog*, (Kami Seya Special Edition, Fall 1997), pp. 35-37; and 'VQ-1 History', *U.S. Navy Patrol Squadrons*.
[12] Class Pedro Rodriguez, 'NIOC Misawa Changes Command', *DVIDS*, 15 June 2012; and 'Data Entry Operator 2 Job (Misawa, Aomori, JP)', *Jobs77*.
[13] Dave Whitney, 'Torii/Sobe/Okinawa COMSEC Operations', *Torii Tribune: Official Newsletter of ASA Okinawa*, (Vol. 10, No. 2), July 2011, p. 3.
[14] See, for example, Bill Person, *The Ravenworks Sanction: A Novel*, (BookSurge, 2004); W. T.

Naud, *Oji: Spy Girls at the Gate*, (Grovesnor Square Press, Lucerne Valley, California, 2011); Donald Wertz Boyd, *The 6924th, 1955-1956*, (San Bernadino, California, August 2013); Robert S. Ruehrdanz, *Chitose Road: A Novel*, (CreateSpace Independent Publishing Platform, 2011); and George Welch, *Insomnia Mimatsu: A Story of Love and Espionage in Misawa*, (Booklocker, 2007).

[15] Wayne G. Barker and Rodney E. Coffman, The *Anatomy of Two Traitors: The Defection of Bernon F. Mitchell and William H. Martin*, (Aegean Park Press, Laguna Hills, California, 1981), pp. 31, 35, 71.

[16] Ed Brandt, *The Last Voyage of USS Pueblo*, (W. W. Norton & Company, New York, 1969), p. 38; Trevor Armbrister, *A Matter of Accountability: The True Story of the Pueblo Affair*, (Coward-McCann, Inc., New York, 1970), p. 164; and Edward R. Murphy, Jr., *Second in Command: The Uncensored Account of the Capture of the Spy Ship Pueblo*, (Holt, Rinehart and Winston, New York, 1971), p. 206.

[17] Larry Tart and Robert Keefe, *The Price of Vigilance: Attacks on American Surveillance Flights*, (Ballantine Books, New York, June 2001), pp. 15-65.

[18] Lloyd M. Bucher, *Bucher: My Story*, (Doubleday & Company, Garden City, New York, 1970), pp.210, 234-236, 317-318; and Trevor Armbrister, *A Matter of Accountability*, pp. 72-74, 250-253, 268-273.

[19] 'Captain Thomas H. Dyer', *America's Navy*; and Matthew M. Aid, 'US Humint and Comint in the Korean War: From the Approach of War to the Chinese Intervention', *Intelligence and National Security*, (Vol. 14, No. 4), Winter 1999, p. 50; 'The NSA Personnel Newsletter', Washington, D.C., March 1954, p. 3; and 'Capt Thomas H. Dyer, USN (1902-1985): 2002 Inductee', National Security Agency/Central Security Service (NSA/CSS).

[20] 'DLIFLC Hall of Fame (2006 and 2007)', *DLI Foundation*; and Larry Tart, *Freedom Through Vigilance: History of U.S. Air Force Security Service (USAFSS). Volume III*, pp. 1158, 1163, 1164, 1166-1167, 1272-1273.

[21] Christopher Koons, 'Capt McGinnis Nominated for Cryptologic Hall of Honor', *InfoDomain: Decision Superiority for the Warfighter*, Fall 2008, pp. 18-19.

[22] 'Maj Gen Doyle E. Larson, USAF: 2009 Inductee', *National Security Agency/Central Security Service Hall of Honor, 2009 Inductees*; 'Major General Doyle Eugene Larson', *U.S. Air Force*; and 'General Larson Retiring, Successor Named', *Hilltop News*, 21 April 1983.

[23] Jeffrey T. Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*, (Westview, Boulder, Colorado, 2001), p. 81.

[24] 'Patrick M Hughes', *LinkedIn*.

[25] Matthew Aid, 'New Commander of U.S. Navy SIGINT/Cyber Command', 14 February 2014.

[26] Marjorie Censer, 'Government IT Contractors', *Washington Post*, 28 February 2011; and 'Centennial Character Sketch: Joan Dempsey', *YouTube*, 7 April 2014.

[27] Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man*, (Vintage Books, New York, 2014), pp. 37-39; and Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, (Metropolitan Books, New York, 2014), p. 43.