Keynote Speech

Signals Intelligence and Japanese Security

John Ferris

This paper investigates the role of signals intelligence (sigint) in war and power politics during the past century. It focuses on British experiences, especially that of the sigint agency, The Government Communications Headquarters (GCHQ), but my narrative and analysis address contemporary Japanese concerns. In 2022, intelligence specialists comprehend much about the history of sigint, which was unknown just a decade ago, but they have not yet provided a continuous narrative of the topic, nor publicised many details which they understand. Strategic and international historians know little of these developments. Japanese historians and the public grasp much about their experiences with sigint between 1904-45, but not about later ones. Though Japanese siginters and officials understand their modern relationship with American sigint, these issues are little discussed within Japan, which is entering competitions of power politics and possibly of war, where intelligence will work as it did during the two world wars, and the cold war. These general experiences with sigint illuminate present Japanese circumstances, needs and opportunities.

Sigint and Two World Wars

Japan has had a unique experience with sigint among the great powers. Between 1900-45, Japan made some gains through sigint, only then to suffer great and one-sided losses, and ultimately redeveloped services which acted as an adjunct to those of another country.

Japan was among the first states to experience sigint derived from radio interception in war. Just before the battle of Tsushima, in 1905, the Russian Admiral Zinovy Rozhestvensky followed Japanese fleet movements by gauging the strength and location of their wireless signals, and sought to penetrate their lines by having his fleet maintain radio silence as it advanced through mist on the seas, and the fog of war. Admiral Togo Heihachiro maximised the use of radio to command his fleet and detect the enemy, which was essential to its victory, but at cost. This knowledge guided a brave, if ultimately doomed, Russian move through Japanese squadrons. Radio silence handicapped the Japanese ability to locate Russian forces, while interception of plain language Japanese signals finally showed Rozhestvenski that his fleet had been detected, and battle was nigh.[1] Despite these failures in sigint, Admiral Togo Heihachiro scored a sensational victory.

A sigint revolution occurred during the First World War, involving the combination of communications intelligence (comint), material derived from providing the texts of messages, and traffic analysis, which observed the links between nodes of communication and command.

---

1 Julian Corbett, *Maritime Operations in the Russo-Japanese War, 1904-1905, Volume II*, (Naval Institute Press, Annapolis, MD, 1994), pp. 216, 231.

Britain led the world in Sigint, which was an unsung contribution to allied power. It won the Sigint struggle against Germany, and British victories were significant; reinforcing material mastery in sea power, so producing the easiest great war the Royal Navy (RN) ever has faced and making the application of blockade more effective and less traumatic than usual; and helping Britain evade dangers with the United States and instead gain American aid for free. France outperformed Britain in military Sigint, where Americans also did well; its allies' greatest successes in Comint may well have been against British diplomatic codes, and its interests. These British (and allied) triumphs, however, were balanced by those of Austro-Hungarian and German Sigint, which helped smaller forces to demolish a larger Russian army. Sigint successes by the Entente and Central Powers occurred at the same times, each immediately countering the others' effect before they could be exploited. The greatest successes of Sigint in the First World War exceed those of the second, and its aggregate quality in 1916-18 probably matches that of 1942-45. But intelligence affected the Great War less because, at the strategic level, each side's successes largely cancelled each other out. Intelligence was harder to use for dramatic results in operations than in the Second World War, when forces struck harder and faster, and between 1942-45 intelligence systematically reinforced one side against the other. Nonetheless, in a war where power was measured in the ability to produce hundreds of thousands of soldiers and millions of tons of steel, Sigint mattered, more than in any previous conflict.[2]

Japan missed this sigint revolution, but Japanese military services quickly developed capabilities, which were respectable but never quite first rate. They purchased copies of virtually every piece of cryptographic kit which entered the market, and designed indigenous systems. Japanese cryptosystems were competent, but American and British siginters often penetrated these military and naval codes and, along with Germany and the USSR, routinely read Japanese diplomatic systems. Japanese forces developed small but competent radio intercept and codebreaking units, augmented by surreptitiously stealing cryptosystems from foes. These practices gave the Japanese army an edge over Chinese forces and rough parity with Soviet military sigint. Intelligence derived from American and British cryptosystems enabled Japan's surprise attacks of December 1941.[3] However, from that moment, sigint became a constant and critical weakness for Japan. Its sigint services stagnated, while Anglo-American ones exploded in quantity and quality. The United States, backed by Britain, rapidly mastered key Japanese cryptosystems, which guided its operations across the Pacific. In their struggle, sigint aided the United States and damaged Japan more than it did any other belligerents of the Second World War.

The intelligence battle of that war was a competition, involving successes and failures on all sides. Before 1942, intelligence worked marginally for the Axis, by multiplying the value of their large and good forces. From 1942, however, the balance of intelligence and power turned

2 John Ferris, *Behind the Enigma, The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency,* (Bloomsbury, London, 2020), pp. 29-64.

3 Ken Kotani, *Japanese Intelligence in World War II*, (Osprey Press, 2009); John Ferris, "'Consistent with an Intention': The Far East Combined Bureau and the Outbreak of the Pacific War", *Intelligence and National Security*, 27/1, January 2012, pp. 5-26.

simultaneously and systematically toward the Allies. The effect was one sided for a long time. Intelligence did little to cause Axis defeat, but much to shape Allied victory.

"Ultra", the allied codeword for material derived from high-grade comint, especially that which Bletchley Park reaped from German cryptosystems like the "Enigma" machine, was the best source of intelligence during this war, but never perfect. Ultra took words straight from the enemy's mouth, but they rarely were straightforward. Its value differed with time and theatre. Ultra became more successful over time, but its history was replete with reversals of fortune. The Allies never read every important enemy message, or most of them. Ultra was not the best source on everything, nor were technical achievements in cryptanalysis and battlefield success linked in a simple way. During the African campaign, Ultra could have been most useful when it was technically most primitive rather than most mature, because of operational conditions. When it was most primitive, force to space ratios were low, as were both sides' strengths; hence, victories with decisive consequences were possible. Once Ultra became mature, large and good armies were locked in prolonged and high intensity struggles of attrition on narrow fronts, like the great war, though more fluid. Even so, intelligence budged the balance of attrition toward the Allies, as knowledge multiplied the power of the stronger side. When they held the initiative, the weaknesses in Axis intelligence were irrelevant, and their strengths in tactical collection counted. On the defensive, their strengths became irrelevant and their weaknesses a danger. As German power declined, its chances for success hinged on deploying elite forces to sectors the enemy would attack where, with their weaker brethren, they might stop breakthrough and force foes into costly and one-sided battles of attrition, toward strategic stalemate. This aim required Germany to guess where and when the enemy would attack. It did not do so. Instead, from 1942, Germans suffered a steady run of surprise at the hands of the western allies. Amphibious operations against North Africa, Sicily and Normandy, hit Germany like thunder at weak points, and by surprise, transforming the front, because its intelligence was incompetent and its command manipulated by Britain. Deception was the most precise, and devastating, form through which Ultra damaged its enemy. Before the invasion of Sicily in 1943, and Normandy in 1944, Britain deceived Hitler into thinking that the allies would attack elsewhere. This success crippled the deployment of German forces before these invasions, ensuring that 33% of their forces were in the wrong place—deception helped to keep many German formations from affecting the battle of Normandy. Intelligence and deception were fundamental to allied success in those campaigns. German intelligence failed precisely when Nazi strategy most needed it to succeed.[4]

In the Pacific War, Ultra of lesser quality than in Europe enabled greater triumphs, because conditions on the battlefield gave intelligence a more dramatic effect. Intelligence affected this war more than any other in history. Radio dominated communications for small forces scattered over millions of square miles. Prisoners and agents were less useful sources than usual, signals intelligence, radar, imagery and captured documents more so. In these

4 Ferris, *Enigma*, pp. 223-66; Ferris, J.R., "Intelligence", in Ferris, J.R. and Ewan Mawdsley (eds), *The Cambridge History of the Second World War, Volume I, Fighting the War*, (Cambridge University Press, Cambridge, 2015), pp. 637-63; Stephen Budiansky, *Battle of Wits, The Complete Story of Codebreaking in World War II*, (Free Press, New York, 2000).

disciplines, the Japanese were poor and their enemies good. Force to space ratios were low, most elements of either side rarely were in contact with the other, and their dispositions were masked. Rarely has the initiative had such power. Unexpected blows were hard to handle--weeks might be required to redeploy naval or air forces from one base to another, months to build the infrastructure necessary to maintain large forces in a new area or to move soldiers by sea or land. To destroy 20,000 men or 200 airplanes, capture one base or outmanoeuvre two divisions, transformed operations in New Guinea, a theatre the size of the Mediterranean. The ability to concentrate against the enemy's weakness, to catch it by surprise and to profit from knowledge of its intentions, were unusually large, especially for that most complex of operations, amphibious assaults. Failures in these areas were unusually expensive. Ultra gave American power a razor, by showing how to execute lines of strategy, where to begin operations, how to force the enemy into error, and to prevent it from returning the favour. Poor signals security and intelligence, imagery and radar , left Japan vulnerable to surprise, defeat in detail, and loss of the initiative. Intelligence was fundamental to the battles between May to December 1942 which crippled the Japanese Navy and stemmed its tide. Intelligence enabled the great American victories of attrition between August 1942 and February 1944, starting with the seizure of Guadalcanal and the 18 month long Solomon Islands campaign, culminating in a terrible campaign of maritime interdiction, where it guided small forces of aircraft and submarines precisely onto Japanese vessels over a large area. In 1944, the island hopping strategy, which broke Japanese defences on the cheap, was possible only because intelligence showed how to strike where the enemy was weakest. In 1945, Ultra on Japanese strength in Kyushu, and Japan's determination to fight, spurred the American decision to end the war through atomic bombs. The United States won the Pacific war because of the quality of its forces and commanders and the scale of their resources, but intelligence let it win far more speedily and cheaply than otherwise could have happened. Here, as in the war as a whole after 1942, intelligence helped the big battalions.[5]

Sigint in the Cold War

Sigint most shaped the cold war by helping to prevent the big battalions from ever fighting at all. In the popular imagination, Cold War intelligence centred on a struggle between spies from west and east, where the KGB reigned supreme. In fact, military intelligence dominated that struggle, in which Sigint was the best western source, while the iconic heart of Cold War espionage – Berlin – mattered more as a bastion for western sigint against the USSR, than as a battleground for spies. That struggle centred not on Checkpoint Charlie, honoured in fiction, but military installations in Berlin, like RAF Gatow and its American and French counterparts. Gatow, at the heart of the Group of Soviet Forces Germany, the greatest conventional formation on earth, was ideally placed to collect Sigint, especially taken from voice communications,

5 John Prados, *Combined Fleet Decoded, The Secret History of American Intelligence and the Japanese Navy in World War Two*, (Naval Institute Press, Annapolis, MD, 2001); Edward Drea, *MacArthur's Ultra, Codebreaking and the War Against Japan, 1942-1945*, (University Press of Kansas, 1991).

in "a Sigint gold mine, a window into the heart of the Communist Bloc military system".[6] This struggle was GCHQ's main task between 1946 and 1992. Through patient and thorough exploitation of low grade systems, GCHQ, the National Security Agency and their European partners penetrated Soviet military intentions and capabilities. GCHQ shaped a stand-off in intelligence with the "main enemy", which aided western victory.[7]

The intelligence services of the cold war were the largest, most sophisticated and technologically advanced ever seen. Supply and demand grew in unprecedented ways. Intelligence on the broadest forms of technology, the narrowest characteristics of weapons and the most secret of programmes, expanded exponentially in value. Signals intelligence became industrialized, mechanized and mathematized, as cryptology and computers drove each other to revolutions. Every year, brute force became stronger and chisels sharper. In unprecedented ways, intelligence alliances linked all coalitions of the cold war, routinely being their closest elements, especially UKUSA, the cryptologic combination between the "Five Eyes", Australia, Britain, Canada, New Zealand and the United States.[8] These alliances were marked by competitive cooperation, and political strains. Largely because the Five Eyes would not share their techniques or take with the sigint agencies of their European allies, NATO intelligence was coordinated badly, wasteful in peace, and fragile for war. Other western sigint agencies either worked as junior partners to UKUSA or the United States, or else formed independent alliances of their own. UKUSA and its looser ties with third parties in the west were more egalitarian than their counterparts to the east, yet members of all of these agencies worked more closely with each other than they did with other bureaus of their own states. Each partner developed capabilities to boost the common pool, and acquire something to trade. Although the dominant partners in these coalitions were greater than their allies, the best of the latter, like Britain and East Germany, matched anyone in quality, while countries like Norway and Hungary had sigint agencies larger than any before 1939. Israel created intelligence and sigint services of world class. Those of nations ranging from India to Iraq were powerful for regional struggles.

Sigint was overwhelmingly the dominant form of secret intelligence during the cold war. Our knowledge of it is limited, but we do know some things and also that we do not know others.[9] Thus, a conservative analysis from known facts illustrates the scale of diplomatic cryptanalysis. When properly used and not physically compromised, leading cryptographic

---

6 Tom Johnson, *American Cryptology during the Cold War,1945-1989, Book One, The Struggle for Centralization, 1945-1960*, p. 118, (Center for Cryptologic History, Fort Meade, MD, 1995).

7 Johnson., op.cit., and Volumes Two to Four; Ferris, *Enigma*, pp. 502-51; Matthew Aid, *Secret Sentry, The Untold History of the National Security Agency*, (Bloomsbury, London, 2010); Richard Aldrich, *GCHQ, The uncensored story of the Britain's most secret intelligence agency*, (Harper Press, London, 2010); Stephen Budiansky, *Code Warriors, NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union*, (Vintage, New York, 2017).

8 Ferris, *Enigma*, pp. 324-89; Michael Smith, *The Real Special Relationship, The True Story of How the British and U.S. Secret Services Work Together*, (Simon & Schuster, New York, 2022).

9 As the authorized historian of GCHQ, between 2015-20, I had access to material which remains secret today. None of it affects this paper, which draws only from sources in the public domain. Simply because I cite an unofficial work does not indicate that still secret material supports its conclusions, merely that I find its evidence and arguments plausible, based on what is known in the open sources.

systems after 1945 should have been impossible to break—just like Enigma. But they were vulnerable to "black bag jobs", like surreptitiously copying cryptographic hardware and software, or to the interception of leakage from electronic devices. Many states used systems that could be solved through cryptanalysis, especially because, unbeknownst to the consumer, they included back-doors which western siginters could exploit.[10] Comint was acquired by ancillary skills, such as intercepting electronic leakage and unencrypted traffic, especially massive amounts of official and private telephone traffic. The KGB bugged all embassies in Moscow, as the United States did the code rooms of every chancery it could reach. Embassies served as bases to intercept microwave and telephone traffic in foreign capitals.

This labour bore fruit. At any point during the cold war, UKUSA read many important messages of most countries on earth. However, it had limited success against the main adversary, because of victories by spies against sigint. In 1946-48, American attacks on Soviet intelligence traffic, cracked the great Soviet mole networks of that era, until a British traitor, Kim Philby, destroyed that access. Meanwhile, an American traitor, William Weisband, wrecked a second Ultra which British cryptanalysts had deployed against Soviet cipher machines. UKUSA rarely read the highest of Warsaw Pact military cryptosystems, but penetrated some of them up to middle levels, and often intercepted important traffic which was unenciphered. UKUSA intercepted around 150,000,000 messages of Soviet agencies between 1945-60, in plain language but including valuable intelligence, especially on economic matters.[11] UKUSA frequently tapped Soviet cables carrying military traffic in plain language in Europe and at sea, which provided masses of material on secondary issues. It exploited a flaw in Soviet systems for enciphering voice communications, which actually failed to cover many channels, including some medium to high level military circuits.[12] Sigint, focused primarily on elint and traffic analysis, remained the west's best source on the Soviet system. Though the topic still is covered in secrecy, Soviet sigint was formidable. If probably less good than its western rivals in pure cryptanalysis, as ever, superb espionage aided that work, especially by penetrating USN cryptosystems. The USSR read some diplomatic traffic of half the world's nations, including from the United States embassy in Moscow during the 1950s, perhaps through bugs or intercepting electronic leakage.[13]

After 1945, the best cryptographic systems rarely were solved, though they remained vulnerable to espionage, which became the greatest weapon against them. Adversaries intercepted important traffic carried by systems of lesser security on one's internal communications, whether submarine cables, voice radio, microwave signals or cellphones. Comint provided more diplomatic information than before, but less often from the major

10 Greg Miller, "'The Intelligence Coup of the Century': For decades, the CIA read the encrypted communications of allies and adversaries", *The Washington Post*, 11.2.2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

11 Carol B. Davis, *Candle in the Dark, COMINT and Soviet Industrial Secrets, 1946-56*, (Center for Cryptologic History, Fort Meade, MD, 2017); Ferris, *Enigma*, pp. 522-25.

12 Ferris, *Enigma*, pp. 525-49.

13 Desmond Ball, *Soviet Signals Intelligence*, (ANU Strategic and Defence Studies Centre, Canberra Papers on Strategy and Defence, No 47, 1989); David Easter, "Nikita Khrushchev and the Compromise of Soviet Secret Intelligence Sources", *Journal of Intelligence and Counter-Intelligence History*, 35/3, April 2021.

systems of leading powers. No longer did strong states regularly defeat each other, though this could happen. French and Japanese codes were weak, while in the late 1970s and early 1980s, American comint cracked some high grade Soviet systems. No doubt other instances will become clear. None the less, comint was less effective as a source between the great powers than it had been during the interwar years, because forms of defence rose in strength.

Diplomatic comint had two main forms. The first was attack by strong states on weak ones. This material was useful in itself, while secondary states with weak cryptography but informed ministers inadvertently illuminate the policy of every great power to all others. The second form is more peculiar. The cold war coalitions were stable. The sigint struggle between them focused on strategic matters. Their members concentrated their diplomatic comint against the people with whom they conducted diplomacy, their allies, and on the issues where they competed, bread and butter matters of foreign policy and economics. Such material, often available through simple means, like telephone intercepts, was easier to acquire than high diplomatic intelligence across the great divide. Comint perhaps most aided its consumers by illuminating the bargaining positions of competitors, usually friendly or neutral, on bilateral and multilateral negotiations over commercial issues. Within these coalitions, diplomatic codebreaking shaped minor rivalries, and alliance management by the powers most responsible for and informed about such matters. So too, during the first decade of cyber-intelligence, when the balance of cryptology turned dramatically toward the attacker, diplomatic material was collected from those with whom one negotiated, allies and neutrals, with a focus on trade and economic matters, where states have no friends, merely rivals. The limited body of documentation in the public domain on diplomatic comint suggests that during the 1980s at least, UKUSA penetrated Japanese cryptosystems and acquired much intelligence on political and especially economic issues, such as GATT. The United States also allowed Japanese governments to use Crypto AG machines, which it read, so placing Japan among the second rank of its allies across the world, alongside Italy and Turkey.[14]

During the military struggle of the cold war, intelligence focused on supporting millions of soldiers and thousands of nuclear warheads in a world-wide competition of power politics against a peer, which never went hot but might have done so at any time. The United States, later followed by the Soviets, developed technical means to determine the current nuclear strength of its rival, although expansion programmes and qualitative developments always remained uncertain. 1939-45 witnessed a comint war. Traffic analysis and imagery dominated the cold war. Each day, hundreds of thousands of their members, east and west, monitored each other's capabilities and intentions, their main task being to say, World War Three will not start today. This news was good to know. These agencies eliminated ignorance, uncertainty and alarm about nuclear forces and stabilized the balance of terror. Intelligence shaped conventional operations as it did in both world wars. For strategic intelligence during the cold war, the triumph lay in military spheres. Nuclear weapons and their effect were hard to mistake, and intelligence on them was good enough. The certainty of nuclear annihilation linked the net estimates of both sides. It forced everyone to minimize risky strategies and to play much of

14 Aldrich, *GCHQ*, pp. 445-6; Greg Miller, "Intelligence Coup", op. cit.

the game the same way. This situation crippled the value of conventional power and left the struggle to centre on economic growth and political stability—the trump suits of the west. Intelligence was secondary in the emergence and the end of this struggle. The USSR lost the cold war because it did not know its enemy, or itself. The west knew itself, and something of the enemy, but won without quite knowing that it had done so, or how.

Techniques of Sigint

Sigint is a process with many moving parts. Siginters, working on the leading edge of communications and data processing, are sensitive to any developments in either area. Change characterises Sigint, but revolutions are rare. The years between 1939 and 1992 were the heart of the first age of Sigint, which was dominated by radio communications, analogue modes of collection and processing, and cryptanalysis by eye and electro-mechanical data processing machines. Until 1992, computers essentially supported cryptanalysis, rather than transform organization, as they quickly did afterward. Computing power rose steadily, as did collection by and against satellites, through automated systems. The roomfuls of data processing machines employed to shatter Enigma vanished, but other systems rose to tackle different targets. Until 1992 GCHQ used variants of the equipment, approach and structure which characterized British Sigint in 1945, or 1918. Teams of operators still intercepted voice, and high-frequency (HF) and very high frequency (VHF) Morse radio. Data processing rested on card indexes and punch cards, and on teams working in typing pools and communication centres. GCHQ was a machine to produce information, driven by a flow of paper instead of steam. Overwhelmingly, its personnel worked in labour intensive tasks of interception, involving skilled craftwork, and data processing, and the pristine copying, recopying and movement of paper.[15]

Means of communication and interception constantly shifted. There were massive numbers of collection sites, both permanent and based on mobile platforms, especially aircraft and submarines. Voice, captured by ear, hand, or tape recorders, matched text in significance. Oceanic telegraphs, once central to communications, declined. Submarine fibre-optic cables restored that position around 2000. Despite predictions that Morse was dead, HF and VHF dominated military signals. “Antenna farms” – aerials concentrated in good locations for interception – best collected such transmissions, which were shielded by complex shifts in frequencies. Only interception and data processing systems of unprecedented sophistication could handle the flood of traffic from satellites. Sigint caught far more material than ever before but proportionately far less of the whole than Britain had done between 1915 and 1945. To know which channels carried the best material at any moment, exploded in significance and absorbed a larger number of staff. Learning the timings and frequencies for messages on Morse, or keywords or telephone numbers for traffic on satellites, improved the take more than merely by expanding the power of interception.

During the heroic age of interception, operators wearing headphones hunched over clumsy sets, hunting wavering frequencies, scribbling messages by pencil. Individual skill and autonomy remained high, driven by knowledge of the nets which operators penetrated.

15 Ferris, *Enigma*, pp. 480-500.

Increasingly, technological and organisational developments changed working conditions. New equipment eliminated frequency drift, and improved interception at high frequencies. Operators managed more sets and monitored more frequencies than before. Craftmanship remained crucial, yet industrialisation boosted interception, ranging from improved interception kit, tuning aids, micro computers and tape recorders. By 1974, the first entirely computer-controlled stations, designed around antennae and machines, not humans and desks, where computers outnumbered operations staff, handled satellite collection.[16]

Not all signals involved words. Elint, which examines non-communications signals from electronic emissions, was among the earliest forms of Sigint, first exploited at the battle of Tsushima. In 1940-45, Elint captured and analysed the emissions of electronic equipment, including radar. It became central to tactical air intelligence and to electronic warfare (EW). After 1945, Elint was essential to Sigint and EW, and to military services. Elint gave air forces and navies tactical intelligence and situational awareness, and enabled EW, while boosting operational assessments for Siginters.[17]

During the Cold War, Comint, Elint, and traffic analysis were fused, and Sigint was central to national intelligence. Siginters provided staggering quantities of material, that required many forms of analysis, always technical and usually expensive. Work against the Warsaw Pact rested on fusion, when high-grade Comint failed, but several low-grade systems together provided useful intelligence. Nor was this a single oddity – it is characteristic of Sigint as a whole. Fusion forced an industrial scale of collection, assessment and reportage. Every piece of traffic analysis received almost as much attention as messages in Ultra had done, which required expanded analytic staff among producers and consumers. Fusion required as many human resources as Ultra, for a product less good, though still fit for purpose. Every day, tens of thousands of operators monitored communications networks they knew like their own families, for any sign of change or danger. Traffic analysis reports on major Soviet operations—some of the best military intelligence of the Cold War, revealing how Warsaw Pact forces planned to fight – might involve 18 months' work, thousands of hours of analysis, and reach 200 closely typed pages in length. No other means or agency could achieve this end.[18] Appreciations turned on agonising analysis and comparison of detail in hosts, like generating datasets from fragments, or considering whether words were used in plural or singular forms.

The Second Age of Sigint

Between 1945-89, Siginters attacked two communications targets, primarily military radio networks, which were protected by specialized personnel and cryptography, and small amounts of traffic (mostly of states, but sometimes foreign people) on civilian communications systems, including cable, microwave and satellites. Then, the end of the Cold War and changes in technology shaped the birth of a second age of sigint, characterised by reliance on computers,

16 *Ibid*, pp. 483-8.

17 Alfred Price, *The History of US Electronic Warfare*, Volumes One (Association of Old Crows, Westford MA, 1984), Two (*The Renaissance Years, 1946 to 1968*) (1989) and Three, *Rolling Thunder Through the Allied Forces, 1964 to 2000* (2000).

18 Ferris, *Enigma*, pp. 543-5.

the internet, and digitised modes of collection and analysis. HF and VHF radio, and the sites that collected them, became marginal to communications and Sigint, though their value would rise whenever conventional forces (especially aircraft and warships) engaged each other. Satellites, and land and maritime cables, became the mainstays for state and civilian communication and Sigint. Targets, whether diplomats, spies, or terrorists, no longer used distinct communications systems, but rather civilian ones. Their traffic could not be intercepted unless one also touched that of civilians, including one's own people, because the source and destination of messages could be identified only by checking their external features. Civilian systems also changed. Communications and information were digitized, and joined to the internet. Anyone on the internet was connected to everyone there. Its prevailing characteristics placed disclosure and surveillance, above security or privacy. Electronic mail carried voice and print messages. Mobile wireless devices increased the amount of private communications susceptible to interception. Communications, carried online and through wireless telephones by signals that crossed national boundaries promiscuously, linked to any data stored on every computer connected to the internet, became open to interception by all comers at once. This material could be copied as easily as electrons, although retrieval and analysis remained frustrating.

Changes in the characteristics of communication spilling across national borders, affected how liberal states intercepted any traffic of their citizens, home or abroad, or foreign messages passing through their space. In the analogue age, lawyers and Siginters could differentiate between traffic transmitted at home and abroad, and illegal and lawful interception. Law restricted interception at home, but not abroad. In the digital age, domestic traffic moved abroad, and foreign messages through one's home. Messages between offices in Tokyo might pass through Beijing; traffic between Russian intelligence in Moscow and Petersburg move via London. Foreign targets might best be attacked by intercepting communications passing through your home, even though this challenged traditional concepts of law. Domestic traffic unavoidably would be acquired through legally acceptable interception abroad. Bulk collection of any internet traffic must include one's citizens, in the first instance. To do otherwise would be to abandon Comint, which one's rivals would not. Yet any analysis of such material, whether intercepted at home or abroad, must touch the envelopes, the metadata, of their citizens' mail, without warrant. These procedures were legal, but felt unpleasant.

The internet enabled the rise of an anarchic international order. "Cyberspace" is not a metaphor, realm, or place, but rather a part of many things, and of the connections between them—a commons of communication and information. As on other commons, like markets or the seas, a struggle between many players, states and otherwise, defines the practices within overlapping competitions between state and non-state actors. These practices alter with changes to conditions, interests, power and time. They always are in dispute. Those practices which emerged over cyber involved as many actors and interests as ever on any commons: intelligence and security for states, and privacy and surveillance for individuals. These developments eased the interception and transmission of signals, and dissolved established borders between states and societies, internal and external relations, war and peace, civil and military, security and insecurity, and sovereign and non-state actors. Once Sigint agencies could distinguish between traffic intercepted at home and abroad, which let liberal states combine civil liberties and

cryptanalysis. That status no longer was true, when messages surged automatically between servers at home and abroad, and Sigint agencies had an unparalleled ability to read the mail of private people, as against foreign states. For the first time, non-state actors used the same techniques of Comint as governments, and applied them against foreign states, or people. Citizens were threatened by attack from their fellows, and foreign governments, firms and criminals. Individuals were more open to attack from pirates, and foreign governments, than on any other commons. States attacked the communications of foreign individuals and corporations far more than ever before in peacetime. States could not easily protect their people against these threats.

In order to man British frontiers on the cyber commons, GCHQ adopted a new and unique form of bulk collection, taking tiny samples from the billions of telecommunications events happening across the world each day, analyzing this traffic for several days, and then purging it, so to make space to hold another sample. If all the world's internet traffic was a billiards table, GCHQ sopped up a beer mat's worth of messages, and processed through traffic analysis only a "full stop", with far less than that amount attacked and read. All of this material had some encryption, elementary at lower levels, but often hard at upper ones. As a practice, traffic analysis turned systematically from assessing the external features of signals between HF radio sets, to the links between the Internet Protocol (IP) addresses of computers within networks. This transformation required operators with different skill sets, though they retained the creative and painstaking ability to analyse the external features of communications which drove GCHQ's successes in fusion during the Cold War. This traffic analysis illuminated potential threats or problems long before any content was read, and was the main part of success against bulk traffic. Cryptanalysis provided just the icing on the cake. In the first round of processing, the metadata of IP addresses was anonymised, stripping all personal details, which simplified Sigint, and GCHQ's legal position for tackling communications which might involve British subjects. Traffic analysis determined which IP addresses communicated with those already under suspicion, so identifying further suspects. Cryptanalysis attacked only messages from suspect addresses. If these addresses involved non-Five Eyes citizens working from non-UKUSA addresses, the decision to attack was purely technical, made by analysts and cryptanalysts. If they touched a Five Eyes citizen, location or address, legal warrants were needed to justify attacks on the content of messages.

As Iain Lobban, the Director of GCHQ, said in 2013, "If you think of the internet as an enormous hay field, what we are trying to do is to collect hay from those parts of the field that we can get access to and which might be lucrative in terms of containing the needles or the fragments of the needles that we might be interested in, that might help our mission. When we gather that haystack, and remember it is not a haystack from the whole field, it is a haystack from a tiny proportion of that field, we are very, very well aware that within that haystack there is going to be plenty of hay which is innocent communications from innocent people, not just British, foreign people as well. And so we design our queries against that data, to draw out the needles and we do not intrude upon, if you like, the surrounding hay. We can only look at the content of communications where there are very specific legal thresholds and requirements which have been met. So that is the reality. We don't want to delve into innocent e-mails and

phonecalls… If I have that haystack, I am looking for needles and fragments of needles. That is what my queries pull out. I do not look at the surrounding hay. It may have been intercepted. A small portion of that may apply to British citizens. We will not look at it without a specific authorization".[19]

The overwhelming number of potential targets, compared to the tiny resources for traffic analysis, cryptanalysis and the reading and translation of texts in many languages, drove this process. States remained the major target, but GCHQ also had to protect British civilian and military lives from terrorists, insurgents and pirates. Internal and external threats fused. GCHQ acted as it rarely had before, more like policemen within Britain than soldiers abroad. Such acts stretched its legal mandate against external threats, yet if it did not take the work, who else had the technical capabilities for it? How else could GCHQ prevent agents based abroad from stealing secrets from firms in Glasgow, inspiring terrorism by British subjects in Bradford, or subverting elections across the country?

GCHQ lacked the means to attack any message which did not have high priority. Every day, it could assess the metadata of billions of messages, yet perhaps touched just tens of thousands of them, and read a small proportion of the traffic of hundreds of new targets. The latter, however, enabled many successes. GCHQ devised efficient means to sample massive quantities of traffic; to hold, examine, and where relevant, retain traffic; and then to flush its databases, and repeat the process. As it later wrote, "GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision. By drawing out fragments of intelligence… and fitting them together like a jigsaw", GCHQ could "discover new threats", provide "unique intelligence about the plans and intentions of current targets", and "protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet".[20]

GCHQ and Cyber Security

The growing need to police the cyber commons posed organisational problems for Siginters. Cybercrime endangered great firms, and countries with large financial sectors, like Britain. States struggled to organise Sigint and Comsec as they confronted new relationships with military organisations, and internal ones. Should Siginters, or soldiers, command the offensive side of cyberwar, where digital and kinetic means combined? Should Siginters or policemen handle cybercrime? These questions raised complex issues of organisation and law. Everywhere, the internal structures of countries drove answers. Some smaller states, especially Israel and Singapore, coordinated cybersecurity years before Britain and the United States, where many agencies confronted larger and more complex versions of these issues.

Over 10 years from 2007, when it stood below American or Israeli standards, a confluence of events pressed Britain to pursue a coherent policy for cybersecurity. Politicians, driven by

19 "Intelligence and Security Committee of Parliament, Uncorrected Transcript of Evidence", 7.11.2013, http://isc.independent.gov.uk/public-evidence/7november2013

20 David Anderson, Q.C., Report of the Bulk Powers Review, CM 9326, 8.2016, pp. 152-6, 159-62, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

their own observations, not advice from GCHQ or departments, thought cybersecurity was a great problem which required solution. They treated the issue in a non-partisan fashion, not constantly overturning each other's work. As Prime Minister, Gordon Brown had Britain define a strategy for cybersecurity. It produced stirring statements, "Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space"; and basic principles, especially the need to coordinate state and private actors; but few practical changes. A small central unit monitored developments on the cyber commons. Another at GCHQ handled threats. GCHQ quietly advised firms about cybersecurity. Still, 15 departments acted as they pleased in the field.[21]

The Conservative/Liberal Democrat coalition of 2010-15 built on Brown's work. Its leading members, including the Prime Minister, David Cameron, made cybersecurity a national priority. As Robert Hannigan, Director of GCHQ, wrote, ministers sought to make Britain "'the safest place to live and do business online'… It is, of course, a relative ambition and does not imply that the UK can be 100% safe. It was based on the key assessment that the UK could harden its defences to the point that cybercrime would be displaced elsewhere to easier targets. While this may sound cynical, it assumed that an international raising of the baseline would make all economies harder targets and encourage others to up their game. The long-term bet was that good resilience and security would become a market differentiator for UK business and attractive for inward investors".[22] Cybersecurity was a leading priority, among Britain's four "Tier One threats", in a tough national security strategy, which slaughtered many sacred cows.[23] The government defined clear criteria for success on the strategy bridge between policy and action, including coordination between departments, and with private firms. A £650,000,000 programme over four years funded cybersecurity well.[24] GCHQ seized almost 60% of that budget, and responsibility for "the most sophisticated nation state attacks". The Computer Emergency Response Team, an open body under the Cabinet Office, handled most assaults on firms.[25]

Directors of GCHQ recognised that the danger existed, must be solved, and offered rewards. They did not understand the technicalities of cybersecurity, but drove subordinates to address them. In order to achieve these aims, they created a new system for cybersecurity. Ciaran Martin, an official with wide experience in Whitehall, including intelligence, but not at GCHQ, became manager of cybersecurity and communications security. He worked with radical modernisers within GCHQ's communication security to handle cybersecurity, where they followed original ideas, and studied American and Israeli models. Between

21 Cabinet Office*, Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space,* (CM 7642, June 25 2009).

22 Robert Hannigan, *Organising a Government for Cyber, The Creation of the UK's National Cyber Security Centre*, RUSI Occasional Paper, February 2019, pp. 7-10.

23 *Securing Britain in an Age of Uncertainty, The Strategic Defence and Security Review*, CM 7948, 10.2010, pp. 47-9.

24 Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011.

25 Hannigan, *Organising*, p. 14.

2011-15, GCHQ worked closely with government agencies and firms, and established offices to assess cyber threats. As Hannigan wrote, assessing threats and risks on the cyber commons "is particularly difficult not just because it is a relatively new field but because it requires in-depth technical understanding alongside assessment of other sources… ministers who had a framework for judging the seriousness of a terrorist threat or incident had no framework against which to measure cyber threats. The figures were always large, because all figures on the internet are, and no one knows what 100% is: internet data is hard to measure and not static. Traditional assessment bodies, notably the venerable UK Joint Intelligence Committee, simply did not have access to the right technical skills to make useful assessments or even to second-guess those made by others". Even more, policy faltered because "no one has asked the obvious question of the right experts. Particularly in the UK civil service, which tends to favour generalism over deep and long expertise, there simply were not individuals who could give creative technical advice, or indeed assess suggestions made by others".[26] Some of these criticisms could also have been applied to GCHQ, at the time.

These successes were dissipated because agencies gave conflicting advice to firms, which could not handle the burden thrust on them. GCHQ gave intelligence, and fought foes on the cyber commons, but firms mostly received advice, not aid, and could not be chivvied into line. State defence for firms was dislocated. Hacking attacks became high-grade, sometimes linked to foreign state Sigint agencies. The Bank of England warned that this chaos damaged Britain's economy, and softened security enough to attract cyber criminals. The national policy based on coordination had reached its limits. Leadership was needed. After the election of 2015, the Conservative government demanded a national strategy, guided by one public centre for cybersecurity, and led by GCHQ. "When a cyber incident happened there were lots of departments represented at the table, but most of the questions gravitated to GCHQ", Cameron told Hannigan. GCHQ, the Chancellor of the Exchequer, George Osborne said, "is rightly known as equal to the best in the world… It is the point of deep expertise for the UK government. It has an unmatched understanding of the internet and of how to keep information safe".[27]

Other departments resisted the loss of authority in cybersecurity, until the security service, MI5, did so, breaking the logjam. Only law enforcement agencies, responsible for tackling forms of cybercrime, remained independent, though working closely with GCHQ. Many members of GCHQ disliked becoming public, and taking responsibility for cybersecurity. Senior ministers overcame these reservations, and assigned those responsibilities to "The National Cyber Security Centre, a part of GCHQ". That body had a unique name, and structure. Martin was the first head of the NCSC, with Ian Levy its Technical Director or, as he said, the government's "chief cyber security geek".[28] Five of its leaders were avowed, able to speak and be named openly, more than in the rest of GCHQ. By spring 2019, NCSC had 740 staff, approaching 10% of the total strength of GCHQ. NCSC had elements within the

26 *Ibid*., pp. 10, 39.

27 *Ibid*., p. 14.

28 "Dr. Ian Levy", Enigma 2017, https://www.usenix.org/conference/enigma2017/speaker-or-organizer/dr-ian-levy-national-cyber-security-centre-uk

Doughnut, GCHQ's headquarters in Cheltenham, alongside world leaders in cyber intelligence and sigint, and offices in London, beside private citizens. NCSC was within the Government Security Zone, close to ministers. During emergencies, NCSC and GCHQ gave Whitehall real-time knowledge of cyber threats, and struck them down where possible as they rose. NCSC combined two compartments, one working with open cybersecurity communities, and the other with secret agencies. NCSC, like Bletchley Park, was freewheeling, with many parts. NCSC became Inspector General for cybersecurity with firms, the mobiliser of civilian resources for that purpose, agony aunt for those suffering digital heartaches, and missionary for social and educational change in the nation.

Once NCSC was created, it quickly took command of British policy for cyber security, aiming to defend Britain's society and economy. As Martin said, "We want this digital revolution to succeed. Our job is to help make the digital economy and digital Government work, by making it safer" against "the three main motivations for systematic cyber attack… One is power: the traditional 'statecraft' just playing out in the digital age. Countries and rogue actors seeking to gain advantage by stealing secrets, or by pre-positioning for a destructive attack in a time of tension. Another one's money: anything from the sophisticated theft of intellectual property to the simple theft of cash from a bank account. Another is propaganda". Hostile states included "great powers, using cyber attacks to spy, gain major commercial and economic advantage or to pre-position for destructive attack". Smaller states exploited "the relatively immature rules of the road in cyberspace to tweak the nose of those they see as bigger powers in a way they would and could never contemplate by traditional military means". Some criminals "operate under the protection or tolerance of uncooperative states, and this is something new about cyber because it makes it much harder to bring them to justice because they don't need to set foot in our jurisdictions or those of our allies to harm us. Some of these gangs are extraordinarily sophisticated. We've seen some of the most MBA-grade management information systems that tell them, in great detail, which lines of attack are profitable and which are not. But not all that much of the crime we see is MBA-grade and too much of it gets through". The "world's major terrorist groups have the intent, but not the capability, to launch a destructive cyber attack. Now, that might change." Meanwhile, Britain must contain "the horrific misuse of the Internet by terrorists across the globe for the purposes of propaganda and radicalization".[29]

NCSC worked with GCHQ, and military cyber forces, against attacks by hackers and nation states, including regular forays across the cyber commons, to find threats, and disable or ambush them. NCSC also followed a deeper strategy, aimed "to make the UK safer in cyberspace… put right some of the security flaws built into the internet" and "change the economic equation for cyber criminals and alter the attacker-defender landscape". The government moved "from blaming users and expecting individuals to bear all the strain of security".[30] Levy formulated this strategy, "The Active Cyber Defence" programme, which

[29] "A new Approach for cyber security in the UK", 13.9.2016, https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

[30] Hannigan, *Organising*, pp. 40-42.

NCSC published openly. He emphasised "a common complaint from industry to governments about cyber security. It's generally that governments tell them they're not doing enough and must do more, often without really understanding the real-world impacts or commercial implications of their demands. Well, our strategy is to use government as a guinea pig for all the measures we want to see done at national scale. We'll be eating our own dog food to prove the efficacy (or otherwise) of the measures we're asking for, and to prove they scale sensibly before asking anyone to implement anything".

The NCSC challenged fundamental principles of the internet, by making security rather than surveillance its base. Working with private firms, NCSC tackled technical weaknesses within the internet, like improving standards for email, or infrastructure protocols by which internet providers routed messages. The NCSC would "drive the UK software ecosystem to be better", by warning British entities that communicated with government websites of vulnerabilities in their software. Levy also attacked firms whose sales pitch "basically says 'you lot are too stupid to understand this and only I can possibly help you – buy my magic amulet and you'll be fine.' It's medieval witchcraft, it's genuinely medieval witchcraft."[31] NCSC also would "go looking for badness and take it down", disabling websites across the internet which attacked British targets. "We're still going to do things to demotivate our adversaries in ways that only GCHQ can do". That statement was "euphemistic by design". Levy warned, "All of this will evolve. Some of it will work: some won't. We'll have to respond to adversaries as they respond to our defences. That's probably the new normal though…It's time to stop talking about what the winged ninja cyber monkeys can do and start countering in an automatic way the stuff we see at massive scale that causes real damage to citizens and businesses alike every day".[32]

These successes occurred despite a great public scandal. In 2013 Edward Snowden, a contractor and systems administrator at NSA, copied reams of records about the working of UKUSA, and leaked them to journalists and activists. Suddenly, the public and technical specialists confronted the reality of militarization and Comint on the cyber commons, and were genuinely shocked. Initially, the disclosures were incomprehensible. As every case of traffic analysis against metadata (and sometimes, merely the number of messages collected and anonymised) was taken to mean the reading of mail, people assumed that the Five Eyes read infinitely more messages than was true, confusing the "full stop" for the "beer mat" and sometimes even the "billiards table". *The Guardian* wrote that authorities had powers "beyond what Orwell could have imagined". Privacy International complained that "while the Stasi had files on one in three East Germans", GCHQ "intercepted and stored" the "communications of almost everybody in the UK".[33] These disclosures were erroneous, one-sided and naïve. Critics assumed that just a few western countries conducted Comint on the cyber commons, unlike

31 Iain Thompson, 3.2.2017, "GCHQ cyber-chief slams security outfits peddling 'medieval witchcraft', *The Register*, https://www.theregister.co.uk/2017/02/03/security_threat_solutions/

32 Ian Levy, Blog Post, 1.11.2016, "Active Cyber Defence—tackling cyber attacks on the UK", https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

33 "UK Debate Grows over 'Orwellian' NSA and GCHQ Surveillance", *The Guardian*, 9.10.2013, https://www.theguardian.com/world/2013/oct/09/debate-grows-orwellian-nsa-technology

nice states such as China and Russia, whose spokesmen swore on their word as gentlemen that they never would consider doing such a thing. Critics held that these practices aimed solely to monitor UK and US citizens' lives, ignoring matters like war, terrorism, cyber-crime and hostile state activity. Critics of Sigint – competent or incompetent, principled or hostile – drove the disclosures. A classic press campaign, like Lord Beaverbrook's Empire Crusade, aimed to sell newspapers. Internet libertarians, viewing state intelligence and secrecy as evil, purported to defend freedom from the slavery caused by pursuit of security. These comments had some force, but more melodrama. They ignored the problems of competitions on common ground, and the existence of enemies. They considered only peoples being attacked by their own state—not those assaulted by foreign governments, or exploited by criminals. In western countries, most people would not be assaulted by their own states: more would be attacked by foreign governments, and private parties. Fewer people might fear Big Brother than need his help, or want it.

This crisis stunned GCHQ. It did not know what material would be published. Its representatives could not at the outset clearly explain the legal or technical issues in public, nor how GCHQ had saved British lives. However, GCHQ's record and myth saved it. Leading Conservative and Labour politicians agreed that GCHQ had properly informed them of its actions. The technicalities involved, and the constant drip of information, confused and bored the public. Quickly, evidence emerged that every competent state conducted Sigint, while cyber criminals and terrorists planned to exploit or attack British subjects. The enemies of Sigint overplayed their hands, by making statements which obviously they could not substantiate, and which were untrue – such as that bulk collection had not reduced terrorist attacks, or by inflating the number of messages of British citizens which GCHQ read. The debate turned on myths. Critics insinuated that GCHQ was Big Brother, or Sauron. Civilians could not easily imagine Bletchley's heirs as orcs. British people thought they faced existential threats, against which they viewed GCHQ as Gandalf and themselves as Hobbits in need of help. Slowly, the debate became informed and public. Balanced reports by objective experts undercut alarmism. Otherwise, British cyber security could not have achieved success.

NCSC's programme involved many actions which might arouse suspicion of government censorship or surveillance. The NCSC countered that danger by establishing a reputation "as a trustworthy and transparent organisation", and publicised means for anyone to opt out of its proposals. The public, even seasoned critics of GCHQ, knew that the problem was great and must be solved. They viewed NCSC as a bobby on the beat, rather than a secret policeman. Openness created trust that Siginters worked for the security of the nation, rather than subverting its liberties. NCSC warnings of threats, and weekly and yearly estimates of security problems, with different versions for technical specialists, businesses, and individuals and families, became a common feature in British media, and reached many audiences. They were an open equivalent of the secret reports which GCHQ, and JIC, published throughout the Cold War. NCSC was the first organisation to provide national intelligence assessments to plain folk regularly, providing, for example, "evidence of Russian pre-positioning on some of our critical sectors, along with detailed technical guidance to business on how to get rid of it from our

networks".[34] Though most of these reports came from open sources, some involved NCSC's own work. No doubt old practices of sanitization covered the dissemination of material from more secret sources. That NCSC and GCHQ both released far more material to the public about their work than ever before, including that against states, was another sign of differences between the first and second ages of Sigint.

Japan and Sigint in 2022

Sigint is a major issue for Japan in 2022, far more than most Japanese appreciate. Secrets surround sigint in every country, but especially in Japan, where siginters emphasise their isolation and autonomy to a remarkable degree, which governments accept and few people challenge. The following comments rest on analysis of the limited material available on the topic in the public domain, and cannot pretend to be complete, though I hope that they are accurate, and useful.

Japan confronts problems in sigint, and the need for solutions. Modern Japanese sigint is perhaps more dependent on that of another country, than is true of any other advanced power. It emerged through cooperation and integration with the United States, which also has shaped Japanese defence policy far more than Washington has done with most of its allies, or possibly any other of them. Japan has a mixed record in using intelligence to bolster its policy, and a long one of mediocrity in communications security. It confronts two threats, Russia and China, which treat intelligence as a great weapon. Russian human intelligence has done well in penetrating the cryptography of foreign navies, so reducing their power in sigint and gaining some degree of intelligence superiority over them. Japan must beware of these threats, and remember that its main ally, the United States, also has a mediocre record in communications security, especially for navies. Every major power, friend, foe or neutral, will attack Japanese diplomatic traffic, while Russia and China will practice cybersubversion and cyberintelligence against Japanese firms, society and politics. Japan must prepare sigint suited to clashes between warships and aircraft, applying classic modes of collection and analysis to "Air/Sea warfare", and also against cyber threats. In both cases, the devil will be in the details.

Japan has taken steps to bolster its cybersecurity. In 2014-15, it established a "Cybersecurity Strategic Headquarters", under the Chief Cabinet Secretary, and a "National Center of Incident Readiness and Strategy for Cyber Security". In 2021, Japan adopted a national "Cyber Security Strategy", which emphasizes ties with allies, and links between state agencies, firms and the public, so to coordinate IT and security. All of this sounds good, but experience shows that such efforts must be tailored to suit an individual country—Britain, Israel, Singapore and the United States each approach the topic in different ways, and through unique institutions. Mere words or forms do not produce cybersecurity. That end requires national and public leadership, novel and difficult forms of coordination between state and society, more openness about sigint, and changes in the attitudes of siginters. British success in cyber security, for example, required a decade's hard work, driven by top levels of government,

34 *NCSC Annual Report 2018*, p. 10.

GCHQ's willingness to accept fundamental reforms in structure, the active involvement of every department of state, and a national decision to funnel great resources to the task, and to make GCHQ a public executive organ, as much like the RAF as MI6. The Japanese tendency to insulate sigint from contact with civilian agencies and the public, and its lack of high grade power in comint and offensive cyber, will handicap the development of its cyber security. In order to achieve these aims, the national government must lead firmly, and ensure that siginters, normal officials, businessmen and opinion leaders, work together, which requires their willing cooperation, translucency by the state and trust from its people. I fear that Japan is far weaker in cybersecurity than Japanese imagine. In 2022, it is no better with cybersecurity than was Britain during 2007. Just as Canadian cybersecurity improved by learning lessons from Britain, Japanese might study the Singaporean experience with the topic.

Japanese also might reconsider the links between sigint and strategy, where a good model lies in recent history. The "maritime strategy" involved the most secretive component of western intelligence during the cold war. From 1975, the Soviet navy abandoned its efforts to deploy nuclear ballistic submarines (SSBNs) across the world, vulnerable to detection and destruction, instead deploying them in the White Sea, where nuclear attack submarines (SSNs) and other forces could protect them. The United States Navy (USN) and the RN prepared to engage all of these forces, especially the SSBNs, so provoking a hidden struggle between both sides.[35] This struggle involved many intelligence sources. The best known of them was "Sound Surveillance System", SOSUS, a system of undersea microphones across the world which detected Soviet submarines, and the most secret is Sigint. Throughout the cold war, SSNs sought to move beside enemy forces without detection, so to train for war. Some of these SSNs carried sigint cells, which tracked Soviet warships, intercepted plain language voice at close range and acquired technical details about detection and communications systems, and the distinct "sound signatures" of machinery and propellers produced by all warships. SSNs collected intelligence to understand and to fight the foe, and used sigint to guide their patrols. The use of sigint was eased because the maritime strategy centred on three members of the Five Eyes, Britain, Canada and the United States, able to share all grades of intelligence, and Norway, among the most trusted of NATO third parties, which also aided the task through aerial reconnaissance, an area of collection which could be isolated from sigint, while still serving its purpose. The power of SOSUS and sigint helped to drive the Soviet Navy from the blue water of the Atlantic to the green water of the White Sea, offered aid even there, and revealed Soviet decisions to American authorities, so sparking the maritime strategy itself. However, Soviet espionage recruited many traitors, especially the Walker-Whitworth family of spies in the United States, but also Geoffrey Prime in Britain, (and a generation later, Jeffery Delisle in Canada), who compromised western maritime intelligence and sigint, and also USN

[35] John B. Hattendorf, "The Evolution of the U.S. Navy's Maritime Strategy", *Newport Papers*, No. 19*, (2004).* https://digital-commons.usnwc.edu/newport-papers/35; John B. Hattendorf and Peter M. Swartz, (eds), *U.S. Naval Strategy in the 1980s: Selected Documents, The Newport Papers, No. 33*, https://digital-commons.usnwc.edu/newport-papers/21; Cote, Owen R. Jr, "*The Third Battle*" *The Newport Papers*. https://digital-commons.usnwc.edu/newport-papers/38 No.16, (2003)

cryptosystems, which would have given the Soviets an edge had the cold war gone hot.[36]

The RN's work during the cold war has parallels with that of the Japanese Navy today, though differences as well. The RN, the third greatest navy of the era, specialized in blue water anti-submarine warfare and fleet operations, with a world capability. It worked organically with the USN, especially on the maritime strategy, which provided access to many key technical developments, while joint membership in the Five Eyes eased intelligence exchange. The enemy was the Soviet Navy, a numerically equal but qualitatively inferior fleet, which faced unusual difficulty in projecting power outside its coasts, but was hard to attack. At that time, the Japanese Navy had a smaller and more defensive and dependent role, but still a crucial one, in helping the USN to block Soviet access to the blue water of the Pacific Ocean. Japanese naval strategy centred on pinning Soviet warships to the Asian coast, where diesel electric submarines lurked in brown water, especially in the straits of Soya, Tsugaru and Tsushima, to locate and sink Soviet forces attempting to break out to the Pacific, so simultaneously protecting Japanese sea-lanes and enabling forward deployment of USN carrier battle groups to strike Soviet forces trapped in the Sea of Okhokst. Japanese submarines reconnoitred Soviet forces around Vladivostok, and its forces and sigint worked with but under their American counterparts.[37] Because of their operationally bilateral relations, probably Japanese sigint cooperated more closely with American agencies, than any European member of NATO did with the Five Eyes. However, Americans controlled the terms of trade on the exchange of techniques and traffic, and had little need to help Japan past a basic level. They gained from Japanese competence in tactical sigint and elint, but not from helping Japan to develop high-grade comint, or communication security. Japanese sigint followed American interests as much as it did Japanese ones. It performed well in traffic analysis and elint against military targets, and perhaps ranked equal to those of France or Germany, decent second rank players, but entirely lacked the interception, cryptanalytic and analytic capabilities of first rate sigint powers.

---

36 Aldrich, *GCHQ*, pp. 125-47; John Olav Birkeland, *Maritime airborne intelligence, surveillance and reconnaissance in the High North—The role of anti-submarine warfare—1945 to the present*, (Ph.d diss., University of Glasgow, 2021); Marcus Faulkner, "Naval Intelligence and Innovation: A Historical Perspective", in Alessio Patalano and James A. Russell, *Maritime Strategy and Naval Innovation, Technology, Bureaucracy, and the Problem of Change in the Age of Competition*, (Naval Institute Press, 2021), pp 90-106; Christopher Ford and David Rosenberg, *The Admiral's Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War*, (Naval Institute Press, Annapolis, MD, 2005); Christopher A. Ford and David Rosenberg, "The Naval Intelligence Underpinnings of Reagan's Maritime Strategy", *The Journal of Strategic Studies*, 28/2, 2005, pp. 379-409; Peter Hennessy and James Jinks, *The Silent Deep, The Royal Navy Submarine Service since 1945*, (Allen Lane, London, 2015); John Schindler, *A Dangerous Business: The USN and National Reconnaissance during the Cold War*, (Center for Cryptologic History, Fort Meade, MD, 2004); Susan Sontag and Christopher Drew, *Blind Man's Bluff: The Untold Story of Cold War Submarine Espionage*, (London, Arrow Books, 2000).

37 Narushige Michishita, Peter M. Swartz, and David F. Winkler, *Lessons of the Cold War in the Pacific: U.S. Maritime Strategy, Crisis Prevention and Japan's Role*, (Woodrow Wilson Center, Washington D.C., 2016); Alessio Patalano, "'The silent fight': submarine rearmament, and the origins of Japan's military engagement with the Cold War, 1955-76", *Cold War History*, 21/1, 2021, pp. 91-111; Alessio Patalano, "Shielding the 'Hot Gates': Submarine Warfare and Japanese Naval Strategy in the Cold War and Beyond (1976-2006)", *JSS*, 31/6, Dec. 2008, pp. 859-95; Alessio Patalano, "Japanese Naval Power", in Robert J. Pekkanen and Saadia M. Pekkanen (eds.), *The Oxford Handbook of Japanese Politics*, (OUP, 2021).

Now, Japan has large and advanced air forces and perhaps the third or fourth best navy at sea. It confronts radical changes with all categories of maritime forces, a new concept for maritime strategy, in the form of Air/ Sea battle, and two foes, Russia and China, each of which has access to green water, and aims to deploy forces into the blue Pacific. Japan has a blue water capability, with commitments against China and Russia in brown and green water from the East China Sea to the Sea of Okhokst. To handle these problems, Japan needs maritime capabilities like those of the RN during the cold war, especially in intelligence. Meanwhile, Japan operates alongside a few friends, sometimes called "The Quad". Two of its members, the United States and Australia, belong to the Five Eyes, as do two other powers which might affect matters, Britain and Canada. No member of "The Quad" is likely to trade sophisticated sigint with its fourth member, India. Under these circumstances, Japan easily might be cut from access to the highest levels of sigint, which could damage not merely Japanese interests, but broader ones, as the Five Eyes did to sigint and strategy with NATO. British experience during the cold war suggests that a nation in Japan's position must have credibility with and leverage on the United States, so to influence the formulation of strategy and to acquire the aid it needs in operations and intelligence. Japan requires more power and independence in sigint in order to become alliance-worthy and have the influence in Washington that it needs.

Against these problems stand opportunities. Since 9/11, advanced states have boosted their spending on sigint, above that for military forces. They all treat sigint as a major matter, one growing in importance. Japan has kept pace with most advanced states in these areas, though not the leading powers in sigint. GCHQ, for example, has 500% more personnel than Japanese sigint, with far greater capabilities in the most sophisticated forms of the practice, which has aided British influence across the world. Meanwhile, though the Five Eyes remain a distinct grouping, some of their old restrictions on sharing techniques and product with third parties have declined. For Japan, expansion in sigint is essential to support its enhanced role as an actor in strategy, both by providing intelligence directly and by driving the United States to offer more support. That expansion must include not merely high grade military targets, but also the diplomatic systems of enemies, neutrals and friends—including the United States, which is sophisticated enough not to complain about the practice, and respects those who help themselves. The stronger Japanese sigint becomes, the more the United States must cooperate with it, and the more Japan can lever Washington, and gain influence over its decisions and strategy. Strong sigint is essential to Japanese security.