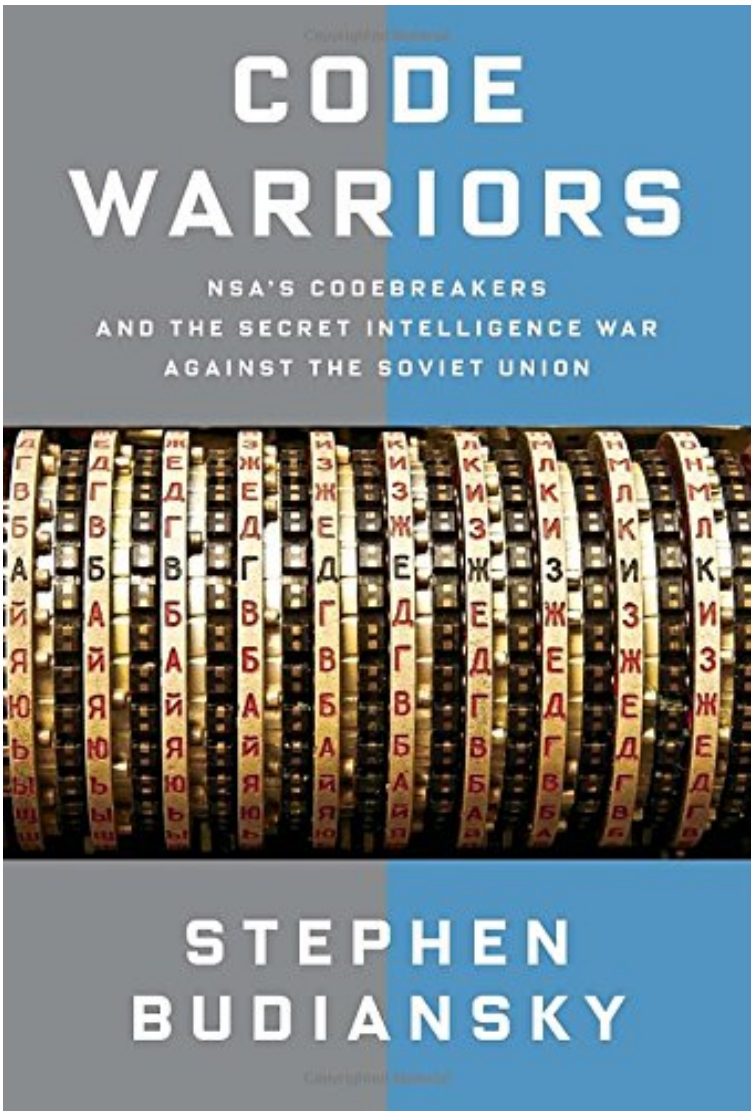
Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union

Stephen Budiansky
*ebooks | Download PDF | *ePub | DOC | audiobook*



#99559 in Books Alfred a Knopf Inc 2016-06-14 2016-06-14Format: Deckle EdgeOriginal language:EnglishPDF # 1 9.60 x 1.31 x 6.75l, 1.63 #File Name: 0385352662416 pagesAlfred a Knopf Inc | File size: 66.Mb

Stephen Budiansky : Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union before purchasing it in order to gage whether or not it would be worth my time, and all praised Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union:

0 of 0 people found the following review helpful. HarrowingBy SALRA well-researched and scary tale of what we like to think of as a model agency of clever sleuths but which is actually another example of government bungling and political rivalries. I'm sure there are many excellent people and success stories at NSA, but if this history since WWII is indicative, it is a harrowing reading experience.0 of 0 people found the following review helpful. Informative, for both the technical and non-technical.By S. JamalInformative, even if you already know a bit about cryptography. Even non-technical people can enjoy this. What is really shocking, and scary, is how foreign intelligence agents were able to operate inside the NSA undetected for so long, even though in some cases they should have been caught much sooner.0 of 0 people found the following review helpful. Just an excellent read on the history of the NSA and domestic ...By CustomerJust an excellent read on the history of the NSA and domestic codebreaking over the last 70 years or so, well written and entertaining considering its subject matter..... if you like this book, you may want to look at The Code Breakers by David Kahn. It's an older book, so not up-to-the-minute on code technology.....but it is a much more longer and more exhaustive history of codes from their very beginnings. A good deal drier to read unless you have a high interest in codes and codebreaking. .

A sweeping, in-depth history of NSA, whose famous cult of silence has left the agency shrouded in mystery for decades The National Security Agency was born out of the legendary codebreaking programs of World War II that cracked the famed Enigma machine and other German and Japanese codes, thereby turning the tide of Allied victory. In the postwar years, as the United States developed a new enemy in the Soviet Union, our intelligence community found itself targeting not soldiers on the battlefield, but suspected spies, foreign leaders, and even American citizens. Throughout the second half of the twentieth century, NSA played a vital, often fraught and controversial role in the major events of the Cold War, from the Korean War to the Cuban Missile Crisis to Vietnam and beyond. In Code Warriors, Stephen Budianskya longtime expert in cryptologytells the fascinating story of how NSA came to be, from its roots in World War II through the fall of the Berlin Wall. Along the way, he guides us through the fascinating challenges faced by cryptanalysts, and how they broke some of the most complicated codes of the twentieth century. With access to new documents, Budiansky shows where the agency succeeded and failed during the Cold War, but his account also offers crucial perspective for assessing NSA today in the wake of the Edward Snowden revelations. Budiansky shows how NSAs obsession with recording every bit of data and decoding every signal is far from a new development; throughout its history the depth and breadth of the agencys reach has resulted in both remarkable successes and destructive failures. Featuring a series of appendixes that explain the technical details of Soviet codes and how they were broken, this is a rich and riveting history of the underbelly of the Cold War, and an essential and timely read for all who seek to understand the origins of the modern NSA.

One of the Wall Street Journal's Top Ten Nonfiction Books of the yearA Washington Post Notable BookAbout the AuthorSTEPHEN BUDIANSKYwas the national security correspondent and foreign editor ofU.S. News World Report, Washington editor ofNature,and editor of World War IImagazine. He is the author of six books of military and intelligence history, includingBlacketts War, aWashington PostNotable Book. He has served as a Congressional Fellow, he frequently lectures on intelligence and military history, and his articles have appeared inThe New York Times,The Washington Post,The Wall Street Journal,The Atlantic,The Economist, and other publications. He is a member of the editorial board ofCryptologia,the leading academic journal of codes, codebreaking, and cryptologic history.Excerpt. Reprinted by permission. All rights reserved.1The Russian ProblemThe men and women who aimed to supplant Mata Hari with the steady, efficient, reliable, and ever so much safer methods of science and technology began their first tentative foray into what they would always call, with a certain clinical detachment, the Russian problem on February 1, 1943. Almost all of the codebreakers who would work over the next several years to achieve the first breaks into the labyrinth of Russian communications secrets were newcomers to the businesswhich made them no different from the other thirteen thousand new recruits, military and civilian, who would by the wars end swell the explosively growing ranks of the U.S. Army and Navy signals intelligence headquarters in Washington.1 The variety of their backgrounds was extraordinary: career officers and new draftees, young women math majors just out of Smith or Vassar, partners of white-shoe New York law firms, electrical engineers from MIT, the entire ships band from the battleship California after it was torpedoed by the Japanese in the attack on Pearl Harbor, winners of puzzle competitions, radio hobbyists, farm boys from Wisconsin, world-traveling ex-missionaries, and one of the worlds foremost experts on the cuneiform tablets of ancient Assyria.In June 1943, Cecil Phillips was an eighteen-year-old chemistry student at the University of North Carolina who had just been rejected for the draft because of flat feet (to my great pleasure and surprise, he later admitted); with no plans for the summer, he wandered into the U.S. Employment Service office in his hometown of Asheville, in the Blue Ridge Mountains, to see if he could get a job. The person there told him there was a lieutenant from the Army Signal Corps over at the town post office who had a large quota of clerk positions to fill.How would you like to go to Washington and be a cryptographer? the lieutenant asked him.That sounds interesting, Phillips answered.The lieutenant, clearly surprised that someone actually knew what he was talking about, blurted out, You mean you know what that means?Phillips did, having once owned a Little

Orphan Annie decoder ring, though that was about as far as his knowledge went. But it was good enough for the lieutenant, who administered him a general aptitude test on the spot, signed him up as a $1,440-a-year GS-2 junior clerk, and told him to report in a week to an address in Arlington, Virginia.2Brought in under nearly identical circumstances was a young home economics instructor, Gene Grabeel, who was teaching high school near Lynchburg in central Virginia and dissatisfied with her job when she met a young Army officer in the post office who was looking for college graduates to go to work at an undisclosed location near Washington, to do a job he could not offer any details about. (The officer, an infantry lieutenant who just days earlier had been posted with the First Army at Governors Island, New York, did not know himself what the work involved. Driven largely by the need to process volumes of Japanese army traffic that had suddenly become readable due to breakthroughs in several systems, the Army would hire four thousand new civilian employees for its signals intelligence operation in 1943 alone. In the rush to meet such burgeoning manpower requirements, the recruiters were as green as everyone else. The lieutenant had been ordered to report to Arlington Hall on Monday the week of Thanksgiving in November 1942; he spent the next day filling out administrative paperwork; Wednesday he was given a crash course on recruiting procedures; and on Thanksgiving morning he found himself at the post office in Lynchburg trying to collect warm bodies, without even having had a chance to find out what his new outfit did.) Grabeel had been thinking about trying to get a job with the federal government and asked her father what he thought of the idea. He told her she might as well go to Washington for six months and shuffle papers. She was off to the capital as soon as she found a replacement teacher to take over for her.3Arlington Hall Junior College had been a finishing school for girls before the Army abruptly seized it under emergency war powers in June 1942. The site was convenient to the Pentagon, the colossal new Army and Navy headquarters, soon to be the largest office building in the world, which was arising on a marshy flat along the Potomac River less than two miles away, just across Arlington National Cemetery. The schools one hundred acres also offered security and ample room for expansion. One of the Arlington Hall recruiters found a prewar postcard of the school, depicting a stately residence hall, manicured lawns, tennis courts, and indoor and outdoor horseback riding arenas and stables, and shamelessly deployed it in his recruiting pitch. What the new arrivals found instead were two huge, dreary, hastily erected warehouselike office blocks built in the traditional U.S. government style with long corridors and a series of perpendicular wings, surrounded by barbed wire and guardhouses. Workers sat side by side at long tables arrayed in rows. Air-conditioning remained a dream for the future; the buildings were sweltering in the humid Washington summers and overrun year-round with legions of rodents. There were no horses in the deserted stables, but there was a drill field and barracks for the enlisted men. The lieutenant who had paraded the prewar postcard avoided eye contact with his recruits when he later encountered them at Arlington Hall.4More than 70 percent of the staff at Arlington Hall were civilians, and by the wars end more than 90 percent of those were women. A similar balance of the sexes quickly took hold at the Navys signals intelligence headquarters, across the Potomac River. The Navy had a deep tradition of never permitting a situation to arise where an officer might have to take orders from a civilian, and insisted on putting all of its new hires in uniform. But with its establishment in summer 1942 of the WAVESWomen Accepted for Voluntary Emergency Service, which allowed women to serve in the Navy as officers and enlisted personnelthe service was also able to freely recruit women for codebreaking duty, and some 80 percent of its cryptanalysts by the wars end were female.5The joke making the rounds in Washington the first year of the war was that if the Army and Navy could capture enemy territory as fast as they were seizing it in the nations capital the fighting would be over in a couple of weeks. Not long after the Army claimed Arlington Hall, the Navy took possession of its own girls school, Mount Vernon Academy on Nebraska Avenue in northwest Washington. In February 1943 the Naval Communications Intelligence Section (known as Op-20-G in the arcane numbering system the Navys bureaucratic administrators had devised to designate its myriad branches and offices) moved into its new home at what was now officially called the Naval Communications Annex; construction crews went to work at once ripping out the schools graceful colonnaded walkways to make room for functional buildings; the headmistresss residence, with its elegant polished hardwood floors, was converted into the post exchange, selling Cokes and cigarettes; and a double line of wire fences went up around the perimeter, guarded by marines patrolling with submachine guns.6That summer there began arriving at Nebraska Avenues Building 4 the first of what would soon be a phalanx of one hundred massive electromechanical calculating machines. Built by the National Cash Register company at its factory in Dayton, Ohio, at a staggering total cost of $6 million, the bombes, as they were called, weighed two and a half tons apiece and housed sixty-four motor-driven wheels whose electrical contacts spun at speeds of up to 1725 rpm; when they were all running together they drew a quarter of a megawatt of electricity, enough to power a thousand homes.7 Their internal electrical logic was the genius of the eccentric British mathematician Alan Turing. Building on prewar work by a small team of Polish cryptanalysts who shared their results with the British just weeks before the Nazi invasion, Turing in the fall of 1939 developed a comprehensive mathematical solution to the Nazis legendary Enigma cipher machine. By guessing a few probable words contained in an enciphered Enigma message, he showed how to eliminate in one mathematical-logical leap about 1014 of the permutations that the Enigmas scrambling machinery relied upon to baffle any would-be codebreaker. That left only a few hundred thousand possibilities to test to recover the unique daily setting of the scrambling rotors used on each of

the high-level radio networks that employed the Enigma, the key to unlocking thousands of extremely secret signals a day: orders to U-boats prowling the Atlantic, reports on the dispositions and plans of Rommels troops in the North African desert or the state of the Nazis Western Wall defenses along the coast of France. The whirring wheels of the U.S. Navys bombes, re-creating the internal wiring of the rotors of the actual Enigma machines, could in twenty minutes try every possible starting setting of the Enigma (each of the three or four rotors of the Enigma could be set at twenty-six different positions, which meant there were 26 26 26 26 = 456,976 possibilities in the case of the four-rotor version used by the German U-boats). When the bombe reached a position consistent with a chain of letters built up from a short sequence of matching plaintext and cipher text, a circuit was completed through a series of interconnected cables used to program the bombe for each test, causing an electrical relay to trip and triggering a clutch and brake that would bring the device jolting to a halt, revealing the daily jackpot.8At the height of the Battle of the Atlantic nearly half of the staff at Nebraska Avenue was working on the Enigma problem; most of the rest were trying to keep up with the huge volume of Japanese navy traffic and the ever-changing complexities of its code systems, most of which used codebooks rather than cipher machines like the Enigma.9 IBM punch card machines turned out to be well suited to the exhaustive cataloging and searching required to break into these Japanese codes. The process involved combing through intercepted messages to hunt for repetitions of their four- or five-digit numerical cipher groupsa possible sign that two different messages had been prepared with the same string of obscuring key. Compared to a modern computer, punch card machines were undeniably primitive, but they could carry out massive data searches that would have overwhelmed a human being. Cards punched with the code groups of tens or even hundreds of thousands of messages could be automatically placed in numerical order by an IBM card sorting machine, then printed out in massive catalogs by a printing tabulator to be scanned by eye for any repetitions. The Japanese army codes worked much the same way as the Japanese navy codes, and by 1943 Arlington Hall and Nebraska Avenue were operating hundreds of IBM machines and paying the company three-quarters of a million dollars a year in rental fees, while burning through hundreds of thousands of punch cards a month.10What had begun as little more than tiny back-office research groups (at the outbreak of World War II in September 1939 the Armys Washington signals intelligence staff was nineteen people, the Navys thirty-six) had become veritable decryption factories, working round-the-clock shifts and tied to a sprawling global network of outstations that fed an uninterrupted stream of intercepted communications. Besides the thirteen thousand workers in Washington there were thousands more in the field manning a dozen principal intercept posts from Winter Harbor, Maine, to Bainbridge Island, Washington, and to points around the world as far-flung as the Aleutian Islands, the Canal Zone, Guam, and Recife, Brazil, each bristling with antennas and equipped with multiple shortwave receiver sets.11 Teams of enlisted men took down Morse code messages by hand and then retransmitted the copied traffic via encrypted landline or radio teleprinter links back to Washington or other cryptanalytic processing centers in Hawaii and Australia.By October 1943 Arlington Hall had up and running a semiautomated decryption processing line for Japanese army traffic that punched incoming teleprinter messages onto paper tape, converted the paper tape to IBM cards, matched the resulting decks of punch cards with other sets of cards punched with the corresponding sequence of cipher key, subtracted one from the other to reveal the underlying code groups and punched those on a third set of cards, and then used a library of cards containing code groups whose dictionary meanings had been recovered to print out the complete decoded message. In some cases Arlington Hall was reading a message before its intended Japanese recipient, who had to manually flip through his codebooks and work out the message on paper and pencil, could do so.12The size and extent of the American wartime cryptanalytic empire reflected the global reach of the conflict, but it also reflected the global nature of communications, and thus of intelligence opportunities ripe to be exploited. One of the most valuable sources of information on German preparations for the Allied D-Day landings would prove to be the reports of Japans ambassador in Berlin, in cables radioed six thousand miles back to his government in Tokyo using the Japanese diplomatic system known to the American codebreakers as Purple, a cipher machine they had cracked in 1940, sight unseen, in one of their most stunning achievements of pure mathematical cryptanalysis.Some of the size of the wartime enterprise, to be sure, also reflected what the British liaison officer sent to Arlington Hall, Captain Geoffrey Stevens, diagnosed with ill-concealed irritation as the American genius for constructing hopelessly overorganized operations.13 The work involved a huge amount of painstaking drudgery, and the American solution was to parcel out tasks exactly like a factory assembly line. When Cecil Phillips arrived at Arlington Hall on June 22, 1943, his first job was to stamp the date on incoming messages. Having demonstrated his competence at that task, he was promoted to stapling. But his first boss saw something in the high school graduate that perhaps Phillips himself did not, and started setting aside an hour or two a day to teach him the rudiments of cryptanalysis. On May 1, 1944, Phillips was led to the back of one of the wings on the second floor of B Building, where a fifty-by-fifty-foot area had been partitioned off with plywood screens from the rest of the open wing. A small opening between the screens, just large enough for one person to squeeze through, led past a desk where an Army captain sat with his back to the entrance, keeping a sharp eye on the several dozen people at work at long tables.14