bayes goes to war

By 1939 Bayes' rule was virtually taboo, dead and buried as far as statisticians in the know were concerned. A disturbing question remained, though. How could wartime leaders make the best possible life-and-death decisions swiftly, without waiting for complete information? In deepest secrecy some of the greatest mathematical minds of the century would contribute to rethinking Bayes' role during the uncertain years ahead.

The U-boat peril was the only thing that ever really frightened Winston Churchill during the Second World War, he recalled in his history of the conflict. Britain was self-sufficient in little other than coal; it grew enough food to feed only one in three residents. But after the fall of France in 1940, Germany controlled Europe's factories and farms, and unarmed merchant ships had to deliver to Britain 30 million tons of food and strategic supplies a year from the United States, Canada, Africa, and eventually Russia. During the Battle of the Atlantic, as the fight to supply Britain was called, German U-boats would sink an estimated 2,780 Allied ships, and more than 50,000 Allied merchant seamen would die. For Prime Minister Churchill, feeding and supplying his country was the dominating factor throughout the war.

Hitler said simply, "U-boats will win the war."[1]

U-boat operations were tightly controlled by German headquarters in occupied France. Each submarine went to sea without orders and received them by radio after it was well out in the Atlantic. As a result, an almost endless cascade of coded radio messages—more than 49,000 are still archived—raced back and forth between the U-boats and France. Although the Brit-

ish desperately needed to know where the U-boats were, the messages were unreadable. They had been encrypted by word-scrambling machines, and no one in Germany or Britain thought their codes could be broken.

Strangely enough, the Poles were the first to think otherwise. A few intelligence officers in Poland, sandwiched as they were between Germany and Russia, realized a full decade before the start of the Second World War that mathematics could make eavesdropping on their rapacious neighbors quite informative. The First World War had made the need for machines to encode radio messages painfully obvious. When an alphabet-scrambling machine was exhibited at an international trade show in 1923, Germany bought some and began introducing complexities to make their codes more secure. The machines were named Enigma.

And enigmas they were. The Poles spent three years trying unsuccessfully to crack German messages before realizing that automated cipher machines had transformed cryptography. The science of coding and decoding secret messages had become a game for mathematicians. When the Polish secret service organized a top-secret cryptography class for German-speaking mathematics students, its star pupil was an actuarial mathematician named Marián Rejewski. He used inspired guesswork and group theory—the new mathematics of transformation—to make a crucial discovery: how the wheels on an Enigma were wired. By early 1938 the Poles were reading 75% of Germany's army and air force messages. Shortly before their country was invaded in 1939 they invited French and British agents to a safehouse in the Pyry Forest outside Warsaw, revealed their system, and sent an updated Enigma machine to London.

To an observer, an Enigma looked rather like a complicated typewriter, with a traditional keyboard of 26 letter keys and a second array of 26 lettered lights. Each time a typist pressed a letter key, an electric current passed through a set of three wheels and advanced one of them a notch. The enciphered letter lit up on the lampboard, and the typist's assistant read the letter off to a third aide, who radioed the scramble in Morse code. At its destination, the process was reversed. The recipient typed the coded letters into his Enigma keyboard, and the original message lit up on his lampboard. By changing the wiring, wheels, starting places, and other features, an Enigma operator could churn out millions upon millions of permutations.

Germany standardized its military communications with increasingly complex versions of the machines. Approximately 40,000 military Enigmas were distributed to the German army, air force, navy, paramilitary, and high command as well as to the Spanish and Italian nationalist forces and the Italian navy. When German troops invaded Poland on September 1, 1939, battery-powered Enigmas were the key to their high-speed blitzkrieg as field officers in Enigma-equipped command vehicles coordinated, as never before, a barrage of artillery fire, dive-bombing airplanes, and panzer tanks. Most German naval vessels, particularly battleships, minesweepers, supply ships, weather report boats, and U-boats, had an Enigma.

Unlike the Poles, the British agency charged with cracking German military codes and ciphers clung to the tradition that decryption was a job for gentlemen with linguistic skills. Instead of hiring mathematicians, the Government Code and Cypher School (GC&CS) employed art historians, scholars of ancient Greek and medieval German, crossword puzzlers, and chess players. Mathematicians were regarded as "strange fellows."[2]

The British government and educational systems treated applied mathematics and statistics as largely irrelevant to practical problems. Well-to-do boys in English boarding schools learned Greek and Latin but not science and engineering, which were associated with low-class trade. Britain had no elite engineering schools like MIT or the École Polytechnique. Two years into the war, when government officials went to Oxford to recruit men proficient in both mathematics and modern languages, they found only an undergraduate mathematics major teaching himself beginning German. The government did not even plan to exempt mathematicians from combat. Knowing that their skills would be needed eventually, mathematicians quietly spread word to their colleagues to register with the government as physicists because they at least were considered vital to the nation's defense.

Exacerbating the emergency was the fact that the government regarded statistical data as bothersome details. A few months before war was declared in 1939, the giant retailer Lord Woolton was asked to organize the clothing for Britain's soldiers. He discovered to his horror that "the War Office had no statistical evidence to assist me. . . . I had the greatest difficulty in arriving at any figures that would show how many suits of uniform and how many boots were involved."[3] The Department of Agriculture ignored a study of the fertilizers needed to increase Britain's food and timber supplies because it thought the Second World War was going to be a nonscientific war and no more data would be needed. Government functionaries also seemed to think that applying mathematics to real life would be easy. When the Ministry of Supply needed to assess new rockets, it gave an employee one week to "learn statistics."[4]

Probability experts were scarce. For a small elite the 1930s had been the golden age of probability theory, the language of statistics. But the majority of mathematicians thought of probability as arithmetic for social scientists. Cambridge, the center of British mathematics, was a backwater in probability. Germany, a leader in modern mathematics and quantum physics, produced few statisticians. And one of the greatest probability thinkers of the twentieth century, Wolfgang Doeblin, was a 25-year-old French soldier fighting for his life as France fell to the Germans in June 1940. The Gestapo was hunting his father, and Doeblin, surrounded and without hope of escape, killed himself to avoid any chance of betraying his parent. Doeblin's work would one day be crucially relevant to chaos theory and random mapping transformations.

Oddly, the Allies' top three statisticians were sidelined during the war. Harold Jeffreys was ignored, perhaps because he was an earthquake specialist and astronomy professor. British security apparently considered Ronald Fisher, the anti-Bayesian geneticist, to be politically untrustworthy because he had corresponded with a German colleague. Fisher's offers to help the war effort were ignored, and his application for a visa to the United States was rejected without explanation. A chemist calculating the dangers of poison gas succeeded in arranging a visit to Fisher only by claiming he was collecting a horse nearby. As for Jerzy Neyman, he persisted in carrying out full theoretical studies that could lead to a new theorem even though the military desperately needed quick and dirty advice; one of Neyman's grants was formally terminated.

With applied mathematicians and statisticians in short supply, wartime data were often analyzed not by statisticians but by actuaries, biologists, physicists, and pure mathematicians—few of whom knew that, as far as sophisticated statistics was concerned, Bayes' rule was unscientific. Their ignorance proved fortunate.

Despite the strange reputation of British mathematicians, the operational head of GC&CS prepared for war by quietly recruiting a few nonlinguists—"men of the Professor type"[5]—from Oxford and Cambridge universities. Among that handful of men was Alan Mathison Turing, who would father the modern computer, computer science, software, artificial intelligence, the Turing machine, the Turing test—and the modern Bayesian revival.

Turing had studied pure mathematics at Cambridge and Princeton, but his passion was bridging the gap between abstract logic and the concrete world. More than a genius, Turing had imagination and vision. He had also developed an almost unique set of interests: the abstract mathematics of topology and logic; the applied mathematics of probability; the experimental derivation of fundamental principles; the construction of machines that could think; and codes and ciphers. Turing had already spent hours in the United States discussing cryptography in his high-pitched stammer with a Canadian physicist named Malcolm MacPhail.

After Turing returned to England in the spring of 1939, his name was quietly added to a short "emergency list" of people with orders to report immediately to the GC&CS in the event war was declared. He worked alone that summer, studying both probability theory and Enigma codes. Occasionally he visited GC&CS to talk with a cryptanalyst, Dillwyn Knox, who had already solved a relatively simple Enigma code used by the Italian navy. By the time Germany invaded Poland, Knox and Turing probably understood more about military Enigmas than anyone else in Britain.

On September 4, the day after England declared war on Germany, Turing took a train to the GC&CS research center in Bletchley Park, a small town north of London. He was 27 but looked 16. He was handsome, athletic, shy, and nervous and had been openly homosexual at Cambridge. He cared little about appearances; he wore shabby sports coats and had dirty fingernails and a permanent five-o'clock shadow. He would devote the next six years to Enigma and to other coding and decoding projects.

On his arrival in Bletchley Park, GC&CS analysts divided up the Enigma systems, and Turing worked awhile on army codes. By January the English were reading German air force messages. During the first weeks of the war Turing also designed the "bombe." This was not a weapon in the traditional sense but a high-speed electromechanical machine for testing every possible wheel arrangement in an Enigma. Turing's bombe, a radical redesign and upgrade of the device invented by the Poles, would turn Bletchley Park into a code-breaking factory. Turing's machine tested hunches, 15-letter tidbits suspected of being in the original message. Because it was faster to toss out possibilities than to find one that fit, Turing's bombe simultaneously tested for wheel combinations that could not produce the hunch.

Turing refined the bombe's design with the help of mathematician Gordon Welchman and engineer Harold "Doc" Keen. Their prototype, a metal cabinet roughly 7 by 6 by 2.5 feet, appeared at Bletchley Park in March 1940. Some believe the bombe's design was Turing's biggest contribution to breaking Enigma.

Despite the progress made on breaking German air force and army codes, no one at Bletchley Park wanted to tackle the German naval codes, the key to winning the U-boat war in the Atlantic. Of all the branches of the

Axis military, Hitler's navy operated the most complex Enigma machines and security systems. By war's end, a naval Enigma machine could be set up an astronomical number of ways. According to a Bletchley Park decoder, "All the coolies in China could experiment for months without reading a single message."[6] At any one time the machine could use 1 of 4 reflector combinations (each of which could be set in 26 different ways); 3 of 8 rotors (giving up to 336 permutations); more than 150 billion plugboard combinations; 17,000 possible clip positions around the rotors; and 17,000 possible starting positions (half a million in four-rotor machines). Many of these settings were changed every two days, sometimes every 8 or 24 hours.

According to Frank Birch, head of the GC&CS naval intelligence branch, superior officers informed him that the "German codes were unbreakable. I was told it wasn't worthwhile putting pundits onto them. . . . Defeatism at the beginning of the war, to my mind, played a large part in delaying the breaking of the codes."[7] The naval codes were assigned to one officer and one clerk; not a single cryptanalyst was involved. Birch, however, thought the naval Enigma could be broken because it had to be. The U-boats put Britain's very existence at stake.

Turing had still another attitude. The fact that no one else wanted to work on the naval codes made them doubly attractive. A close friend called Turing "a confirmed solitary."[8] Isolation appealed to him. Announcing that "no one else was doing anything about it and I could have it to myself," Turing decided to attack the German naval code.[9] He began working on naval Enigma with a staff of two "girls" and an Oxford mathematician-physicist, Peter Twinn.[10] Turing thought the code "could be broken because it would be so interesting to break it."[11]

One of Turing's first jobs was to reduce the number of tests a bombe had to conduct. Although it was fast, a bombe took 18 minutes to test a possible wheel setting. Assuming the worst, a bombe would need four days to test all 336 possible wheel permutations on an Enigma. Until more bombes could be built, their workload had to be drastically reduced.

Late one night soon after joining Bletchley Park, Turing invented a manual method for reducing the burden on the bombes. It was a highly labor-intensive, Bayesian system he nicknamed Banburismus for the nearby town of Banbury, where a printing shop would produce needed materials.

"I was not sure that it would work in practice," Turing said.[12] But if it did, it would let him guess a stretch of letters in an Enigma message, hedge his bets, measure his belief in their validity by using Bayesian methods to

assess their probabilities, and add more clues as they arrived. If it worked, it would identify the settings for 2 of Enigma's 3 wheels and reduce the number of wheel settings to be tested on the bombes from 336 to as few as 18. At a time when every hour counted, the difference could save lives.

Turing and his slowly growing staff began to comb intelligence reports to collect "cribs," Bletchley-ese for German words predicted to occur in the plain-text, that is, the original, uncoded message. The first cribs came primarily from German weather reports because they were standardized and repeated often: "Weather for the night," "Situation Eastern Channel," and, as one blessed fool radioed nightly, "Beacons lit as ordered." Reports from British meteorologists about weather in the Channel provided more hunches. Knowing the most frequent letter combinations in German words helped too. When a prisoner of war told them the German navy spelled out numbers, Turing realized that the word "ein" ("one," "a," or "an") appeared in 90% of Enigma messages; Bletchley Park clerks catalogued by hand 17,000 ways "ein" could be encrypted, and a special machine was constructed to screen for them.

In a fundamental breakthrough, Turing realized he could not systematize his hunches or compare their probabilities without a unit of measurement. He named his unit a ban for Banburismus and defined it as "about the smallest change in weight of evidence that is directly perceptible to human intuition."[13] One ban represented odds of 10 to 1 in favor of a guess, but Turing normally dealt with much smaller quantities, decibans and even centibans. The ban was basically the same as the bit, the measure of information Claude Shannon discovered by using Bayes' rule at roughly the same time at Bell Telephone Laboratories. Turing's measure of belief, the ban, and its supporting mathematical framework have been called his greatest intellectual contribution to Britain's defense.

To estimate the probability of a guess when information was arriving piecemeal, Turing used bans to discriminate between sequential hypotheses. He was thus one of the first to develop what came to be called sequential analysis. He used bans to quantify how much information was needed to solve a particular problem so that, instead of deciding how many observations to make, he could target the amount of evidence needed and stop when he had it.

Bans involved a manual, paper-and-pencil system far removed from a modern computerized Bayesian calculation. Bans automated the kind of subjective guessing that Émile Borel, Frank Ramsey, and Bruno de Finetti

had tried to validate during the anti-Bayesian onslaught of the 1920s and 1930s. Using Bayes' rule and bans, Turing began calculating credibility values for various kinds of hunches and compiling reference tables of bans for technicians to use. It was a statistics-based technique and produced no absolute certainties, but when the odds of a hypothesis added up to 50 to 1, cryptanalysts could be close to certain they were right. Each ban made a hypothesis 10 times more likely.

A top modern-day cryptographer explained Turing's thinking: "When you work day after day, year after year, you need to make a best guess of what's most likely to be breakable with the resources at hand. You may have too many choices, so you pick the more checkable guesses. At every step you hedge bets. . . . Sometimes you make approximations, and other times you have precisely correct numbers with the right formulas, the right numbers, for the decibans."[14]

In operation, Banburismus used 5- or 6-foot-long strips of thin cardboard printed in Banbury. Decoders look for repetitions and coincidences, so Wrens, technicians from the Women's Royal Naval Service, punched each intercepted message by hand, letter by letter, into a Banbury sheet. Then they slipped one strip on top of others so that any two messages could be compared. When enough letter holes showed through both Banburies, the number of repeats was recorded.

As Patrick Mahon, who worked on Banburismus during the war, wrote in his secret history of Bletchley Park, "If by any chance, the two messages have identical content for 4 or 6 or 8 more letters . . . such a coincidence between cipher texts is known as a 'fit.'"

"The game of Banburismus involved putting together large numbers of pieces of probabilistic information somewhat like the reconstruction of DNA sequences," Turing's statistical assistant, I. J. "Jack" Good, explained later.[15] Good, the son of a Jewish watchmaker from tsarist Russia, had studied pure mathematics at Cambridge and waited a year for a defense job before being hired on the strength of his chess playing. Good thought "the game of Banburismus was enjoyable, not easy enough to be trivial, but not difficult enough to cause a nervous breakdown."[16] Bayes' rule was proving to be a natural for cryptography, good for hedging bets when there were prior guesses and decisions to be made with a minimum of time or cost.

Turing was developing a homegrown Bayesian system. Finding the Enigma settings that had encoded a particular message was a classic problem in the inverse probability of causes. No one is sure where Turing picked Bayes

up, whether he rediscovered it independently or adapted it from something overheard about Jeffreys, Cambridge's lone defender of Bayes' rule before the war. All we know for sure is that, because Turing and Good had studied pure mathematics and not statistics, neither had been sufficiently poisoned by anti-Bayesian attitudes.

In any event, Turing talked at Bletchley Park about bans, not Bayes.

Once Good asked, "Aren't you essentially using Bayes' theorem?"[17] Turing answered, "I suppose." Good concluded that Turing knew of the theorem's existence. But Turing and Good may have been the only ones at Bletchley Park who realized that Banburismus was Bayesian, and heavily so.

Good met a friend, George A. Barnard, one day in London and—strictly against the rules—"told him that we were using Bayes factors, and their logarithms, sequentially, to discriminate between two hypotheses but of course I did not mention the application. Barnard said that curiously enough a similar method was being used for quality control in the Ministry of Supply for discriminating between lots rather than hypotheses. It was really the same method because the selection of a lot can be regarded as the acceptance of a hypothesis."[18] Sequential analysis differed from frequency-based testing, where the number of items to be tested was fixed from the beginning. In sequential analysis, once several tests or observations strongly cleared or condemned a case of, say, field rations or machine-gun ammunition, the tester could move on to the next box. This almost halved the number of tests required, and the use of logarithms massively simplified calculations by substituting addition for multiplication. Abraham Wald of Columbia University is generally credited with discovering sequential analysis for testing ammunition in the United States later during the war. But Good concluded that Turing had used it first and that Turing, Wald, and Barnard all deserved credit for discovering and applying it. Oddly enough, after the war Barnard would become a prominent anti-Bayesian.

Turing was making progress when, in May 1940, the doldrums hit. He had both the theory and the method for breaking Enigma codes but still could not read U-boat messages. The Germans were building more U-boats, and Adm. Karl Doenitz had formed wolf packs of subs strung across the North Atlantic; when one U-boat spotted a convoy, it radioed the rest. During the first 40 months of the war, U-boats sank 2,177 merchant ships totaling more than 1 million tons, far more than were lost to German aircraft, mines, warships, and other causes.

If the British were going to be able to route supply convoys around the U-boats, Turing needed more information. He needed to see one of the codebooks that U-boat Enigma operators used before broadcasting a ciphered message. One of the factors that made breaking the Enigma code so difficult was that the operator doubly-enciphered a trio of letters that began each message and that indicated the starting positions of the Enigma's three wheels. The operator enciphered the three letters twice over: once mechanically, with his Enigma machine, and once manually, by selecting one of nine sets of tables in a codebook issued to each sub. The operator learned which table to use each day by consulting a calendar issued with the tables. If a U-boat came under attack, crews had strict orders to destroy the tables either before abandoning ship or as the enemy was about to board.

In a brilliant piece of deduction shortly after war was declared, Turing figured out this double-encipherment system, but he needed a copy of the codebook to make Banburismus work. Enigmas had so many variations that trial-and-error methods were ineffective. A codebook had to be "pinched," as Turing put it. The wait for a pinch would stretch through ten nerve-racking months.

As Turing waited desperately for the navy to get him a codebook, morale at GC&CS sank. Alastair G. Denniston, the head of GC&CS, told Birch, "You know, the Germans don't mean you to read their stuff, and I don't expect you ever will."[19]

Long and bitter arguments broke out about whether more bombes should be built, and if so, how many. In August 1940 Birch wrote, "Turing and Twinn are like people waiting for a miracle, without believing in miracles. . . . Turing has stated categorically that with 10 machines [bombes] he could be sure of breaking Enigma and keeping it broken. Well can't we have 10 machines?"[20]

A second bombe incorporating Welchman's improvements arrived later that month, but the fight for more bombes continued throughout 1940. Birch complained that the British navy was not getting its fair share of the bombes: "Nor is it likely to. It has been argued that a large number of bombes would cost a lot of money, a lot of skilled labour to make and a lot of labour to run, as well as more electric power than is at present available here. Well, the issue is a simple one. Tot up the difficulties and balance them against the value to the Nation of being able to read current Enigma."[21]

To capture a codebook, Lt. Cmdr. Ian Fleming, the future creator of James Bond but at the time an aide to the head of Britain's Directorate of Naval Intelligence, concocted Operation Ruthless. It was a scheme worthy of his postwar spy. The British would outfit a captured German plane with a crew that was to include a "word-perfect German speaker" (Fleming himself, who had studied German in Austria as a youth).[22] After the plane faked a crash into the Channel and its crew was rescued by a German boat, the British would capture the vessel and bring it and its Enigma equipment home to Turing. The escapade was elaborately planned but canceled, and Turing and Twinn went to Birch looking "like undertakers cheated of a nice corpse . . . , all in a stew."[23] Instead, documents and papers—bits and pieces of clues to the contents of the all-important codebooks—were taken from two weather ships captured off Iceland and, in a commando raid organized specifically to help Turing, from an armed German trawler off the Norwegian coast. With these clues, Turing began trying to deduce the contents of the all-important codebooks.

Turing's group was beginning to break the German naval cipher on the glorious day of May 27, 1941, when the British sank the *Bismarck*, then the world's largest battleship. By June Turing had succeeded in reconstructing the codebooks from various clues, and for the first time Bletchley Park could read the messages to and from the U-boat wolf packs within an hour of their arrival. Finally, the British could reroute convoys safely around the subs. For 23 blessed days in June 1941, a time when Britain still fought alone, no convoy in the North Atlantic was attacked.

By then, Bletchley Park regarded Turing fondly as its eccentric genius, although some of his unconventional behavior made practical sense. He wore a gas mask while bicycling to work during the June hay fever season. And he managed his bicycle's broken chain by counting pedal strokes and executing a certain maneuver every 17 revolutions. Bicycle parts were scarce, and he liked identifying repeated patterns in his work.

By autumn of 1941, Banburismus was again in trouble, critically short of typists and junior clerks, otherwise known as "girl power." Turing and three other decoders took a direct but unorthodox approach to the problem. Appealing directly to Churchill on October 21, they wrote, "We despair of any early improvement without your intervention." Welchman probably drafted the letter, but Turing signed it first, followed by Welchman, their colleague Hugh Alexander, and P. Stuart Milner-Barry, a Cambridge mathematics graduate who was the chess correspondent for *The Times* newspaper. Milner-Barry took a train to London, hailed a taxi, and "with a sense of total incredulity (can this really be happening?) invited the taxi driver to take him

to 10 Downing Street." There he persuaded a brigadier general to deliver the letter personally to the prime minister and to stress its urgency.

Churchill, who had visited Bletchley Park, had recently been informed that Britain was running out of food and war supplies. He immediately sent a memorandum to his chief of staff: "Action this day: Make sure they have all they want on extreme priority and report to me that this had been done."[24] Turing and company heard nothing directly in response but noticed that work went more smoothly, bombes were built faster, and staff arrived sooner.

As Bletchley Park was beginning to break naval Enigma, Hitler invaded Russia with two-thirds of his forces in June 1941 and launched a merciless bombardment of Moscow. Early in the campaign, Russia's greatest mathematician, Andrei Kolmogorov, was evacuated east to safety in Kazan along with the rest of the Russian Academy of Sciences. Shortly after, Russia's Artillery Command, reeling from Germany's massive bombing raids, asked Kolmogorov to return to the capital for consultations. Amidst the chaos, he was lodged for awhile on a sofa.

In a country that idolized its intelligentsia, Kolmogorov was a famous man. When a professor's wife heard he was going to visit her home, she began frantically cleaning and cooking. When a maid asked why, the hostess replied, "How can I explain it to you? Just imagine that you will be getting a visit from the tsar himself."[25] Kolmogorov's legend began with his mother, an independent woman of "lofty social ideals" who never married and died in childbirth. Her two sisters raised Andrei, ran a small school for him and his friends, and published a newsletter with little problems he had composed, such as "How many different ways can a button with four holes be sewn?"[26] At the age of 19 at Moscow State University he escaped final examinations in his 14 courses by writing 14 original papers. He was more proud of having taught school to pay his way through the university than of winning any of his awards; late in life he volunteered at a school for gifted children, where he introduced them to literature, music, and nature.

Kolmogorov became the world's authority on probability theory. In 1933 he demonstrated that probability is indeed a branch of mathematics, founded on basic axioms and far removed from its indecorous gambling origins. So fundamental was Kolmogorov's approach that any mathematician, frequentist or Bayesian, could legitimately use probability. Kolmogorov himself espoused the frequentist approach.

Now the generals were asking him about using Bayes against the German barrage. Russia's artillery, like that of the French, had used Bayesian firing tables for years, but the generals were split over an esoteric point about aiming. They asked Kolmogorov his opinion.

"Strictly speaking," he told the generals, starting with Bayes' 50–50 prior odds was "not only arbitrary but surely wrong because it contradicts the main requirements of the probability theory."[27] But with Germany on Moscow's doorstep, Kolmogorov felt he had no choice but to start with equal priors. Agreeing with Joseph Bertrand's strictly reformed version of Bayes, Kolmogorov told the generals they should start with 50–50 odds whenever shooting repeatedly at a small area. Because it was sometimes better to shoot randomly than aim precisely, the guns in a battery of weapons should aim slightly wide of the mark, the way a hunter shooting at moving birds uses pellets for wider dispersion.

That same autumn of 1941, Kolmogorov taught a wartime course at Moscow State University on firing dispersion theory and made the class compulsory for probability majors. Surprisingly, on September 15, 1941, three months into the German invasion of Russia, Kolmogorov submitted his theory of firing to a journal for publication. The article was so mathematical and theoretical that Russia's censors, not realizing it could help the Germans as well as the Russians, allowed it to be printed in 1942. Fortunately, the enemy did not understand the theory any better than the censors did. After the war Kolmogorov published two more practical problems of Bayesean artillery that are still in print—in English—for military authorities to study. Years later a general in the Russian artillery recalled that during the invasion Kolmogorov "did a lot of useful things for us as well, we remember it, and appreciate him too."[28]

Shortly after Germany attacked Russia, British radio listening posts intercepted a new kind of German army message. Analysts at Bletchley Park thought it came from a teletype machine. They were right. The Germans were encrypting and decrypting at the speed of typing. The new Lorenz machines and their family of ultrasecret codes were technically far more sophisticated than the Enigmas, which had been built for commercial use in the 1920s. The supreme command in Berlin relied on its new codes to communicate the highest level of strategy to army group commanders across Europe. The messages were so important that Hitler himself signed some of them.

Code-naming the new Lorenz machines Tunny for "tuna fish," a group of Britain's leading mathematicians began a year of desperate struggle. They

used Bayes' rule, logic, statistics, Boolean algebra, and electronics. They also began work on designing and building the first of ten Colossi, the world's first large-scale digital electronic computers.

When Good and others started work on the Tunny-Lorenz codes, they incorporated Turing's Bayesian scoring system and his fundamental units of bans, decibans, and centibans. They employed Bayes' theorem and a spectrum of priors: honest priors and improper ones; priors that represented what was known and sometimes not; and in different places both Thomas Bayes' uniform priors and Laplace's unequal ones. To deduce the pattern of cams surrounding the wheels of the Tunny-Lorenz machines Turing invented a highly Bayesian method known as Turingery or Turingismus in July 1942. Turingery was a paper-and-pencil method, "more artistic than mathematical. . . . [You had to rely on what] you felt in your bones," according to Turingery player William T. Tutte.[29] The first step was to make a guess and assume, as Bayes had suggested, that it had a 50% chance of being correct. Add more and more clues, some good, some bad, and "with patience, luck, a lot of rubbing out, and a lot of cycling back and forth," the plain text appeared. When the odds of being correct reached 50 to 1, a pair of wheel settings was declared certain.[30]

As Bletchley Park analysts worked on Tunny's wheel patterns and Russia resisted the German onslaught, Japan attacked the United States at Pearl Harbor on December 7, 1941. Supplying Great Britain immediately became more difficult. When American ships that had protected the convoys supplying Britain were quickly transferred to the Pacific, 15 German U-boats took their places in the shipping lanes off the American East Coast. As convoys of Argentine beef and Caribbean oil hugged the coast, they were silhouetted at night against shore lights that local communities dependent on tourism refused to dim. Miami's neon signs, for example, stretched for six deadly miles. The U-boats, lying in wait at periscope depth, caused three months of devastation until the U.S. military ordered coastal lights turned off at dusk.

Making matters worse, the Atlantic U-boats added a fourth wheel to their Enigmas, and the Turing-Welchman bombes were stymied. For most of 1942 Turing and his coworkers could not read any message to or from German submarines. Bletchley Park called it the Great Blackout. For four months the U-boats ran riot in the Atlantic at large, sinking 43 ships in August and September alone. The average U.S. vessel crossed the Atlantic and back three times before it was sunk on its fourth trip.

Finally, in December 1942, three young British crewmen, Lt. Anthony Fasson, Able-Seaman Colin Grazier, and Tommy Brown, swam from their ship to a sinking German submarine off Egypt to pinch its vital codebook of encrypting tables. Fasson and Grazier drowned in the attempt, but Brown, a 16-year-old canteen assistant, survived to rescue the tables. At last Banburismus was fully operational. Within hours of Bletchley Park's receiving the tables, U-boat messages from the Atlantic were being decrypted and convoys rerouted.

The month before that happened, however, would be the war's most dangerous month for Allied shipping, and during it Turing sailed for the United States on the *Queen Elizabeth*, a fast ship that traveled without convoy. Clearance from the White House made Turing a liaison between Bletchley Park and the U.S. Navy. The British had been teaching the Americans about Enigma in general before Pearl Harbor. Now Turing was to tell U.S. officials everything that had been learned, and the United States would accelerate the production of bombes. Surprisingly, the British planned his trip rather haphazardly. He arrived with inadequate identification, and U.S. immigration authorities almost confined him to Ellis Island. In addition, he had not been told whether he could discuss Tunny code breaking with Americans, and the Americans did not realize he expected to have full access to their voice-scrambling research. Nevertheless, during his stay he held high-level meetings in Dayton, Ohio, Washington, and New York City.

Turing spent at least one afternoon in Dayton, where the National Cash Register Company planned to manufacture 336 bombes. He was dismayed to discover that the U.S. Navy was ignoring Banburismus and its ability to economize on bombe usage. The Americans seemed uninterested in the Enigma outside of their obligation to supply bombes for it.

In Washington, Turing discussed Bletchley Park's methods and bombes with U.S. Navy cryptographers. According to a previous agreement, the United States was concentrating on Japanese navy codes and ciphers while the British worked on Enigma. Bletchley Park had already sent a detailed technical report of its work to the Americans, but a civilian navy cryptographer, Agnes Meyer Driscoll, had sat on it; she had broken many Japanese codes and ciphers before the war and had her own, mistaken notions about how to solve Germany's naval Enigma. Turing's mathematics may also have been too technical for the Americans. At first he was alarmed that no one seemed to be working mathematically "with pencil and paper," and he tried

in vain to explain the general principle that confirming inferences suggested by a hypothesis would make the hypothesis itself more probable." Later, he was relieved to meet American mathematicians involved in cryptography.

From Washington, Turing went to the Bell Laboratory in New York City, where he and Claude Shannon met regularly at afternoon tea. Shannon, like Turing and Kolmogorov, was a great mathematician and an original thinker, and he was using Bayes' rule for wartime projects. But Turing and Shannon had more than Bayes in common. Both were shy, unconventional men with deep interests in cryptography and machines that could think. As young men, both had written seminal works combining machines and mathematics. In his master's thesis in mathematics, written at the University of Michigan, Shannon showed that Molina's relay circuits could be analyzed using Boolean algebra. Both Turing and Shannon liked cycling. Turing rode a bicycle for transportation and exercise; Shannon avoided social chitchat by riding a unicycle through Bell Labs' hallways, sometimes juggling balls along the way. Both men liked to design equipment, in Shannon's case whimsical machines like a robotic mouse to solve mazes or a computer for Roman numerals. His garage was filled with chess-playing machines. Unlike Turing, though, Shannon had a warm family life. His father was a businessman, his mother a high school principal, and his sister a mathematics professor, and he and his wife had three children.

When Turing visited Bell Labs, the next cryptographic frontier was speech. Britain and the United States wanted their best people, Shannon and Turing, working on it. Shannon was already developing the SigSaly voice scrambler; it had a nonsense nursery-rhyme name but by war's end Franklin D. Roosevelt, Churchill, and their top generals in eight locations around the world could talk together in total secrecy. With naval Enigma reduced to a largely administrative problem, Turing would tackle voice communications when he returned to Britain. When Turing and Shannon met for tea, they probably discussed the SigSaly.

Shannon was also working on a theory of communication and information and its application to cryptography. In a brilliant insight Shannon realized that noisy telephone lines and coded messages could be analyzed by the same mathematics. One problem complemented the other; the purpose of information is to reduce uncertainty while the purpose of encryption is to increase it. Shannon was using Bayesian approaches for both. He said, "Bell Labs were working on secrecy systems. I'd work on communications systems and I was appointed to some of the committees studying cryptanalytic techniques. The work on both the mathematical theory of communications and the cryptography went forward concurrently from about 1941. I worked on both of them together and I had some of the ideas while working on the other. I wouldn't say that one came before the other—they were so close together you couldn't separate them."[32]

Shannon's efforts united telegraph, telephone, radio, and television communication into one mathematical theory of information. Roughly speaking, if the posterior in a Bayesian equation is quite different from the prior, something has been learned; but when a posterior is basically the same as the prior guess, the information content is low.

Communication and cryptography were in this sense the reverse of one another. Shannon called his logarithmic units for measuring information binary dibits, or bits, a word suggested by John W. Tukey of Bell Labs and Princeton University. In a confidential report published in 1949 Shannon used Bayes' theorem and Kolmogorov's theory of probability from 1933 to show that, in a perfectly secret system, nothing is learned because the prior and posterior of Bayes' theorem are equal. Bell Labs communications theorists were still developing extensions of Shannon's theory and using Bayesian techniques extensively in 2007.

Returning home, Turing boarded the *Empress of Scotland* in New York City on March 23, 1943. New York was the world's greatest port during the war: more than 50 vessels streamed in and out of the city's harbors each day. Turing was traveling during what would be the second most dangerous month of the war for Allied shipping. The U-boat offensive reached its peak that month and would sink 108 Allied ships while losing only 14 subs. Germany had broken the convoys' routing cipher, and the U-boats' four-wheel Enigmas still had Bletchley Park's cryptographers stymied. Approximately 1,350 mostly unarmed merchant ships were at sea every day that spring. They joined a long coastal shipping line that stretched from Brazil to the mouth of the St. Lawrence River, where they formed convoys to cross the Atlantic. Allied escort vessels concentrated on protecting convoys carrying troops to Britain for an invasion of Europe, however, so Turing's ship was one of 120 fast-moving ships that traveled unescorted. Speed was no guarantee of safety, though; the week before, U-boats had sunk the *Empress of Scotland*'s sister ship. Despite the Enigma blackout, Turing made it back to England without incident.

Clearly, the Allies had to locate and destroy the U-boats, not just evade them. U-boats were tying up thousands of Allied ships, planes, and troops needed to

supply Britain and invade Continental Europe. The hunt for U-boats involved Bayes' rule in still another part of the Battle of the Atlantic.

Applying scientific techniques to the antisubmarine campaign, the British Air Ministry organized a small group of scientists to improve its operational efficiency. This was a new idea, and the British called it O.R., for operational or operations research. Its statistics were fairly elementary but imbued with Bayesian ideas.

O.R. concentrated on boosting the efficiency of torpedo attacks, airplane navigation, and formation flying by squadrons of planes searching for U-boats. Bayes' "a priori Method" played "quite a large role in operational research," especially when comparatively few variables were involved, reported O.R.'s chief, the future developmental biologist Conrad H. Waddington.[33]

Typically, O.R. employed Bayes for small, detailed parts of big problems, such as the number of aircraft needed to protect a convoy, the length of crews' operational tours, and whether an aircraft patrol should deviate from its regular flight pattern. Observing the success of British O.R., Adm. Ernest King, commander in chief of the U.S. Fleet, assigned 40 civilian physicists, chemists, mathematicians, and actuaries to his staff. This Anti-Submarine Warfare Operations Research Group was headed by physicist Philip M. Morse of MIT and chemist George E. Kimball of Columbia University.

The Allies had built a string of high-frequency direction-finding stations along the perimeter of the Atlantic. Much of the system was devoted to capturing encoded radio messages and relaying them to code breakers in the United States and at Bletchley Park. With six or seven listening posts intercepting the same message from a particular U-boat, the position of a submarine in the Atlantic could be determined within about 10,000 square miles. This gave patrol planes a good idea of where to look, but 10,000 square miles still meant a circle some 236 miles across. The Allies needed an efficient method for narrowing the search.

Since almost every aspect of searching for targets in the open seas involves uncertainties and probabilities, mathematician Bernard Osgood Koopman of Columbia University was assigned the job of finding a workable method. After graduating from Harvard in 1922, Koopman had studied probability in Paris and earned a Ph.D. from Columbia. His dream was to bridge the gap between Bayes' "intuitive probability . . . of a subjective nature" and the "purely objective" frequency-based probability used in quantum physics and statistical mechanics.[34]

A crusty man with a rough frankness and a pungent wit, Koopman saw

no reason to be bashful about Bayes or Bayesian priors. He assumed from the very beginning that he was dealing with probabilities: "Every operation involved in search is beset with uncertainties; it can be understood quantitatively only in terms of . . . probability. This may now be regarded as a truism; but it seems to have taken the developments in operational research of the Second World War to drive home its practical implications."[35]

Searching for a U-boat at sea, Koopman first asked what its heading was likely to be. To him, this was a classic Bayesian "probability of causes" problem. Priors would obviously be needed. "No rational prospector would search a region for mineral deposits unless a geological study, or the experience of previous prospectors, showed a sufficiently high probability of their presence," he commented. "Police will patrol localities of high incidence of crime. Public health officials will have ideas in advance of the likely sources of infection and will examine them first."[36]

Koopman started right off by assigning Thomas Bayes' 50–50 odds to the presence of a target U-boat inside the 236-mile circle. Then he added data that were as objective as possible, as Jeffreys advised. Unlike Turing, Koopman had access to enormous amounts of detailed information that the military had accumulated about U-boat warfare.

Unfortunately, a U-boat could spot a destroyer long before the destroyer's sonar picked up the U-boat. Many U.S. planes were not equipped with windshield wipers, and crews peered through scratched and soiled windows. "The need for keeping the windows clean and clear cannot be overemphasized," Koopman admonished. If a crew was lucky enough to get binoculars, they were standard navy 7 x 50 issue, hazy at best. Unless crew members changed stations frequently to minimize the monotony, they lost focus. And the best angle for watching was generally 3 or 4 degrees below the horizon—"a rough and ready rule for finding this locus," Koopman wrote, "is to extend the fist at arm's length and look about two or three fingers below the horizon."[37] He figured that most aircraft crews were only a quarter as efficient as lookouts working under laboratory conditions.

As a practical problem, Koopman asked how a naval officer could find a U-boat within a 118-mile radius if he had 4 planes, each of which could fly 5 hours at 130 knots up and down 5 search lanes, each 5 miles wide. Although few O.R. investigations required such intricate mathematics, Koopman found a way to answer the question mathematically using logarithmic functions. Knowing only that 3 of the 5 lanes had a 10% probability of success, another had 30%, and a fourth had 40%, Koopman could do the Bayesian math. The

officer should assign two planes each to the 40% lane and the 30% lane and none to the least probable areas. He calculated this by hand; his problem was not calculating but getting appropriate observational data. He later said that computers would have been irrelevant.

Applying his theories, Koopman wrote a fat manual of precomputed recipes for conducting a U-boat search. The effort needed for each subsection of the search area equaled the logarithm of the probability at that point. The regions to be searched did not have to be boxes or circles; they could have squiggly, irregular shapes. But using his formulas, he could tell a commander how many hours of search to devote to each squiggly region.

Using Koopman's cookbook, a shipboard officer could lay out the optimal way to search given his limited resources: the expected time needed to find the target; the boundaries beyond which he should not venture; and what he should do every two hours until either the U-boat was found or the search was called off. He could plan an eight-hour day, starting off with an optimum search for the first four hours; then, if a U-boat had not been found, the commander could use Bayes' rule to update the target's probable location and launch a new plan every two hours to maximize his chance of locating it.

All of the commander's planning for two-hour sequential searches could be done ahead of time in his stateroom. Koopman called it a "continuous distribution of effort." His U-boat sea searches were theoretically similar to Kolmogorov's artillery problem. Koopman was searching for an unknown U-boat and needed to spread the search effort over an area in an optimal way, just as Kolmogorov figured the optimal amount of dispersion in order to destroy a German cannon. Minesweepers, who worked with similar problems, adopted Koopman's techniques.

Three crucial turning points—two of them top secret—occurred in the European war during 1943. First, in what the Russians still call the Great Patriotic War, the Soviets defeated the Germans on the Eastern Front, at a cost of more than 27 million lives. Second, the tide began to turn against the Germans' U-boats; they sank a quarter million tons in May but 41 subs were lost. Third, Bletchley Park became a giant factory employing almost 9,000 people. As more bombes came online, the laborious Banburismus cardboards were phased out. Barring unforeseen changes by German cryptographers, decoding naval Enigma was under control.

Back home safely and free of responsibility for the Enigma and Tunny-

Lorenz codes, Turing, the great theoretician, was free to dream. During long walks in the countryside around Bletchley Park, Turing and Good discussed machines that could think with Donald Michie, who would pioneer artificial intelligence. Michie, who had joined Bletchley Park as an 18-year-old, described the trio as "an intellectual cabal with a shared obsession with thinking machines and particularly with machine learning as the only credible road to achieving such machines." They talked about "various approaches, conjectures, and arguments concerning what today we call AI."[38]

Max Newman, formerly Turing's mathematics instructor at Cambridge, wanted to automate the British attack on Tunny-Lorenz's codes, and he, Michie, and Good were already working on new machines to do it. Michie had refined Turingismus, but it soon became obvious that mechanical switches would be far too slow. The process would have to be electronic; engineer Thomas H. Flowers suggested using glass vacuum tubes because they could switch current on and off much faster. With backing from Newman, Flowers built the first Colossus at the Post Office Research Station, which ran Britain's telephone system. Installed at Bletchley Park, Colossus decrypted its first message on February 5, 1944. Flowers's car broke down that day but not his Colossus.

Flowers had strict orders—no reasons given—to get a second, more advanced Colossus model operational no later than June 1. Working until they thought their eyes were dropping out, Flowers and his team had Colossus II ready on schedule.

Almost as soon as it began operating, Hitler teletyped an encrypted message to his commanding officer in Normandy, Field Marshal Erwin Rommel. He ordered Rommel not to move his troops for five days after any invasion of Normandy. Hitler had decided it would be a diversionary feint to draw German troops away from the ports along the English Channel and that the real invasion would take place five days later. Colossus II decoded the message, and a courier raced a copy from Bletchley Park to Gen. Dwight "Ike" Eisenhower. As Ike and his staff were trying to decide when to launch the invasion of Normandy the courier handed him a sheet of paper containing Hitler's order. Unable to tell his staff about Bletchley Park, Eisenhower simply returned the paper to the courier and announced, "We go tomorrow," the morning of June 6.[39] He later estimated that Bletchley Park's decoders had shortened the war in Europe by at least two years.

The Colossi became the world's first large-scale electronic digital computers, built for a special purpose but capable of making other computations

too. Flowers would build ten more models during the war. With the Germans introducing complexities that made manual decrypting methods useless, the Colossi replaced Turing's pencil-and-paper Turingery in August 1944. As Michie reported, Turing's Bayesian scoring system based on bans had started "first as a minor mental aid in a variety of jobs" but then turned into "a major aid in the [Colossi's] wheel pattern breaking."[40] Turing's method also contributed intellectually to the use of the Colossi and produced procedures that made the machines much more effective. Each new Colossus was an improvement over the previous one, and Michie believed the eleventh "nudged the design further in the direction of 'programmability' in the modern sense."[41]

By 1945 Turing had moved on to voice encryption at a nearby military installation at Hanslope Park. Late in the war, others at Bletchley Park, ignorant of Turing's work on Enigma, decided to use Bayesian methods to try to break the Japanese naval codes in the Pacific. Japan's main naval cipher, JN-25, was becoming increasingly complex, and Bletchley Park began working on some particularly difficult versions shortly after September 1943.

A trio of British mathematicians was assigned to work in tandem with Washington. The three were Ian Cassels, later a professor at Cambridge; Jimmy Whitworth; and Edward Simpson, who had joined Bletchley Park in 1942, immediately after earning a mathematics degree at Queen's University, Belfast, at the age of 19. Simpson had been working on Italian codes at Bletchley Park, but after Italy's surrender he was switched to JN-25.

"The unbelievably tight security ethos" at Bletchley Park prevented the group from getting advice from Turing or Good, Simpson explained in 2009 after his wartime work was revealed.[42] As a result, the men adopted and developed Bayes on their own. It was a full year before they were able to speak with Turing's colleague Alexander, who by that time had begun work on Japanese naval codes too.

Japanese coding clerks who used the principal code, JN-25, transmitted their messages in blocks of five digits. The British mathematicians knew that each block was the result of adding a random five-digit group, called an additive, to a five-digit code group taken from the JN-25 codebook. In effect, British cryptanalysts had to perform the reverse operation—but without the JN code and additive books. First, they identified groups that might be additives. Then a team composed of civilians and Wrens who, despite being newcomers to cryptography, had to identify the most probable additives rapidly, objectively, and in a standardized manner. They could judge the plausibility of an additive according to the plausibility or probability of the deciphered code group produced by the additive. As a measure of their belief, team members assigned a Bayesian probability to each speculative code group according to how often it had occurred in already deciphered messages. The most probable blocks, as well as borderline or especially important cases, were studied further.

"For practical purposes, it was not necessary to agonise over the prior odds to be assigned to the hypothesis that an additive was true," Simpson explained. "Instead, the essential judgment to be made was whether the [weight of] collective evidence . . . was sufficiently convincing for it to be accepted as genuine . . . As always in cryptanalysis, the inspired hunch grounded in experience could sometimes make the most important contribution of all."[43]

After October 1944 Alexander, Bletchley Park's finest Banburismus solver, developed an elaborate use of Bayes' theorem and Turing's decibans for the Japanese codes.

By 1945 U.S. cryptanalysts were writing memos to one another about Bayes' theorem. Whether the Americans learned about Bayes from Bletchley Park or discovered its usefulness on their own is not known; 65 years after the war, the British government still refuses to declassify many documents about wartime cryptography. A young American mathematician, Andrew Gleason, who was working on Japanese naval codes and who looked after Turing during his stay in Washington, almost certainly knew about Bayes during the war. He, Good, and Alexander continued to work on top-secret cryptography for decades after the war. Gleason helped establish a postwar curriculum for training cryptanalysts at the U.S. National Security Agency (NSA), taught mathematics at Harvard and NSA, and published a probability textbook that instructed a generation of NSA's cryptanalysts in how to use Bayes' theorem, Turing's decibans and centibans, Bayesian inference, and hypothesis testing. Some 20 of his students became leaders in Soviet code breaking during the 1960s and 1970s. Gleason was deeply knowledgeable but pragmatic about Bayes; his textbook also discussed methods developed by Neyman, the arch anti-Bayesian.

A few days after Germany's surrender in May 1945 Churchill made a surprising and shocking move. He ordered the destruction of all evidence that decoding had helped win the Second World War. The fact that cryptography, Bletchley Park, Turing, Bayes' rule, and the Colossi had contributed to victory was to be destroyed. Turing's assistant Good complained later that everything

about decryption and the U-boat fight "from Hollerith [punch] cards to sequential statistics, to empirical Bayes, to Markov chains, to decision theory, to electronic computers" was to remain ultraclassified.[44] Most of the Colossi were dismantled and broken into unidentifiable pieces. Those who built the Colossi and broke Tunny were gagged by Britain's Official Secrets Acts and the Cold War; they could not even say that the Colossi had existed. Books by British and U.S. participants in the U-boat war were almost immediately classified, confined to high-level military circles, and not published for years or in some cases decades. Even classified histories of the war excluded the decryption campaign against the U-boats. Only after 1973 did the story of Bayes, Bletchley Park, and Turing's nation-saving efforts begin to emerge.

Why was the story concealed for so long? The answer seems to be that the British did not want the Soviet government to know they could decrypt Tunny-Lorenz codes. The Russians had captured a number of Lorenz machines, and Britain used at least one of the two surviving Colossi to break Soviet codes during the Cold War. Only when the Soviets replaced their Lorenz machines with new cryptosystems was Bletchley Park's story revealed.

The secrecy had tragic consequences. Family and friends of Bletchley Park employees went to their graves without ever knowing the contributions their loved ones had made during the war. Those connected with Colossus, the epitome of the British decryption effort, received little or no credit. Turing was given an Order of the British Empire (OBE), a routine award given to high civil servants. Newman was so angry at the government's "derisory" lack of gratitude to Turing that he refused his own OBE.

Britain's science, technology, and economy were losers, too. The Colossi were built and operational years before the ENIAC in Pennsylvania and before John von Neumann's computer at the Institute for Advance Study in Princeton, but for the next half century the world assumed that U.S. computers had come first.

Obliterating all information about the decryption campaign distorted Cold War attitudes about the value of cryptanalysis and about antisubmarine warfare. The war replaced human spies with machines. Decryption was faster than spying and provided unfiltered knowledge of the enemy's thinking in real time, yet the Cold War glamorized military hardware and the derring-do of spydom.

The secrecy also had a catastrophic effect on Turing. At the end of the war he said he wanted "to build a brain."[45] To do so, he turned down a lectureship at Cambridge University and joined the National Physical Laboratory

in London. Because of the Official Secrets Act he arrived as a nobody. Had he been knighted or otherwise honored he would surely have found it easier to get more than two engineers as support staff. Ignorant of Turing's achievements, the director of the laboratory, Charles Galton Darwin, a grandson of Charles Darwin, repeatedly reprimanded Turing for morning tardiness after working late the night before. Once an afternoon committee meeting with Darwin and others stretched late in the day. At 5:30 p.m. Turing promptly stood up and announced to Darwin that he was leaving—"punctually."[46]

At the laboratory, Turing designed the first relatively complete electronic stored-program digital computer for code breaking in 1945. Darwin deemed it too ambitious, however, and after several years Turing left in disgust. When the laboratory finally built his design in 1950, it was the fastest computer in the world and, astonishingly, had the memory capacity of an early Macintosh built three decades later.

Turing moved to the University of Manchester, where Newman was building the first electronic, stored-program digital computer for Britain's atomic bomb. Working in Manchester, Turing pioneered the first computer software, gave the first lecture on computer intelligence, and devised his famous Turing Test: a computer is thinking if, after five minutes of questioning, a person cannot distinguish its responses from those of a human in the next room. Later, Turing became interested in physical chemistry and how huge biological molecules construct themselves into symmetrical shapes.

A series of spectacular international events in 1949 and 1950 intruded on these productive years and precipitated a personal crisis for Turing: the Soviets surprised the West by detonating an atomic bomb; Communists gained control of mainland China; Alger Hiss, Klaus Fuchs, and Julius and Ethel Rosenberg were arrested for spying; and Sen. Joseph McCarthy of Wisconsin began brandishing his unsubstantiated list of so-called Communists in the U.S. State Department.

Even worse, two upper-crust English spies—an openly promiscuous and alcoholic homosexual named Guy Burgess and his friend from Cambridge student days Donald Maclean—evaded arrest by fleeing to the USSR in 1950. The United States told British intelligence they had been tipped off by Anthony Blunt, another homosexual graduate of Cambridge, a leading art historian, and the queen's surveyor of paintings. With both the British and American governments panicked by visions of a homosexual spy scandal, the number of men arrested for homosexuality in Britain spiked.

On the first day of Queen Elizabeth II's reign, February 7, 1952, Turing

was arrested for homosexual activity conducted in the privacy of his home with a consenting adult. As Good protested later, "Fortunately, the authorities at Bletchley Park had no idea Turing was a homosexual; otherwise we might have lost the war."[47]

In the uproar over Burgess and Maclean, Turing was viewed not as the hero of his country but as yet another Cambridge homosexual privy to the most closely guarded state secrets. He had even worked on the computer involved in Britain's atomic bomb test. As a result of his arrest, Britain's leading cryptanalyst lost his security clearance and any chance to continue work on decoding. In addition, because the U.S. Congress had just banned gays from entering the country, he was unable to get a visa to travel or work in the United States.

As the world lionized the Manhattan Project physicists who engineered the atomic and hydrogen bombs, as Nazi war criminals went free, and as the United States recruited German rocket experts, Turing was found guilty. Less than a decade after England fought a war against Nazis who had conducted medical experiments on their prisoners, an English judge forced Turing to choose between prison and chemical castration. He chose the estrogen injections. Over the next year he grew breasts. And on June 7, 1954, the day after the tenth anniversary of the Normandy invasion he helped make possible, Alan Turing committed suicide. Two years later the British government knighted Anthony Blunt, the spy who later admitted tipping off his friends Burgess and Maclean and precipitating the witch hunt against homosexuals. Even today, it is difficult to write—or read—about Turing's end. In 2009, 55 years after Turing's death, a British prime minister, Gordon Brown, finally apologized.

Turing's Bayesian work lived on in cryptography. Secretly for decades, an American colleague of Turing's taught Bayes to NSA cryptographers. With Turing's blessing, Good developed Bayesian methods and theory and became one of the world's leading cryptanalysts and one of the three leaders in the Bayesian renaissance of the 1950s and 1960s. He wrote roughly 900 articles about Bayes' rule and published most of them.

Outside of cryptography, however, no one knew that some of the most brilliant thinkers of the mid-twentieth century had used Bayes to defend their countries during the Second World War. It emerged from the war as vilified as ever.

5.

dead and buried again

With its wartime successes classified, Bayes' rule emerged from the Second World War even more suspect than before. Statistics books and papers stressed repeatedly and self-righteously that they did not use the rule. When Jack Good discussed the method at the Royal Statistical Society, the next speaker's opening words were, "After that nonsense . . ."[1]

"Bayes" still meant equal priors and did not yet mean making inferences, conclusions, or predictions based on updating observational data. The National Bureau of Standards suppressed a report to Aberdeen Proving Ground, the U.S. Army's weapons-testing center, during the 1950s because the study used subjective Bayesian methods. During Sen. Joseph McCarthy's campaign against Communists, a bureau statistician half-jokingly called a colleague "un-American because [he] was Bayesian, and . . . undermining the United States Government."[2] Professors at Harvard Business School called their Bayesian colleagues "socialists and so-called scientists."[3]

"There still seems to remain in some quarters a lingering idea that there is something 'not quite nice,' something unsound, about the whole concept of inverse probability," a prominent statistician wrote.[4] Unless declared otherwise, a statistician was considered a frequentist.

The Bayesian community was small and isolated, and its publications were well-nigh invisible. Prewar theory by Frank Ramsey, Harold Jeffreys, and Bruno de Finetti lay unread. Nearly all the papers published in the *Annals of Mathematical Statistics* concerned issues framed by Jerzy Neyman's frequentist work from the 1930s. Thanks to Ronald Fisher's genetics research and the powerful anti-Bayesian stance of an Iowa State University statistician named