UNCLASSIFIED

Cryptologic Almanac 50th Anniversary Series The World at the End of the War

More than 50 years after, the Second World War retains its hold over our imaginations. Military operations were conceived and carried out on a scale unimaginable in earlier times. The number of casualties among both combatants and civilians was far higher than ever before in history.

The unconditional surrender of the Axis powers in mid-1945 brought an end to the fighting, but the problems of peace were more difficult to comprehend and solve than previously imagined. Both sides, victor and vanquished alike, had suffered destruction, death, dislocation, the loss of national cultures, and the breakdown of national and international political life.

Soon enough, to make things worse, the world would divide along ideological lines as the wartime Allies fell out.

Wartime cryptanalysis in retrospect also seems legendary, but the truth is spectacular. Great Britain and the United States cooperated in exploiting a very large number of high- and low-level cryptographic systems used by the Axis. The ability to read the enemy's messages shortened the war by perhaps as much as two years and saved tens of thousands of Allied lives.

Both sides had developed intricate machine systems for protection of their communications. Germany, Great Britain, and the United States all deployed powerful cryptomachines. The Allies were able to exploit Germany's cryptographic machines, however, because they also developed highly sophisticated machine cryptanalytic techniques.

Victory at the end of World War II caused unforeseen and ironic problems for America's cryptologic agencies also, as we shall see.

WORLD SITUATION

With VJ Day, August 15, 1945, the Allies achieved full victory -- and near total destruction -- over the Axis nations.

Approved for Release by NSA on 06-12-2009, FOIA Case # 52567

Italy, Germany, and Japan had suffered significant destruction. All were occupied by Allied armies, and, in the case of Germany, the country had been divided into four zones of occupation. Two Japanese cities had been obliterated in the world's first use of atomic weapons.

The Big Three -- Great Britain, the United States, and the Union of Soviet Socialist Republics -- whose forces had borne the brunt of the fighting and whose policies had determined much of the course of the war, changed as they shifted from war to peace.

In the United States, Franklin D. Roosevelt, who had been elected to an unprecedented four terms as president, died unexpectedly in April 1945. Harry Truman, his vice president, was little known to the American public, and many were apprehensive about his ability to meet the demands of the office. There was also uncertainty about what role the country should have in world affairs -- before the war, the U.S. had had few permanent international entanglements.

After December 7, 1941, the U.S. had raised the largest military force in its history, well in excess of 16 million men and women under arms. Most draftees, however, considered themselves misplaced civilians in uniform only "for the duration," and expected to be demobilized quickly once the war was over. In addition, President Truman believed the American people wanted him to reduce government spending drastically.

Military or civilian, isolationist or internationalist, all Americans resolved that there be "no more Pearl Harbors!"

Great Britain changed leadership at the very end of the war. In July 1945, the Labor Party won a majority in Parliament, and Clement Atlee replaced Winston Churchill as prime minister. The British public was anxious to concentrate on an urgent domestic agenda after seven years of war.

Josef Stalin in the Soviet Union remained the only principal wartime leader to retain his position into the postwar period. The Soviet people, however, had suffered the highest number of casualties of any country, and, arguably, the devastation in their territory was the worst.

At the end of the war, the Soviet Red Army remained in occupation of half of Germany and much of Eastern Europe.

The U.S. and the U.K., used to dealing with a wartime ally, found in the peacetime Soviet Union, as historian Herbert Feis once remarked, "The difference between the devil sick and the devil well."

CRYPTOLOGIC ORGANIZATIONS

At the end of the war, the U.S. military possessed two agencies for producing COMINT and maintaining COMSEC. The Navy's COMINT service was composed overwhelmingly of uniformed personnel. The Army had a mixture of civilians and active-duty military.

Army COMINT was pro-duced by the Signal Security Agency (SSA), soon to be renamed the Army Security Agency (ASA). SSA had its headquarters at Arlington Hall Station in Virginia, not far from the Pentagon.

Navy COMINT came from the Communications Intelligence Organization (OP-20-G), located at the former Mount Vernon Seminary on Nebraska Avenue in the District of Columbia. In 1946, this organization was redesignated the Communications Supplementary Activ-ity, Washington, or CSAW.

Some cooperation between the two services dated to the prewar period, when both processed Japanese diplomatic messages. Wartime interservice collaboration began in 1944 with an agreement to exchange data and liai-son officers, followed by a purely unofficial, working-level group -- with a rule of unanimity for all formal actions.

Relatively small in prewar days, the Army and the Navy's cryptologic organizations grew to about 10,000 people each by 1945. In the Army particularly, this increase included a very high percentage of women; they saw the sacrifices their male colleagues were making and wanted to make their own contribution to the nation's war effort.

Once Germany surrendered, however, both cryptologic agencies began to reduce the staff that could not be shifted to the Japanese target. The agencies made efforts to place those who wanted to stay in cryptology, but, ultimately, as demobilization proceeded, most wartime hires had to go.

BRUSA

The cryptanalytic work during the world war was a bilateral effort, the American services working with Britain's GC&CS (Government Code and Cipher School). Moreover, the Americans adopted a great deal from the British, including techniques of machine processing and the method for distributing COMINT, the Special Security Officer system.

The close wartime alliance had benefited both nations, extending the reach of each in exploiting the communications of their common enemies. It is unusual for two countries to cooperate closely in such a sensitive enterprise as COMINT. The question had to be faced,

therefore, as to whether the relationship should or would continue, and what form would it take.

TARGETS

Now that the principal enemies of the United States had been defeated, the cryptologic organizations had to address the question of new targets and new priorities.

During the war, particularly in the Army, they had worked the communications of "neutral nations," countries that had diplomatic or economic relations with the Axis. This gave cryptologists a start in determining possibilities for the postwar period, but questions of requirement and priorities would have to be addressed.

The U.S. Navy, which had concentrated on enemy systems during the war, wished to resume work on others in peacetime, so targets would have to be reallocated between the services.

COLLECTION

Prior to and during the war, the United States had established a sophisticated network of listening posts, but the posts were, for the most part, aimed at eavesdropping on Japanese communications. As the war progressed, the U.S. conducted intercept against Germany as well, but, to a large degree, depended on British sources for European collection.

This left the COMINT agencies with many obsolete sites after hostilities ended, and the need for new ones in new locations. Some existing sites could be converted for use against emerging new targets, but these sites simply did not have adequate coverage for the needs of the new era.

MACHINE PROCESSING

One major lesson the cryptologic services learned from the world war was the criticality of advanced machines, for both cryptographic and cryptanalytic purposes. American cryptanalysts adapted a Polish/U.K. device known as the bombe for processing German communications.

The bombe was an electromechanical device of great utility to cryptanalysis, but it was essentially a machine for fast sorting and comparing text. In the last two years of the war, GC&CS cryptanalysts invented COLOSSUS, the next generation of machine processors. It

had many characteristics now associated with computers, including the ability to reprogram electronically.

With the invention of COLOSSUS, it became clear to most in the cryptologic organizations that the need for research, development, and manufacturing would increase in the postwar world. However, they knew that postwar budget cuts meant funding would grow scarcer.

COMMUNICATIONS SECURITY

Just prior to the outbreak of the war, the U.S. Army and Navy, in a possibly unprecedented fit of cooperation, invented the strongest cryptographic machine of the war, known as the SIGABA to the Army and the ECM to the Navy. This machine had kept American high-level communications absolutely secure from enemy exploitation.

However, it was not clear to the military authorities how secure lower-level communications had been.

As they studied the joint service operations of the war, many in command also perceived the need for enhanced interoperability in communications between the services, which meant a companion requirement for interoperability in protecting these communications.

CENTRALIZATION

A few farsighted officers in the cryptologic services realized that the combination of budget reductions and rising cryptologic costs would likely result in pressure from high government officials to centralize and perhaps consolidate operations. Wartime cooperation between the Army and the Navy in cryptologic matters had been slight, and run on a strictly voluntary basis.

In addition, the U.S.-U.K. wartime relationship was unusual in another aspect that would affect postwar relations. The U.S. Army and Navy had each maintained a separate agreement on sharing with the British COMINT organization; personnel made this arrangement work under wartime pressure, but the question of consolidation of international cooperation had to be addressed in peacetime.

In summary, on a national level, the United States had to decide if it wanted the sensitive COMINT relationship with Great Britain to continue, and, if so, what form it should assume. The American cryptologic agencies in 1945 had to address matters of personnel and funding immediately, tough issues further linked to the question of consolidation of

operations. While these were being debated, the agencies also had to solve practical questions in research and development in the strange new field of computers, work with consumers to determine changed priorities, and arrange for collection in new areas of the world.

This was the bright new world of peace.

Horizontal Line

Almanac 50th Anniversary Series

Content Owner: Feedback

Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days