Cena a bordo do *U-507*, que efetuou os primeiros ataques de submarinos alemães na costa brasileira, em agosto de 1942. No convés do submarino, alguns sobreviventes de um navio afundado (não se sabe quando foi batida a foto e se foi feita durante essa operação).

RADIOINFORMAÇÕES E A SUA IMPORTÂNCIA NA SEGUNDA GUERRA MUNDIAL*

JURGEN ROHWER

* Palestra proferida pelo autor no Estado-Maior da Armada, em Brasília, a 1º de abril de 1982.

Eu apreciei muitíssimo a oportunidade que me foi concedida para apresentar-lhes alguns resultados de minha pesquisa sobre a influência que as radioinformações tiveram no decorrer e resultado da Segunda Guerra Mundial.

Em muitas publicações dos últimos anos foi feito um uso pouco cuidadoso dos termos técnicos nos campos das radioinformações e comunicações.

Assim, um grande número de idéias completamente erradas foi desenvolvido sobre as possibilidades e os limites dessas técnicas e suas conseqüências para o transcurso da guerra.

Algumas publicações sugeriram ao público que, com a decifração das mais secretas comunicações alemães e japonesas, os criptoanalistas anglo-saxões podiam penetrar no processo de decisões do Eixo, no mais alto nível, e o Alto Comando Aliado tinha, quase sempre, conhecimento das intenções do inimigo.

Mas — eu penso —, se verdadeiro, isso deveria ter levado a terminar a guerra mais cedo.

Deve-se muito a livros escritos por autores britânicos muito bem informados, como Patrick Beesly, Ronald Lewin, R. V. Jones ou Harry Hinsley, e a algumas outras publicações nos Estados Unidos e Alemanha, que muitas distorções e mal-entendidos tenham sido corrigidos.

Também cerca de uma dúzia de conferências internacionais feitas a partir de 1976 nos Estados Unidos, Grã-Bretanha, República Federal da Alemanha, Canadá, Dinamarca, Suécia e Romênia colaboraram para um melhor entendimento entre os criptologistas, o pessoal de informações, líderes militares e historiadores.

Para se obter um entendimento real da importância dos serviços de informações nos processos de tomada de decisão durante a guerra é necessário ter uma idéia clara de duas coisas.

Primeiramente, sobre os diversos métodos usados pelos diferentes serviços dos beligerantes para suas comunicações e os sistemas criptográficos para fazer estas comunicações com segurança contra serviço de informações do inimigo. E, em segundo lugar, dos métodos técnicos usados pelos criptoanalistas do outro lado e seu relacionamento com seções de informações e os que trabalhavam no processo de tomada de decisão nos vários níveis de comando.

Para transmitir as mensagens, os dois lados usavam, na Segunda Guerra Mundial — à parte os métodos acústico e visual —, principalmente o telégrafo ou telefone, com ou sem fio.

As comunicações por fio — a teleimpressão ou o telefone — estabelecem ligação apenas entre os participantes diretos e não permitem que sejam ouvidos, por acaso, por pessoas não autorizadas.

Assim, esses sistemas de comunicação por fio dão ao seu usuário uma grande segurança.

Mas era impossível usar tal modalidade se um ou ambos participantes estivessem em movimento.

Neste caso era necessário usar a comunicação sem fio, a radiotelegrafia ou o rádio, mas como as ondas de rádio se espalham em todas as direções, estações receptoras sintonizadas na mesma freqüência podem interceptar o tráfego — autorizadas ou não.

Conseqüentemente, na política, diplomacia ou Forças Armadas, em todo o mundo, as mensagens secretas eram transmitidas usando as comunicações com fio quando possível.

Assim, quando os quartéis-generais distribuíam suas ordens para as forças terrestres em posição, para as unidades aéreas antes da decolagem ou navais antes de suspender, usavam as comunicações por fio.

Mas as mensagens-rádio tornavam-se indispensáveis logo que essas unidades estivessem em movimento ou quando não houvesse ligação por fio ou esta tivesse sido destruída.

As comunicações-rádio em VHF-voz podiam ser somente utilizadas por unidades que se encontravam próximas devido ao limitado alcance e conseqüentemente seu emprego se restringia ao nível tático.

Os serviços de radioinformações do inimigo, dessa forma, somente tinham co-

nhecimento das mensagens decifradas trocadas entre os quartéis-generais e os comandos em nível mais elevado.

A principal fonte para os serviços de radioinformações era o tráfego de mensagens no nível operacional entre — digamos — o Quartel-General do Exército e os Comandos de Divisões que se encontravam em movimento ou entre estações terrestres e formações de aeronaves em vôo ou navios e submarinos no mar.

Esta fonte de informações para obter um quadro mais claro da situação do inimigo era acrescentada pelo tráfego-rádio em VHF interceptado, entre os batalhões ou companhias, aeronaves na esquadrilha ou navios numa unidade-tarefa.

Na maioria dos casos não era uma simples mensagem que mostrava a informação importante, mas o oficial podia somente chegar a uma conclusão próxima da verdade coletando, comparando e analisando um grande número de mensagens mais ou menos triviais e montando-as como pedras que formam uma figura de mosaico.

É importante lembrar que isto foi feito não somente pela decifração das mensagens interceptadas.

Em muitas ocasiões, a análise do volume do tráfego e a radiogoniometria foram da mesma importância.

É uma tarefa difícil para o historiador descobrir agora qual das muitas possibilidades de transmissão de uma mensagem e qual dos sistemas ou subsistemas criptográficos foi usado em cada caso especial.

Mas ele também deve verificar as possibilidades do inimigo interceptar a mensagem, usá-la para obter a direção de onde vem a transmissão (radiogoniometria) ou para análise do volume de tráfego ou para criptoanalisar.

Se a criptoanálise era possível, ele deve inquirir sobre o tempo necessário para obter a mensagem decifrada e traduzida, comparar o seu conteúdo com a estimativa da situação do inimigo e então transmitir a nova e importante informação extraída da mensagem do inimigo de forma bastante segura para o comando operacional interessado.

No pouco tempo disponível é impossível entrar em muitos detalhes sobre as técnicas de criptologia e criptoanálise.

Mas tentarei acrescentar à minha descrição do papel das radioinformações na Segunda Guerra Mundial algumas informações gerais sobre os diferentes sistemas criptográficos e suas soluções pelo inimigo.

Para entender as condições reais de trabalho na criptoanálise é necessário fazer-se uma clara distinção entre os diferentes métodos de criptografia.

O mais simples é cifrar a mensagem trocando o texto em linguagem clara por grupo de letras obtidas num dicionário chamado livro-código.

A outra maneira é substituir ou transpor as letras ou números de um texto claro por outras letras dadas numa lista ou tabela de substituição ou de transposição.

A substituição ou a transposição podem ser feitas por métodos manuais ou pelo uso de formulários ou máquinas de cifra.

Vou agora descrever a máquina *Enigma* usada pelos alemães como exemplo de uma das muitas máquinas de cifrar usadas durante a Segunda Guerra Mundial e confrontar esta, mais tarde, com o código combinado manual-máquina de cifrar, usado pela Marinha Inglesa.

Durante os anos 20, um número de inventores desenvolveu máquinas de cifrar com cilindros criptográficos ou rotores e algumas dessas máquinas foram produzidas e vendidas com vários graus de sucesso comercial. Uma delas foi a *Enigma*.

É muito importante saber que esta máquina a que nos referimos não é do tipo idêntico à máquina usada durante toda a guerra para cifrar todas as mensagens dos mais altos níveis de Comando da Alemanha.

Enigma era uma série completa de máquinas de cifra desenvolvida por firmas particulares alemães e construída por mais de 23 anos com algumas modificações de subséries para subséries.

As primeiras versões foram apresentadas em 1939 em exposições e foram vendidas para empresas privadas.

Existiam várias patentes, e cópias alemãs, holandesas e inglesas da série D — como mostrada nesta propaganda — foram vendidas para agências na Polônia, Suécia, Suíça, Grã-Bretanha, Estados Unidos e Japão.

Durante a Guerra Civil Espanhola os italianos e os espanhóis de Franco obtiveram também algumas cópias dos referidos modelos.

Em 1926, a Marinha Alemã introduziu uma nova versão desta máquina — a *Funkschlüssel C*.

Como a primeira versão comercial usava quatro rotores com 26 letras cada, a *Funkschlüssel C* tinha somente três diferentes rotores, além de dois outros alternativos, para troca, e cada um tinha 29 letras, incluindo o trema alemão.

Mas este tipo, assim como o similar *Enigma G,* que foi usado pelo Exército Alemão a partir de 1928, não é considerado suficientemente seguro.

Assim, em 1934, o Exército e a Marinha Alemães trocaram para duas novas versões de *Enigma.*

Esta máquina tinha três rotores internos e dois rotores adicionais intercambiáveis.

Para evitar os mal-entendidos que resultaram do uso do trema, o número de letras foi novamente reduzido a 26.

Mas em acréscimo a máquina ganhou o *Steckerbsett* ou *Plugboard* (quadro de ligações) para um total de 13 conexões entre as 26 letras do alfabeto.

Inicialmente, o Exército utilizou somente os rotores 1 a 3, que podiam ser trocados nas posições, dando seis possíveis posições de rotores.

Os três rotores internos permitiam, cada qual com suas 26 letras, 16 900 permutações possíveis de serem ajustadas na unidade de cifras.

Além dessas ajustagens internas, o operador devia fazer outras duas:

Primeiro, as conexões de tomadas, que dão cerca de 1 500 possibilidades, e depois a posição inicial dos rotores, novamente com 17 567 possibilidades.

Multiplicando-se todos esses fatores pode-se entender por que os alemães pensaram que a máquina era suficientemente segura para evitar uma quebra de sigilo por criptoanalistas inimigos em um tempo razoável.

Para assegurar-se de que não haveria quebra de cifra, se o inimigo fosse capaz de capturar uma máquina, foram tomadas algumas medidas adicionais para evitar o uso repetido do mesmo símbolo em mensagens diferentes.

Chaves de cifras separadas eram usadas para cada mensagem e todas as mensagens com mais de 100 letras deviam ser partidas em duas diferentes mensagens.

Mas não sabíamos que exatamente esta medida seria o ponto fraco do sistema *Enigma* alemão.

O Biuro Szyfrow da Polônia tomou conhecimento, em 1928, do emprego de máquinas de cifrar nas Forças Armadas da Alemanha.

Alguns jovens matemáticos poloneses, que falavam alemão, foram preparados para ajudar a resolver os problemas das máquinas.

Em 1932 obtiveram sucesso. Através de análises matemáticas puderam reparar a cabeação interna dos primeiros três rotores de cifrar do *Enigma* usados pelo Exército.

O sucesso deveu-se um pouco ao auxílio do *Deuxième Bureau,* que deu algum material para os colegas poloneses, obtido de um traidor alemão.

Os criptoanalistas poloneses conseguiram desenvolver alguns auxílios necessários, eletromecânicos, como o *zyclometer* e o *bomba,* para acelerar o processo de resolver a chave usada na máquina *Enigma.*

Mas, quando, em 1938, os alemães mudaram os seus métodos de cifrar e introduziram no campo de comunicações do Exército dois rotores adicionais, os poloneses conseguiram encontrar soluções teóricas pelo uso de algumas folhas perfuradas, mas foi impossível produzir uma nova máquina eletromecânica que pudesse resolver as 60 diferentes posições do rotor agora existentes, em vez das 6 usadas até então.

Com o perigo de um ataque iminente, a Polônia tentou entrar em contato novamente com os especialistas franceses e agora os britânicos. Em julho de 1939 houve um acordo entre os três grupos para cada um concentrar suas atenções em áreas especiais.

Os especialistas poloneses deviam continuar seu trabalho de análise. Os franceses deviam tentar obter mais informações dos agentes alemães, e os ingleses deviam preparar os meios administrativos e técnicos para a utilização desses sucessos da criptoanálise numa época de grande guerra.

Durante a primeira parte das operações da *Blitzkrieg* da Alemanha na Polônia, Dinamarca, Noruega e França, esta organização inglesa, que foi transferida para Bletchley Park, estava trabalhando duramente para vencer as primeiras dificuldades e não podia obter um grande aumento de informação.

Da mesma forma ocorreu com a Organização Francesa, que incorporou, após a campanha da Polônia, o gabinete * de criptoanálise polonês, que escapou através da Romênia.

Iniciando no final de 1939, obtiveram alguns sucessos na decodificação, mas só após muitas semanas de trabalho e assim não foram de uso real nas operações.

Assim, as agências de informações dos Aliados tiveram de trabalhar com suas fontes convencionais, como as notícias obtidas dos diplomatas e informações enviadas por agentes, reconhecimento aéreo e interrogatório de prisioneiros.

Do lado alemão, durante este tempo, a situação estava um pouco melhor.

As Forças Armadas Alemãs, além de outras agências, já antes da Segunda Guerra Mundial, tinham um grande interesse em criptoanálise e radioinformações.

Especialmente o escritório alemão naval de criptoanálise, o xB-Dienst, era uma organização de grande eficiência, após a Marinha Germânica tomar conhecimento do trabalho bem sucedido do escritório de criptoanálise inglês, a Sala 40 do Almirantado, durante a Primeira Guerra Mundial.

A Marinha Britância usou durante a primeira metade da guerra três principais criptossistemas e alguns outros métodos inferiores.

Estes três sistemas foram baseados numa combinação de código e cifra.

O texto claro era inicialmente cifrado pelo uso de um livro de código de quatro ou cinco letras maiúsculas e então supracifrado pelo uso de uma coluna de dígitos.

Estes sistemas manuais não podiam ser mudados com freqüência por causa de problemas logísticos nos vários locais em que a Marinha tinha que operar.

Mas o grande número de materiais de cifra colocava um grande problema para o esforço de criptoanálise.

Somente após o uso de um sistema durante um período relativamente longo de tempo era possível reconstruir mais e mais partes do livro de código e das colunas de dígitos utilizadas.

Ao lidar com todas as mensagens interceptadas, os criptoanalistas tinham primeiro que achar o ponto de partida das colunas de dígitos por comparação desta com a série conhecida de colunas.

Este sistema foi considerado por um número cada vez maior de oficiais ingleses como desajeitado e ultrapassado, e sabemos que o falecido Lorde Mountbatten já antes da guerra propôs a introdução de uma máquina de cifras na Marinha Inglesa.

Talvez a Marinha da Inglaterra tenha sido feliz por não ter usado estas máquinas.

As mais desenvolvidas máquinas cifrantes eram nesta época o tipo da Real Força Aérea, que tinha alguma relação com as velhas máquinas comerciais *Enigma* ou suas patentes.

Se todo o tráfego de comunicações navais inglês tivesse sido cifrado por uma máquina como esta na sua forma preliminar, os eficientes criptoanalistas da Marinha Alemã podiam ter concentrado seus

---

* Assim denominado um conjunto de analistas.

esforços neste sistema sobre o qual havia algum conhecimento na Alemanha.

Mas o velho sistema manual permaneceu o principal sistema criptográfico operacional da Marinha da Inglaterra e assim os criptoanalistas germânicos tinham de atacar cada mensagem de *per si* e conseqüentemente a quantidade de tráfego decifrado conseguia alcançar algumas vezes 10% do tráfego total, mas somente uma parte podia ser decifrada a tempo para ser usada nas operações.

Mas o serviço xB-Dienst conseguiu obter informações sobre o deslocamento de quase todas as importantes unidades da Marinha Inglesa, utilizando esta fonte em combinação com análise do tráfego-rádio e radiogoniometria, de modo que o Alto Comando alemão tinha uma imagem bastante exata da situação do lado do inimigo durante a primeira parte da guerra.

Quando houve uma mudança do código e cifra, como sucedeu em agosto de 1940, ocorreu uma interrupção do entendimento das mensagens, mas pouco tempo depois o xB-Dienst estava novamente apto a recompor partes do livro-código e das colunas de dígitos.

Era especialmente importante que o xB-Dienst tivesse capacidade para decifrar partes da cifra naval aliada nº 3, usada para atribuir as derrotas ao sistema de comboios.

As agências de radioinformações da Força Aérea da Alemanha, o Exército e o Ministério das Relações Exteriores obtiveram também sucesso com algum dos criptossistemas do inimigo e de neutros.

Em cooperação com o reconhecimento aéreo, as radioinformações do Exército Alemão foram muito importantes durante a campanha da França, porque os criptoanalistas furaram a maior parte dos sistemas do Exército Francês.

Mas a separação em sete diferentes serviços de radioinformações levou a uma grande perda de eficiência do lado alemão, o que foi o mais importante, porque os alemães tinham de trabalhar contra um número muito maior de diferentes criptossistemas.

Bletchley Park, por outro lado, tinha de trabalhar contra um sistema principal — *Enigma* — do lado alemão, que era usado em algumas diferentes versões e com algumas diferenças em suas regras.

Em maio de 1940, os ingleses obtiveram sucesso ao completar a primeira máquina eletromecânica — *Bomba* —, desenvolvida pelo genial matemático Allan Turing.

Com esta *Bomba* foi possível experimentar um grande número de possibilidades de cifras do *Enigma*, num tempo mais reduzido, para obter a chave do dia de um ou mais circuitos de cifras.

Quando a primeira máquina ficou disponível, os ingleses sabiam, pela sua análise de tráfego, que havia um circuito de cifra usado com mais freqüência que outro — era o circuito principal da Força Aérea. A maior parte do tráfego-rádio operacional da Força Aérea estava usando esta cifra.

Logicamente, por sua mobilidade, tinham de usar as comunicações por rádio com muito maior freqüência.

Mas, por outro lado, a Força Aérea usava as radiocomunicações com muito menor cuidado do que o Exército e a Marinha.

Por exemplo, o seu Alto Comando queria obter de seus comandos subordinados relatórios da situação quatro vezes por dia.

Estes relatórios, com seus conteúdos rotineiros, permitiam a Bletchley Park furar as chaves diárias com maior rapidez do que na maioria dos outros circuitos.

Assim, foi possível, iniciando em 22 de maio de 1940, obter a chave diária do circuito de cifra da Força Aérea da Alemanha já umas poucas horas após o início de seu uso e então foi fácil decifrar todas as mensagens que empregaram esta chave.

É importante saber que a maioria das informações de Bletchley Park, até 1942, versando sobre as operações aéreas e sobre o Exército, também resultou de furos dos circuitos de cifras da Força Aérea.

Mas é um grande erro pensar que o Alto Comando Aliado obteve desta fonte de informações todos os detalhes sobre o

planejamento operacional ou estratégico alemão porque, como foi dito, o conteúdo deste tráfego dizia mais respeito a detalhes táticos e logísticos.

Somente a compilação do material deu ao Serviço de Informações Britânico em Bletchley Park um conhecimento muito profundo sobre a ordem de batalha dos alemães e a situação logística e de pessoal das diferentes unidades.

Assim, não foi a decodificação das ordens operativas de Göring ou seus comandantes de unidades aéreas que deram ao Comandante-em-Chefe do Comando de Caça Britânico, Marechal-do-Ar Dowding, as necessárias informações para obter sua vitória na Batalha da Inglaterra.

Foi seu conhecimento da situação das unidades da Força Aérea da Alemanha, em combinação com os resultados do eficiente trabalho das estações de radar na Costa Sul da Inglaterra, que permitiu o uso dos seus aviões de caça da forma mais econômica.

E não foi uma ordem de Hitler para o cancelamento da Operação Sealion que deu a Churchill esta informação, mas um detalhe de uma aparentemente trivial mensagem para a 7ª Divisão Aerotransportada foi a gota d'água que mudou a estimativa que Churchill tinha da situação.

Agora sabemos que sua interpretação estava correta, mas nesta época não era a opinião dos especialistas de informações.

É muito importante para o historiador, hoje, que ele não veja só as decodificações mais importantes nos arquivos.

Ele deve olhar não somente para um, mas para um grande número de mensagens e deve analisá-las no contexto de todas as fontes de informações.

Com grande freqüência, uma nova informação sobre um evento futuro era tão clara para os especialistas ou líderes políticos e militares na época, assim como podemos pensar com novo conhecimento e preocupação de hoje.

Há muitos exemplos para ressaltar este ponto, mas o tempo parece ser muito curto para falarmos, por exemplo, sobre a real estória de Coventry, que sofreu muitas distorções.

No Mediterrâneo, as radioinformações foram de especial importância.

Os britânicos foram capazes de decifrar os códigos e sistemas de cifra dos italianos até a declaração de guerra da Itália.

E os serviços italianos de criptologia também obtiveram sucesso contra alguns dos criptossistemas dos Aliados.

Mas logo após o início da guerra no Mediterrâneo, os italianos mudaram completamente os seus sistemas criptográficos e assim Bletchley Park ficou cego.

As radioinformações tiveram sucesso no teatro do Mediterrâneo durante os primeiros 18 meses da guerra, principalmente pela utilização do tráfego tático.

No início de 1941 apareceu mais uma importante fonte, quando Bletchley Park conseguiu resolver a cifra especial do *Enigma* para as unidades da Força Aérea da Alemanha no Mediterrâneo.

Uma outra importante fonte foi a solução da cifra de *Enigma* para a organização das estradas de ferro germânicas que deu informações sobre o movimento de trens durante as fases de deslocamento antes das operações nos Bálcãs e Leste.

Também foi obtida em Bletchley Park a solução para a cifra da Marinha da Itália, usada por *Enigma,* que foi empregada pelos italianos durante um curto período de tempo na primavera de 1941.

Este resultado e a solução da cifra da Força Aérea da Alemanha no Mediterrâneo levaram os britânicos à vitória no Cabo Matapan.

E todas estas fontes tiveram grande valor na obtenção dos detalhes do planejamento alemão para o ataque aerotransportado contra Creta.

Mas a criptoanálise e as radioinformações sozinhas não eram capazes de ganhar uma única batalha.

Durante a guerra na África do Norte, alguns outros problemas, em conexão com as radioinformações, tiveram de ser aprendidos por ambos os lados.

O Comandante do Africa Corps, General Rommel, tinha de usar comunicações por rádio para conduzir suas tropas

móveis no deserto e manter-se em contacto com seus superiores.

Mas Rommel era um líder muito dinâmico e com grande freqüência não obedecia estritamente as ordens recebidas quando uma situação lhe oferecia chances de sucesso.

Por outro lado, em seus relatórios de situação, ele dava, freqüentemente, notícias pessimistas dos problemas logísticos para obter mais suprimentos da Itália.

Assim, Churchill, com sua experiência em radioinformações da Primeira Guerra Mundial, que queria sempre ver as mensagens originais decifradas, algumas vezes chegava a estimativas erradas de situação no Norte da África e empurrava os seus comandantes que tinham maior conhecimento nas operações que falharam.

Assim, Churchill sacrificou os seus dois Comandantes, Wavell e Auchinleck.

As cautelosas operações de Montgomery, após a Batalha de El Alamein, foram, talvez, uma conseqüência de sua experiência e conduziram à fuga do Exército Germano-Italiano da África.

No Mediterrâneo, teve grande importância a decodificação das mensagens dos italianos e alemães em ligação com o tráfego do abastecimento para a África, de modo que foi possível enviar submarinos, forças de superfície e aéreas para os locais onde os comboios deveriam passar.

As conseqüências das radioinformações na Guerra Rússia—Alemanha não são tão bem conhecidas.

Análise do tráfego-rádio e radiogoniometria, além da decifração das mensagens táticas, foram empregadas por ambos os lados para montar o quadro da ordem de batalha do inimigo.

Do lado alemão a criptoanálise obteve sucesso parcial com os sistemas criptográficos também, mas não se tem conhecimento de como se saíram os soviéticos nesta área.

As estimativas do plano alemão contra a União Soviética foram enviadas para Moscou pelo Governo Britânico, mas sempre para um escritório especial de ligação, sob uma estória-cobertura, porque era receado que a revelação da fonte real de informações conduziria os alemães a saber do furo das cifras em um prazo curto.

Possivelmente, os russos não acreditavam muito nessas informações.

Um resultado desta campanha foi que após o início das operações da *Blitzkrieg* no Leste Europeu houve um grande aumento no tráfego-rádio do Exército Germânico.

Assim, foi possível a Bletchley Park, com a experiência obtida com os outros sistemas *Enigma*, penetrar em alguns dos circuitos do Exército, em setembro de 1941, e decifrar a maior parte de suas mensagens mais regularmente a partir de abril de 1942.

Na Batalha do Atlântico, as radioinformações tiveram as mais importantes conseqüências.

Na primeira parte da guerra o xB-Dienst alemão parece ter obtido maior sucesso que os seus correspondentes britânicos.

Mas quando Bletchley Park não pôde resolver a cifra da Marinha da Alemanha, conhecida como *Schlüssel M*, na primavera de 1941, o Almirantado deu ordem para a Esquadra Inglesa usar todas as possibilidades de capturar materiais dos códigos e cifras alemães.

O problema principal era que a máquina de cifra da Marinha usava 3 rotores, num total de 8 disponíveis, enquanto que o Exército e a Força Aérea tinham apenas 5 à disposição.

Os 3 rotores de cifras adicionais não podiam ser resolvidos com os meios de análise disponíveis e assim era necessário obtê-los por captura.

Em 3 de março isto foi conseguido com sucesso durante o reide a *Lafoten*, e Bletchley Park pôde dar início a um trabalho real na cifra naval *Enigma*.

Mas inicialmente foi uma tarefa que consumiu muito tempo e os resultados vieram tarde demais para serem de utilidade operacional.

Somente quando em 7 e 8 de maio foi possível capturar, durante uma operação especial de um navio de análises meteorológicas, algum importante material das ci-

fras e capturar uma máquina e muitos outros manuais e materiais secretos do *U-110*, foi possível preparar a máquina de decifrar ou *bombas* para as 336 possíveis seqüências do rotor, ao invés das 60 ou 120 usadas até então.

A partir do início de junho de 1941, foi possível entender as mensagens alemãs usando os programas mensais de ajustagem das cifras.

A segunda operação contra um navio de previsão de tempo no final de junho trouxe as ajustagens das cifras necessárias para julho.

Foi então necessário resolver as chaves diárias da cifra *Hydra* por meios analíticos.

Para dar uma impressão geral de como o sistema de derrotas dos comboios aliados e as táticas das "matilhas" * de submarinos alemães estavam operando com seus respectivos métodos de comunicações e que possibilidades ofereciam para as radioinformações do inimigo, ou descrever um modelo geral de operações de ambos os lados.

Começamos com os Aliados:

Como primeira base para o planejamento, o Almirantado em Londres transmitiu uma recomendação de derrota para todos os comandos interessados cerca de 8 dias antes da partida dos comboios de Halifax ou Sidney, no Oeste, e de Liverpool, no Leste.

Era feita uma avaliação da situação do inimigo e considerada a disponibilidade de escoltas aéreas e navais.

Aproximadamente dois ou três dias mais tarde, após coordenação com os outros comandos interessados, a derrota era aprovada e uma mensagem era difundida para todos os comandos participantes.

Enquanto estas instruções podiam ser transmitidas por cabo (fio) ou redes de comunicações semelhantes, uma mensagem de partida teria de ser enviada por rádio na hora da saída do comboio, porque algumas das forças interessadas estavam no mar e tinham de ser informadas.

Mas eram indispensáveis as comunicações por rádio para efetuar a apresentação dos comboios que se integravam, para a substituição dos grupos de escolta local pelos grupos de escolta de oceano, especialmente quando as ordens para mudança da derrota tinham de ser dadas devido ao rumo de um comboio que se incorporava, atrasado pelas condições meteorológicas, e que se aproximava demasiado do rumo original ou porque haviam sido detectados submarinos próximos da derrota prevista.

Este tráfego inevitável abriu algumas possibilidades para o serviço xB-Dienst da Marinha Alemã.

A análise do tráfego de mensagens oferecia bons resultados no que diz respeito à estrutura do tráfego, como, por exemplo, a programação dos comboios podia ser deduzida estudando-se as características das mensagens interceptadas, freqüências escolhidas, endereços etc.

A radiogoniometria oferecia menos possibilidades do lado alemão porque as bases para cruzamento de marcações eram muito pequenas e os comboios muito raramente enviavam mensagens.

As estações de rastreamento da *Luftwaffe*, entretanto, podiam freqüentemente dar indicações das posições dos comboios pela localização dos sinais das aeronaves de escolta.

Para a criptoanálise, o xB-Dienst podia utilizar a grande quantidade de mensagens que eram necessárias para despachar um grande número de comboios no mar ao mesmo tempo.

Era uma excelente fonte de informações.

A Marinha da Inglaterra usava, além dos métodos especiais, três sistemas principais de criptografia, baseados no método de código e cifra combinados.

Dois foram introduzidos já anteriormente à Segunda Guerra Mundial e eram usados para o tráfego operacional.

Por representar sempre um grande problema logístico a mudança dos livros de

* *Wolf-Pack*, no original, grupo de submarinos.

código, estas mudanças só podiam ser feitas a intervalos muito longos.

Assim, o xB-Dienst alemão podia furar cada vez mais os códigos quando estavam sendo utilizados por tempo demasiado longo.

Mas, quando foram mudados, como foi feito em 1º de setembro de 1940, 1º de janeiro de 1942, 4 de maio de 1943 e 10 de junho de 1943, sempre havia uma interrupção para o xB-Dienst e levava algum tempo até que conseguisse furar os novos códigos.

Os grupos-código dos dois sistemas operacionais, chamados *Cologne* e *Munich* pelo xB-Dienst, e da cifra 3 introduzida em 1941 para a orientação do sistema de comboios, denominado *Frankfurt* pelo xB-Dienst, foram supercifrados por uma série de longos dígitos, chamada longos subtraendos pelos ingleses.

As cifras referidas eram trocadas inicialmente a cada dois meses e posteriormente duas vezes por mês.

O problema para os criptoanalistas germânicos era que eles deviam analisar toda mensagem interceptada e assim continuamente, sem interrupção.

Quando os alemães, no fim de um período, tinham resolvido um grande número de códigos de grupos e longas séries de dígitos, como, por exemplo, em agosto de 1940 e fevereiro de 1943, o serviço xB-Dienst, no mínimo, podia solucionar 10% das mensagens que eram interceptadas e somente 10% destas podiam ser decifradas a tempo de serem utilizadas nas operações de guerra.

Assim, é completamente errado dizer que — por exemplo — o xB-Dienst alemão podia ler todas as mensagens de informações de derrotas dos ingleses ou as de situação dos submarinos ao mesmo tempo.

Somente parte deste material chegava ao comando dos submarinos alemães a tempo de ser utilizado nas operações.

Mas, como sempre acontece quando se trata de informações, este registro era de grande importância.

Por exemplo, pode-se ver que o xB-Dienst recompôs a tabela de horários dos comboios aliados no Atlântico Norte em outubro/novembro de 1941 utilizando estes tipos de materiais.

Agora, olhemos o outro lado, o alemão.

A tática do grupo conhecido como "matilha", ou *Wolf-Pack*, foi desenvolvida pelo comandante dos submarinos antes da Segunda Guerra Mundial.

As primeiras operações para experiência desta tática foram já iniciadas no outono de 1939 e as operações reais começaram no verão de 1940.

Estas operações de grupos de submarinos contra os comboios do Atlântico Norte obedeciam ao padrão a seguir descrito.

Aproximadamente 10 ou 15 submarinos, que partiam da Noruega ou bases francesas com intervalos de vários dias, após comunicarem ter ultrapassado a linha Islândia—Ilhas Faröe ou a área a oeste da Baía da Biscaia recebiam ordens para seguir para um ponto posicionado de acordo com um sistema de grades numa área em que o Comando dos submarinos pretendia estabelecer uma linha de patrulha.

Após cinco ou seis dias, quando a maioria dos submarinos havia alcançado a área, era dada a ordem para formação da linha de patrulha.

Esta linha era posicionada de tal maneira que o comboio que era esperado de acordo com o planejamento passaria pela barragem com luz do dia.

Se não fosse obtido contacto com o comboio, a linha de patrulha era movimentada numa "direção de avanço", sendo estabelecido por quantos dias deveria se adiantar. Desta forma, o grupo de submarinos podia se posicionar em relação ao rumo assumido do comboio.

Ao avistar os navios-alvo, o primeiro submarino a obter contato transmitia suas informações e o Comando ordenava a concentração dos submarinos no comboio sob ataque.

Durante a operação, um dos submarinos era empregado para manter o contacto e tinha de enviar mensagens de posição do comboio a cada hora, indicando, por marcações em relação a sua posição

atual, a situação de alvos para os outros submarinos da "matilha".

Após o ataque, o Comando dos submarinos enviaria uma nova mensagem determinando uma mudança de posição para as unidades que ainda dispunham de combustível e torpedos, fazendo retornar os outros à base ou aproximando-os de um submarino de reabastecimento.

O grande tráfego-rádio que esta espécie de operação e controle tático dos grupos de submarinos exigia dos Comandos em terra criava muitas oportunidades para as radioinformações dos Aliados.

Durante todo o período de guerra e especialmente após a expansão da rede de estações de escuta em todo o Atlântico, durante os anos de 1940 e 1941, as análises do tráfego-rádio e a radiogoniometria feita por estações de terra davam, com bastante precisão, informações, a tempo, sobre as posições de cada submarino e indicavam mesmo quando eles haviam estabelecido contacto com os comboios.

Para a comunicação de contactos o submarino usava uma mensagem abreviada que era baseada num livro-código que reduzia todos os termos importantes, posições e outras informações necessárias a uns poucos grupos compostos de quatro letras.

Estes grupos eram então cifrados pela chave diária da máquina *Schlüssel M*.

Estas mensagens abreviadas podiam ser transmitidas em poucos segundos.

Para que todas as outras estações que operavam na mesma freqüência permanecessem em silêncio, cada mensagem abreviada começava com duas letras gregas, *beta-beta,* ou, em inglês, *B-bar*.

Quando os ingleses começaram a operar o radiogoniômetro com válvula de raios catódicos, proposto por Sir Robert Watson Watt, tornou-se possível obter uma posição determinada, por exemplo, a de um submarino enviando uma mensagem de contacto de avistamento de um comboio.

Pela comparação de uma mensagem *B-bar* com o mapa de situação dos comboios, a Sala de Acompanhamento dos Submarinos podia identificar o comboio ameaçado e enviar uma mensagem de alerta mesmo sem conhecer o conteúdo da comunicação do submarino alemão.

Com este método de integração da radiogoniometria e análise do tráfego-rádio, o acompanhamento dos submarinos tinha uma importante fonte de informações que era independente da criptoanálise e que estava disponível durante toda a guerra, especialmente durante a época das grandes batalhas de comboios no Atlântico Norte.

Mas estes métodos de análise do tráfego e radiogoniometria eram não somente de grande importância se usados independentes da criptoanálise, mas foram também de grande utilidade no processo de decifrar as mensagens alemãs, quando as novas *bombas* adaptadas para os rotores de 336 posições entraram em uso.

Como os analistas de tráfego de mensagens conheciam a composição normal de uma mensagem de contacto e podiam estimar de seu próprio mapa de situação o conteúdo destas mensagens, podiam alimentar as *bombas* com um texto em linguagem clara e o mesmo texto cifrado.

Mudando as datas e os termos do texto, era, algumas vezes, possível chegar ao texto em linguagem clara com mais rapidez do que seria possível sem esta técnica.

Quando era possível decifrar uma mensagem, então o criptoanalista tinha a solução para a chave diária e era mais fácil decifrar todas as mensagens interceptadas, da mesma cifra e do mesmo dia, em poucas horas.

Como a tática de "matilha" dos submarinos para atacar os comboios dependia muito das radiocomunicações com a utilização destas técnicas, com tão grande eficiência, pela Sala de Acompanhamento de Submarinos, muitos comboios foram salvos de pesadas perdas e desviados totalmente dos grupos atacantes.

Para avaliar as conseqüências reais do processo de decifrar as mensagens é necessário estabelecer as diferenças entre cada ação, como pode ser mostrado com o uso do gráfico.

No lado esquerdo estão as datas e em cima as horas e pode-se entender, por exemplo, que era possível decifrar todas as mensagens-rádio dos alemães na cifra *Hydra,* de 27 de agosto, no dia seguinte, de 14:05 às 18:30 horas.

Aparece então um intervalo e as mensagens de 28, 30 e 31 de agosto podem ser resolvidas somente em 1º de setembro. Mas parece não ter sido possível resolver a chave diária do dia 29 de agosto, definitivamente.

Novamente aparece um intervalo de 3 dias antes que os ingleses conseguissem ler as mensagens do dia 1º de setembro.

Então ocorreu um intervalo entre dois e quatro dias para os primeiros dez dias de setembro.

Mas na avaliação do desenvolvimento da Batalha do Atlântico é muito importante lembrar que resultados das radio-informações, desta ou de outra forma, estavam disponíveis para ambos os lados durante toda a guerra.

Os sucessos da criptoanálise não eram obtidos regularmente, mas somente durante parte da batalha e na sua maioria com intervalo de tempo, falhas ou interrupções.

As conseqüências deste processo para a guerra dos submarinos alemães pode ser mostrada por meio deste gráfico.

Pode ser visto o número médio de submarinos na área de operações, na parte superior, nas áreas mais distantes e na inferior, nas derrotas dos comboios.

Somente a última é de maior interesse no nosso texto.

Freqüentemente estavam em operação de 8 a 10 submarinos até a primavera de 1941.

Mas, desde o início da operação dos comboios, no verão de 1940, eles afundaram em média cerca de 200 mil toneladas mensalmente.

Quando *Ultra* começou a funcionar, seu resultado, além do afundamento de submarinos alemães, foi principalmente evitar as perdas do tráfego marítimo aliado.

Quando calculamos os possíveis sucessos dos submarinos alemães, considerando-se as áreas de operações e o número de unidades empregadas com sua média de toneladas afundadas por dia, pode-se estimar as prováveis perdas de navios em condições normais verificando-se o quanto *Ultra* concorreu para evitar estes afundamentos, pela facilidade de desviar os comboios, em suas derrotas, dos grupos de ataques de submarinos.

Cerca de 1,6 milhão de toneladas foram salvas na segunda parte de 1941.

A primeira grande crise na guerra submarina foi superada no início de 1942.

Mas isto não foi conseqüência de uma melhoria nas cifras alemãs, o que conduziu ao *black-out,* interrupção, do trabalho em Bletchley Park.

Desde janeiro de 1942, o principal campo de ação dos submarinos alemães foi alterado para a Costa Leste dos Estados Unidos e o Caribe, onde cruzavam escoteiros numa determinada área de operações, tentando afundar o maior número possível de navios que trafegavam sem escolta.

Nesta forma de operação, o tráfego de mensagens-rádio permanecia baixo.

Assim, as radioinformações podiam somente dar um pequeno auxílio na prevenção de perdas de navios mercantes.

Esta interrupção deveu-se ao receio dos alemães de terem comprometido uma cifra, que se seguiu a grandes perdas dos navios de abastecimento no Atlântico em junho de 1941.

Não obstante o fato de que uma investigação levou à conclusão de que deveria ter havido algumas outras causas para estas perdas, o Comando dos submarinos introduziu algumas medidas adicionais de segurança.

Assim, supercodificou as duas letras da grade de referência de posicionamento e introduziu uma nova versão da máquina cifrante para utilização pelos submarinos.

Em 1939 era possível cifrar todas as mensagens diárias da Marinha, numa média de 190, transmitidas por rádio, com a utilização de dois circuitos de cifras, no estrangeiro e no território alemão.

Mas o volume sempre crescente do tráfego das mensagens tornou necessário

estabelecer primeiramente um circuito adicional com freqüências separadas e em seguida novos circuitos de cifras para reduzir o número de mensagens com as mesmas introduções de cifras.

Também foi preparado um novo livro de códigos para as mensagens abreviadas e grupos identificadores que formou a base para as chaves dos telegramas.

Acima de tudo pretendiam introduzir um novo circuito de cifra especial para os submarinos no mar e utilizar somente a nova máquina *M4* de quatro rotores.

Com este quarto rotor adicional, a medida dos ciclos da máquina aumentou de 16 900 para 440 mil.

Como os criptoanalistas ingleses não estavam preparados para uma máquina cifrante com quatro rotores, todas as suas tentativas falharam durante onze meses.

Isto teve algumas conseqüências após a mudança efetuada pelo Comando dos submarinos, retornando à sua principal área de operações nas derrotas dos comboios do Atlântico Norte, após ter sido introduzido o sistema de comboios na Costa Leste dos Estados Unidos, em julho de 1942.

Agora, sem *Ultra,* as derrotas dos comboios aliados dependiam de outras fontes do Centro Operacional de Informações (COI), como as notícias de todas as espécies de ataque, detecção e acompanhamento dos submarinos alemães pelos navios e aeronaves aliados, assim como posições obtidas pela radiogoniometria e pela análise do tráfego-rádio.

Com estas informações podiam apenas posicionar corretamente uma pequena fração de submarinos no mar a cada dia.

Mas o COI (em inglês OIC — Operational Intelligence Centre) mantinha-se muito bem informado sobre o número de submarinos no mar por meio do tráfego-rádio das forças de patrulha alemãs no canal da cifra *Hydra,* que podia ser facilmente decifrada.

Assim, os órgãos de informações dos ingleses podiam fazer algumas estimativas baseadas na forma conhecida de operação dos submarinos, mas raramente tinham a necessária precisão para evadir o comboio de uma linha de patrulha da "matilha", especialmente quando o Comando dos submarinos recebia informações decifradas de mensagens de posição ou derrotas dos comboios que eram esperados, do seu próprio xB-Dienst, a tempo de serem usadas operacionalmente.

Em algumas ocasiões era possível às forças de escolta dos Aliados obter marcações da primeira mensagem de contacto com o comboio enviada por um submarino alemão, localizá-lo, fazendo-o imergir, o que levava à perda de contacto com o seu alvo, evitando então que o comboio fosse detectado pelos outros submarinos.

Esta era uma outra forma de radioinformações que nada tinha a ver com a decifração de mensagens, mas foi de grande importância para o curso tomado pela Batalha do Atlântico.

Em dezembro de 1942, Bletchley Park novamente conseguiu sucesso com a cifra *M4* usada pelos submarinos alemães.

Isto — muito provavelmente — foi conseqüência de uma nova captura de material de cifras de um submarino, afundado no Mediterrâneo Oriental.

Após um início vagaroso na segunda parte, em dezembro de 1942—primeiros dias de janeiro de 1943, períodos em que o atraso na decifração levou à ocorrência de duas grandes batalhas de comboios com pesadas perdas de navios dos Aliados, *Ultra* obteve tantos sucessos em seguida, que foi possível evitar os submarinos alemães que faziam as linhas de patrulha no Atlântico Norte, com 6 comboios indo para o Leste e 8 para o Oeste.

Mas, em fevereiro, o número de submarinos aumentou para mais de 40 na área e o Comando pôde posicionar três linhas de patrulha que eram difíceis de ser contornadas.

O xB-Dienst apoiava o Comando dos submarinos no movimento de seus grupos, pois esta organização tinha capacidade para decifrar cada vez mais as mensagens de derrotas dos comboios ou as mensagens de posição dos submarinos germânicos enviadas pelos Aliados, a tempo de se antecipar aos desvios de rotas dos navios mercantes.

A exatidão das mensagens de situação dos submarinos deu origem a uma nova preocupação sobre a segurança da cifra, entre os alemães.

Novamente o Almirante Dönitz ordenou que fosse realizada uma grande investigação, chegando-se à conclusão de que todas as informações dos Aliados deviam ter sido obtidas de outras fontes, tais como radiogoniometria, localização por radar e avistamentos por navios e aeronaves.

Esta conclusão apoiava-se no fato de que em fevereiro, inicialmente, dois comboios no rumo leste, seguindo-se a três outros rumando para oeste, foram interceptados e dois deles atacados com grande sucesso.

Mas compreendeu-se que era tempo de introduzir um novo refinamento na máquina de cifras.

No dia 14 de março foi colocado em serviço um segundo rotor na posição da esquerda, utilizando-se uma palavra-código.

Quando esta palavra-código foi decifrada em Bletchley Park houve um grande receio de um novo *black-out* no entendimento das mensagens.

Esta era uma situação muito ruim.

Sem contar com as informações altamente confiáveis das disposições do inimigo, parecia quase impossível alterar as derrotas dos comboios para tirá-los do alcance das "matilhas" dos submarinos alemães, cujo número crescia incessante e rapidamente.

O sistema de comboios parecia estar em sério perigo, se comboio após comboio estava sendo interceptado e perdendo até 20 por cento dos seus navios, como foi o caso dos quatro que estavam rumando para leste no mês de março.

Assim, tudo ficou dependendo da rapidez com que Bletchley Park poderia resolver o novo problema criptológico.

Concentrando todos os meios disponíveis em Bletchley Park e utilizando também os equipamentos da Força Aérea e do Exército, os experientes analistas puderam resolver o novo truque dos alemães.

Penso que foi o segundo grande resultado dos criptoanalistas de Bletchley Park durante a guerra.

A partir de 20 de março, *Triton* estava novamente disponível para a Sala de Acompanhamento de Submarinos com um retardamento de um a três dias.

Os comboios podiam ter suas rotas alteradas convenientemente, mais uma vez.

Mas tornou-se possível uma nova utilização destas informações agora.

Durante a Conferência de Casablanca, em janeiro de 1943, o Presidente Roosevelt e o Primeiro-Ministro Churchill decidiram colocar a vitória na Batalha do Atlântico no mais alto grau de prioridade para a estratégia dos Aliados em 1943.

Foi decidido então colocar à disposição, nas rotas do Atlântico Norte, 6 grupos de apoio capitaneados pelos primeiros navios-aeródromos de escolta disponíveis.

Para obter os navios necessários foi preciso cancelar os comboios para o Norte da Rússia durante o próximo mês, e tomada a decisão de enviar algumas das aeronaves de longo raio de ação *Liberator* para a área do Atlântico Norte.

A utilização destas novas aeronaves e navios de forma tão eficiente na Batalha do Atlântico foi a conseqüência mais decisiva do emprego de *Ultra*.

Somente 8 semanas após, o Almirante Dönitz teve de admitir a derrota dos submarinos alemães na batalha dos comboios do Atlântico Norte e encerrou a luta naquela área.

Não há qualquer dúvida, sem *Ultra* teriam sido necessários muito mais grupos de apoio com porta-aviões de escolta e Bombardeiros *Liberator* de longo raio de ação para inverter a maré da batalha.

Estas forças adicionais não estavam disponíveis na primavera e verão de 1943, no Altântico.

Naturalmente, numa crise no Atlântico Norte, em abril e maio, os líderes aliados poderiam tomar a decisão de transferir algumas forças do Mediterrâneo ou do Pacífico, mas somente após ser alcançado um acordo para antecipar os assaltos anfíbios na Sicília (Itália), no Mediterrâneo, e as operações ofensivas no Pacífico, no outono de 1943.

E mesmo neste caso somente no verão de 1943 teriam forças suficientes para conter o perigo que os submarinos alemães representavam.

Uma demora de cerca de 3 ou mais meses para inverter a maré na Batalha do Atlântico conduziria a maiores perdas de navios, representando cerca de meio milhão de toneladas, o que teria modificado todo o esquema de tempo para a estratégia aliada.

Provavelmente não seria possível a invasão da Normandia em junho de 1944 ou mesmo no verão deste ano.

As radioinformações foram de crescente importância em quase todos os teatros de guerra.

O tempo disponível para apresentarmos este assunto não nos permite discutir seus problemas durante a operação de Pearl Harbor e as campanhas subseqüentes na área do Pacífico.

Nosso conhecimento é insuficiente, no momento, para discutir a importância das radiocomunicações na guerra contra a União Soviética.

Mas temos uma grande quantidade de material que permite discorrer sobre os problemas das radioinformações durante as operações aliadas no Norte da África e Tunísia, durante as operações anfíbias na Sicília, Salerno, Anzio e a campanha na Itália.

Em todas estas operações, os comandantes aliados, com muito poucas exceções, depositavam cada vez maior confiança nas informações oriundas desta fonte.

Mas deve ser lembrado que *Ultra,* muito raramente, decifrou ordens de operações que pudessem ser apresentadas aos comandantes aliados.

A informação mais importante, que vinha da análise de um número astronômico de mensagens, era o quadro verdadeiro da ordem de batalha e do pessoal, material e situação logística do lado alemão.

Em acréscimo, aprenderam muito sobre o estilo de trabalho e as possíveis reações dos líderes germânicos.

Assim, obtiveram, como o meu amigo Harold Deutsch algumas vezes relatou-nos, um grau de conhecimento maior, que foi de grande influência não somente para a sua liderança tática, mas algumas vezes para a estratégia também.

Existem dois fatores que devemos apreciar, na época do preparo da invasão da Normandia.

Na situação estática na Europa Ocidental, o Alto Comando Germânico podia usar comunicações por cabo, de modo que somente ocorreram poucas mensagens *Ultra.*

Assim, o movimento de resistência francês recebeu ordens para destruir as estações de amplificação das linhas de teleimpressoras, de modo que os alemães tinham de usar comunicações sem fio para sanar estes problemas.

Passaram então a usar as radiocomunicações que podiam ser interceptadas pelos ingleses através de suas estações de recepção, fora da zona de guerra alemã.

Mas os alemães usaram um sistema de cifras totalmente diferente para as linhas de teleimpressoras e transferiram as mesmas cifras para as radiocomunicações.

O criptossistema era baseado numa máquina teleimpressora cifrante, fabricada pela firma Siemens e chamada *Gekeimschreiber.*

Quando os ingleses conseguiram saber o segredo desta máquina, começaram, com grande esforço, a construir uma nova máquina decifrante para se opor a este sistema.

Após algumas versões iniciais sem qualquer sucesso, em outubro de 1943, o primeiro grande computador *Colossus* estava pronto para uso e foi introduzido.

Como nas linhas das teleimpressoras o grau de sigilo do tráfego era sempre muito maior, era possível agora furar algumas vezes os circuitos dos Altos Comandos e chegar diretamente a ordens estratégicas e operacionais mais importantes.

Havia também um outro importante campo de ação para *Ultra.*

O sucesso dos desembarques na Normandia dependia, em grande parte, de um grande plano de diversão que foi estudado para confundir o Alto Comando Alemão quanto aos principais locais do esperado desembarque.

Assim, por exemplo, os Aliados criaram uma operação-rádio de grande envergadura, apoiada por outros meios para sugerir ao lado alemão a existência de mais um Grupo de Exército completo, o 1º

Grupo de Exército dos Estados Unidos, no Sudeste da Inglaterra, aguardando a oportunidade de um segundo desembarque, maior do que o realizado na Normandia.

Com *Ultra* foi possível para o Estado-Maior dos Aliados conhecer a reação alemã a este plano de diversão e reagir rapidamente às previsões germânicas.

Esta operação apoiada por *Ultra* obteve tanto sucesso que permaneceu por muitas semanas e meses, não obstante o fato de que, nesta época, o 1º Exército dos Estados Unidos era composto somente por unidades inteiramente fictícias.

Quando a guerra iniciou-se novamente na França, após o desembarque, as comunicações tornaram-se cada vez mais importantes e *Ultra* teve relevante papel ao parar o contra-ataque alemão de Mortain. Isto criou uma eufórica superestimativa das possibilidades de *Ultra.*

Quando as forças alemães, que se retiravam, aproximaram-se da fronteira da Alemanha, tornou-se possível utilizar, cada vez mais, o telefone, cujas redes estavam ainda intactas.

O Alto Comando deu ordens para manter um estreito silêncio-rádio e assim a quantidade do tráfego dos alemães diminuiu sensivelmente de setembro de 1944 até o fim da guerra.

Mas a alta confiança depositada em *Ultra* conduziu a alguns erros de cálculo pelos Aliados e negligência com algumas outras fontes de informações.

A conseqüência foi a falha no desembarque aéreo em Arnheim e a surpresa no início da ofensiva alemã nas Ardenas.

Se voltarmos atrás devemos chegar à conclusão de que as radioinformações foram de grande importância no processo de tomada de decisões da Segunda Guerra Mundial.

As radioinformações são somente uma parte de todas as fontes disponíveis.

As informações não se compõem normalmente de poucos itens, mas de uma grande quantidade de "pedras de mosaicos" de diferentes valores que, juntos, estabelecem uma correta estimativa da situação do inimigo.

Assim, as informações e, no seu contexto, as radioinformações influenciaram as operações e a estratégia das partes combatentes, especialmente dos Aliados.

Mas não se questiona que colaborou para reduzir o tempo da guerra nas áreas da Europa e do Pacífico.

Sem *Ultra,* a forma de ser obtida a vitória final sobre a Alemanha de Hitler e o Japão teria sido muito mais longa, e em muitas áreas seria percorrido um caminho bem maior, com gravíssimas conseqüências para os vencedores e as nações derrotadas.

Traduzido por

Carlos Alberto Almeida Pereira da Silva
Capitão-de-Fragata