CRIPTOANÁLISE, SUA IMPORTÂNCIA NA CONDUTA DA GUERRA

Sergio Ernesto Alves Conforto

Major de Artilharia, com os cursos de Oficial de Comunicações da Escola de Comunicações do Exército, e o curso da Escola de Comando e Estado-Maior do Exército.

INTRODUÇÃO

"A História da humanidade é a História das guerras"

Realmente, se estudarmos os diversos volumes da História Universal concluiremos que a maior parte dos acontecimentos ali narrados e que remontam às civilizações mais antigas até os dias em que vivemos, têm por tema principal os conflitos que desde as épocas mais longínqüas são a constante do relacionamento entre os povos.

Já se estimou que se somássemos os dias de paz absoluta no mundo, iniciando no tempo mais remoto de conhecimento histórico até os dias atuais, o total não atingiria duas dezenas de anos. Entretanto, nem sempre os vencedores foram os mais fortes, possuidores de Exércitos mais numerosos e melhor armados; e estas vitórias passam à posteridade como grandes feitos e consagram inúmeros personagens, levando-os à galeria dos grandes capitães, dos gênios militares. Longe de nós qualquer intenção de diminuir, por pouco que fosse, o brilho desses nomes. Seria absurdo e sem cabimento dizermos que Rommel, Von Hindenburg, Ludendorff, Nimitz, Foch, Montgomery, Patton e muitos outros, obtiveram os seus louros apenas por serem bafejados pela sorte ou que não fossem profundos conhecedores da arte militar.

Estudam-se as suas vitórias chegando-se aos menores detalhes da manobra. Desse estudo, extraem-se os ensinamentos que por sua vez, dão lugar às doutrinas militares.

Entretanto, dificilmente se encontra, no relato das batalhas a presença do fator que foi talvez, aquele que fez pender a balança da vitória para determinado lado. Na verdade, sempre se evitou sequer fazer-se referência a este fator, não que isto diminuisse a glória do vencedor, mas para proteger aquilo que se tem constituído em um dos mais preciosos segredos de todas as nações: — o trabalho de criptoanálise.

Considerada como assunto merecedor do mais elevado grau de sigilo, tem sido a criptoanálise afastada das páginas do noticiário e da História e só há pouco, graças ao extraordinário desenvolvimento dos meios de comunicação, uma pequena parte de sua influência foi divulgada e mesmo assim, cercada de uma aura de mistério que como que a aproxima do subrenatural. No entanto, aqueles que têm a oportunidade de conhecer um pouco mais sobre ela freqüentemente se porão a pensar se, não existisse a criptoanálise, seriam os mesmos os nomes que figuram na relação dos grandes generais.

Este trabalho tem por principal objetivo despertar o interesse do leitor militar para esse fator que normalmente não é demonstrado durante os seus estudos e fazer com que venha a ser levado em conta quando, na paz ou na guerra, uma decisão deva ser tomada.

Durante o seu desenvolvimento serão dados alguns exemplos históricos que ilustram o que acima foi dito. Posteriormente procuraremos mostrar aspectos da situação atual de nosso país seja no que diz respeito às medidas de proteção às nossas comunicações, seja no estabelecimento de um sistema que permita realizar a criptoanálise na escala desejável. A nossa conclusão constará de algumas sugestões no sentido de melhorar nossa atual posição.

DESENVOLVIMENTO

Exemplos Históricos

Poderíamos citar exemplos de emprego da criptoanálise na conduta das operações militares e políticas desde algumas centenas de anos, mas isto seria certamente fastidioso. Limitar-nos-emos aos fatos conhecidos de maior importância no século XX e que tiveram, de alguma forma, o poder de mudar o curso da História.

A Batalha Final

A RÚSSIA entrou em colapso em 1917 e isto possibilitou à ALEMANHA equilibrar a grande desvantagem que lhe trouxera a entrada dos EE.UU. na guerra, pois lhe permitiu transferir para o front ocidental cerca de três milhões de homens que lutavam no leste, enquanto o grosso do potencial americano não tivera tempo de ser aplicado.

Durante o inverno a ALEMANHA verificou que teria que vencer a guerra na primavera de 1918 ou a perderia de vez. LUDENDORFF planejou romper as linhas aliadas e tomar PARIS. As divisões francesas eram esqueletos de apenas 6.000 homens. Os ingleses tinham um claro de 100.000 homens e não tinham mais como preenchê-lo. O moral aliado estava em seu mais baixo nível. Em toda a frente os alemães estavam mais fortes. Se PARIS caísse, a guerra estaria vencida.

Os alemães não tencionavam repetir os erros do princípio da guerra, em que a fraqueza de seus sistemas criptográficos fora intensamente aproveitada, principalmente pelos franceses. Por isto criaram uma cifra inteiramente nova para ser utilizada em tudo que se referisse à ofensiva final.

Os aliados pressentiam aquela operação, mas precisavam de dois ou três meses para que os americanos pudessem ser plenamente aplicados na guerra. O aparecimento da nova cifra em si já se constituía em um sinal da iminente ofensiva alemã. Entretanto, as mensagens continuaram indecifráveis e a 21 de março, 62 divisões alemãs irromperam em uma frente de 64 km. Em uma semana os alemães estavam a menos de 59 km de PARIS. Entretanto, o mais brilhante criptoanalista francês, GEORGES PAINVIN, trabalhava furiosamente na tentativa de decifrar o sistema alemão. Enquanto isto, o grande canhão BERTHA já despejava suas granadas no interior da capital da FRANÇA. Os ministros preparavam-se para evacuá-la.

Os alemães tinham ainda cerca de quinze dias para o assalto final. Era essencial atacar os aliados onde eles menos esperassem, como das outras vezes, e o sucesso dependia da segurança das mensagens. Para aumentá-la, fizeram uma modificação no sistema. Isto, entretanto, deu a PAINVIN a inspiração para a solução. A 2 de junho ele resolveu a mensagem mais importante, e que dizia: "Enviem munições urgente. Mesmo durante o dia, se não forem vistos". Embora simples, esta mensagem era vital, pois fora endereçada ao EMG do 18º EXÉRCITO alemão em RENAMGIES, uma pequena cidade a meio caminho dos dois braços da pinça que ameaçava PARIS.

O serviço de informações aliado deduziu imediatamente que a munição mencionada era necessária para a enorme preparação de artilharia que precedia os ataques alemães tal como tinham feito em março e maio e que os tinham levado às portas da vitória. Tudo indicava, pois, que LUDENDORFF iria golpear no interior da pinça, entre MONTDIDIER e COMPIEGNE, um setor a cerca de 80 km ao Norte de PARIS.

FOCH colocou suas reservas em posição de forma a bloquear aquela região. Jogara uma cartada por tudo ou nada. Mas a 9 de junho a ofensiva alemã se lançou exatamente onde era esperada. Pela primeira vez, naquele ano, LUDENDORFF não obtivera a surpresa.

Durante cinco dias a batalha se desenrolou, ora favorável aos alemães, ora aos franceses. Finalmente, os germânicos foram detidos e pouco depois a iniciativa passou para os aliados, reforçados pelos americanos. A guerra mundial estava perdida para os alemães.

O início da I Guerra Mundial foi o ponto de inflexão da história da criptoanálise. Antes, tivera pequeno emprego; depois assumiu papel preponderante. A causa disto foi o grande incremento das comunicações, principalmente por rádio.

Romel – Gênio Militar (até que ponto?)

Poderíamos citar ainda, numerosos exemplos da influência da criptoanálise naquela conflagração. Preferiremos, entretanto, passar a outros mais recentes, ocorridos durante a II Guerra Mundial.

Em inícios de 1941 os ingleses colhiam explêndidas vitórias no Norte da ÁFRICA. Os italianos são capturados aos milhares. MUSSOLINI quase que implora o auxílio alemão que finalmente lhe é dado, mas com a condição de que todas as unidades rápidas ficassem sob o comando de um general alemão. Isto fez com que ERWIN VON ROMMEL fosse colocado à testa do DEUTSCHE AFRIKAKORPS.

Em fevereiro,o general já se acha no continente africano. Com ele a astúcia, a intuição do terreno já demonstrada na depressão de HOUX e no planalto de HORNOY. Com ele a Cia FERNMELDEUFKLARUNG, que interceptava toda e qualquer estação de rádio do 8º Exército inglês, ouvia as conversas dos rádio-operadores, localizava concentrações de tropas e movimentos por rádio-goniometria e estudava os criptogramas ingleses, somando-se estas ações às desenvolvidas pelo PERS Z um dos órgãos de criptoanálise de alto nível dos alemães.

Suas vitórias não se fazem demorar. Apesar da cautela recomendada por HITLER e pelo fato de não contar ainda com todas as forças que receberia, a partir de 24 de março toma EL AGHEILA, AGEDÁBIA, BENGASI. Generais ingleses são aprisionados. Em dez dias chega à fronteira egípcia. Neste tempo seu nome é citado em todo o mundo.

Durante a campanha da ÁFRICA adquire o cognome de "RAPOSA DO DESERTO". Mas há fatos que poucos livros contam. O mais importante deles diz da existência do adido militar americano no CAIRO, CEL BONNER FRANK FELLERS, brilhante oficial que percorria os campos de batalha e estudava a tática e os problemas da guerra no deserto, fazia perguntas e observava os acontecimentos tendo acesso a muitos segredos dos britânicos.

FELLERS enviava extensos relatórios de suas atividades e do que observava a seus superiores em WASHINGTON, usando o código "Negro", do serviço diplomático americano. Ele discorria sobre as forças inglesas no front, suas missões, capacidade e eficiência; falava de reforços esperados, navios de suprimento que chegavam, problemas de moral, analisava as diversas operações em estudo pelos britânicos, e até mesmo descrevia planos de operações.

As interceptações de suas mensagens eram enviadas imediatamente aos criptoanalistas alemães que as decifravam, traduziam e recifravam em um sistema germânico e as transmitiam a ROMMEL. Freqüentemente, ele lia as mensagens apenas poucas horas após terem sido enviadas por FELLERS.

E que mensagens eram? Elas davam a ROMMEL o mais fidedigno e amplo

relatório sobre as forças inimigas e suas intenções que qualquer comandante do Eixo jamais teve.

No vai e vem da guerra na ÁFRICA, ROMMEL fora forçado a recuar através o deserto pelo Gen AUCHINLECK, no final de 1941, mas no início de 1942 ele retornou com tal vigor que em 17 dias ele empurrou os ingleses de volta por quase 500 quilômetros. Durante esses dias ele dispôs de informações como estas, provindas de mensagens do CEL FELLERS:

– 23 Jan – 270 aviões e certa quantidade de artilharia antiaérea foram retiradas do Norte da ÁFRICA para reforçar as forças britânicas no Extremo Oriente.

– 25 – 26 Jan – Avaliação das deficiências do Eixo em blindados e aviões.

– 29 Jan – Completa relação das forças blindadas britânicas, incluindo número de carros disponíveis e indisponíveis e suas localizações. Localização e grau de eficiência das unidades blindadas e motorizadas.

– 1º Fev – Próximas operações de comandos; grau de eficiência de diversas unidades britânicas; informação que os tanques americanos M3 não poderiam ser utilizados antes do meio de fevereiro.

– 6 Fev – Localização e grau de eficiência da 4ª Divisão Indiana e 1ª DB; alterações nos planos ingleses de penetrar através da linha ACROMA – BIR HACHEIN; reconhecimento da possibilidade das forças do Eixo alcançarem a fronteira egípcia desde que as divisões blindadas viessem a ser reagrupadas.

– 7 Fev – Forças britânicas estabilizadas na linha AIN EL GAZALA – HACHEIN.

Mensagens posteriores deram a ROMMEL a informação de que os ingleses pretendiam fixar sua linha defensiva em MERSA MATRUTH; quando AUCHINLECK decidiu que esta posição seria insustentável, as interceptações permitiram a ROMMEL saber que os ingleses tinham mudado de idéia.

Assim as espetaculares vitórias de ROMMEL dependiam quase que apenas de ter ou não combustível.

Mas a 10 de junho a maré da sorte do comandante alemão começou a esvaziar-se. O comandante da Cia de Inteligência de Campanha e a maioria do seu pessoal foram mortos ou capturados durante uma ação relâmpago dos comandos ingleses. Muitos dos seus registros caíram em mãos britânicas. Isto dificultou em muito o trabalho dos futuros recompletamentos e deu aos ingleses uma visão do que estava ocorrendo.

Cerca de um mês depois o CEL FELLERS foi chamado de volta à AMÉRICA e o sistema de cifras americano mudado.

ROMMEL perdera o seu maior trunfo justamente quando estava às portas da vitória, frente a EL ALAMEIN.

Os ingleses, graças aos documentos capturados, taparam as brechas de seu sistema de comunicações.

Pouco depois, chega MONTGOMERY e os fatos restantes são conhecidos.

Posteriormente, o 1º Ministro CHURCHILL disse:

"Antes de ALAMEIN nós nunca tivemos uma vitória; após ALAMEIN nós nunca tivemos uma derrota."

O início do fim para o Japão.

Após o ataque a PEARL HARBOUR a esfera de domínio japonês na ÁSIA expandiu-se largamente. GUAM fora capturada a 10 de dezembro, WAKE a 23 e HONG KONG a 25. Os aviões nipônicos afundaram o Prince of Wales e o Repulse, praticamente expulsando os ingleses do Pacífico Oeste, Oceano Índico, Oceania e praticamente deixando a AUSTRÁLIA à mercê do JAPÃO.

SINGAPURA, MALAIA, ÍNDIAS ORIENTAIS HOLANDESAS, o SIÃO e ILHAS SALOMÃO foram conquistadas, possibilitando enormes recursos de borracha e petróleo.

A CHINA achava-se bloqueada e as FILIPINAS não demoraram a cair.

O JAPÃO, vitorioso tratou agora de consolidar o domínio que conquistara. Para isso, o seu mais brilhante chefe naval idealizou um plano mediante o qual arriscaria de vez com o que restou da esquadra americana e estenderia o seu cordão defensivo de forma a manter inexpugnável o Império e suas conquistas.

O plano de YAMAMOTO, que já idealizara o ataque a PEARL HARBOUR, dividia-se em duas partes:

— A primeira consistia na captura do atol de MIDWAY, considerado a sentinela do HAVAÍ e dotado de enorme importância estratégica pois controla o Pacífico Central e permite ou impede o prosseguimento para qualquer dos seus extremos.

— A segunda e mais importante parte do plano residia no ataque e destruição do restante da esquadra americana, que fatalmente iria em socorro de MIDWAY, por forças japonesas muito maiores.

Realmente, os efetivos em presença na batalha eram totalmente favoráveis. Os japoneses dispuseram de mais de 200 navios, entre os quais 11 couraçados, 5 porta-aviões, 22 cruzadores e 65 contra-torpedeiros. Os americanos tinham, no máximo 2 couraçados, 3 porta-aviões, 9 cruzadores e cerca de 30 contra-torpedeiros, sendo que várias destas embarcações estavam avariadas.

Entretanto, um fator não fora levado em conta.

Os americanos já tinham decifrado o sistema de código japonês e receberam a ordem de operações de YAMAMOTO às suas unidades ao mesmo tempo que estas a recebiam pelo rádio. Desta maneira, pode o Almte NIMITZ posicionar a sua frota no local mais favorável e apanhar de surpresa os japoneses, no momento em

que seus aviões espalhados nos convezes dos porta-aviões ressupriam-se de combustível e bombas.

Os resultados foram largamente expostos em um filme há pouco exibido. O JAPÃO começava a perder a guerra.

Outra brilhante vitória americana devida à criptoanálise ocorreu pouco depois. O próprio YAMAMOTO foi morto mediante um ataque ao avião em que viajava por terem tido as forças americanas conhecimento da viagem de inspeção que fazia.

Outros Exemplos

Poderíamos ainda relatar inúmeras ações em que a criptoanálise teve papel preponderante. Entretanto, isto alongaria demasiado este trabalho, sem maiores proveitos. Apenas, citaremos alguns, para a memória do leitor:

– Malogro do ataque aéreo aliado a PLOESTI.

– Sucesso alemão na invasão à NORUEGA.

– Alto rendimento alcançado pelos ataques de submarinos alemães aos comboios aliados até 1943.

– Desistência dos alemães em invadir a INGLATERRA, em 1940.

– Neutralização da guerra submarina movida pelos alemães, a partir de 1944.

– Obtenção da surpresa quando do desembarque aliado na NORMANDIA.

– A batalha das ARDENAS, em fins de 1944.

– A reação finlandeza à invasão russa, em 1940.

– Sucessos alemães na invasão à RÚSSIA, em 1941 e 1942.

Incontáveis foram os sucessos obtidos em ações de pequenos escalões graças a criptoanálise. Os grandes chefes militares bem sucedidos nas últimas guerras tiveram atrás de si uma seção de criptoanálise. E por que foi tão grande o seu sucesso?

Talvez por uma tendência muito natural que possui o não especialista em acreditar na impossibilidade do adversário ler as suas cifras e códigos.

Os manuais de comunicações nos dizem que o comandante utilizará ou não os sistemas criptográficos mediante o estudo dos fatores rapidez e segurança que pretenda imprimir às suas mensagens. Tendo dado maior valor à segurança e decidido pelo emprego de cifras ou códigos poderá ser levado a crer demasiado nesta segurança e isto lhe poderá ser fatal.

E como proceder então, já que nos parece ter-se chegado a um impasse?

Como em outros tipos de operações, a melhor defesa continua a ser o ataque. Um comandante que disponha de uma boa seção de criptoanálise poderá só pesquisar e revelar os segredos de adversários como também avaliar até que ponto

são seguros os seus de forma a usá-los na exata medida.

Situação Atual

Antes de nos dedicarmos ao nosso país, vamos procurar dar uma idéia do que ocorre em outros, para que se possa estabelecer uma comparação.

Inglaterra

Iniciou suas atividades de criptoanálise com um pequeno número de pessoas apenas interessadas, chefiadas pelo diretor de ensino naval, Sir Alfred Ewing, no ano de 1914. A seção foi inicialmente denominada "Room 40", pela sala que ocupavam. Posteriormente veio a ser conhecida por "ID 25" (Seção 25 da Intelligence Division).

A natureza o o volume de mensagens a serem estudadas logo exigiu o aumento do efetivo e a descentralização das ações.

O Exército inglês também criou sua seção, o M. I. 1 (b), ligada ao Ministério da Guerra e que possuía uma agência de campanha, no QG das Forças Expedicionárias Britânicas, no continente. Criptoanalistas individuais trabalhavam em diversos Exércitos.

O M. I. 1 (b) possuía inicialmente (dezembro de 1915), apenas quatro elementos e o seu chefe era um major que fora ferido no ano anterior, capturado pelos alemães e posteriormente repatriado, por ser julgado incapaz para o serviço militar devido a uma paralisia parcial que adquiriu.

Como o seu correspondente naval, iniciou seus trabalhos com amadores de criptoanálise, mas logo seu efetivo subiu, chegando a 84, inclusive 30 mulheres, ao fim da guerra.

Posteriormente os britânicos unificaram esses serviços e na II Guerra Mundial o seu trabalho foi de valor inestimável. O 1º Ministro recebia diretamente um relatório diário de suas atividades.

O "Jornal do Brasil", de 7 de setembro de 1974, publica uma reportagem sobre um grupo denominado "HUT 3" e relata seus sucessos que chegaram à leitura de mensagens alemãs cifradas pela máquina "Enigma".

Alemanha

Quando do irrompimento da I Guerra Mundial não possuía serviço de criptoanálise, o que lhe trouxe sérios problemas na elaboração de seus próprios códigos e cifras, bastante elementares aos olhos de seus adversários. Podemos dizer que os alemães não tinham capacidade para fazer a autocrítica de seus sistemas.

Somente em 1916 foi criado o Abhorchdienst (Serviço de interceptação) onde criptoanalistas, a maioria dos quais recrutados entre matemáticos, logo obtive-

ram ótimos resultados embora nunca pudessem suplantar os serviços similares dos aliados que, desde os primeiros dias da guerra já se familiarizaram com a fraseologia e vícios dos seus adversários e, com estes ensinamentos, puderam melhorar, sobremaneira, a segurança de seus próprios sistemas de comunicações.

A mesma situação não se aplicou à ALEMANHA quando da II Guerra Mundial. O serviço de criptoanálise do seu Ministério de Relações Exteriores fora criado em 1919 e era conhecido por Referat IZ, a seção Z da 1ª Divisão. Em 1936 a reorganização do Ministério fez com que a seção passasse a denominar-se PERS Z, a Seção Z da Divisão Administrativa e de Pessoal.

No intervalo entre as guerras a seção trabalhou ativamente, solucionando diversos sistemas diplomáticos estrangeiros.

Quando da ascenção de HITLER, em 1933, a PERS Z possuía cerca de trinta elementos. A partir daí o seu efetivo cresceu rapidamente e o recrutamento era feito de forma tal que os prováveis recrutas não sabiam que estavam sendo selecionados para um trabalho altamente secreto. Posteriormente, durante a guerra, o número de elementos da seção chegou a 300.

Ao final da guerra tinham como resultado do seu trabalho a leitura de comunicações secretas de 34 países, a saber: Inglaterra, Irlanda, França, Bélgica, Espanha, Portugal, Itália, Vaticano, Suíça, Yugoslávia, Grécia, Bulgária, Romênia, Polônia, Egito, Etiópia, Turquia, Irã, China, Japão, Mandchúria, Tailândia, Estados Unidos, Brasil, Argentina, Chile, México, Bolívia, Colômbia, Equador, Peru, República Dominicana, Uruguai e Venezuela.

Desde 1933 o Ministério da Aeronáutica possuía o seu "FORSCHUNGSAMT" (Gabinete de Pesquisas), ligado diretamente ao Ministro e que era, afinal, o elemento de criptoanálise de GOERING.

Quando HITLER fundiu as três forças armadas na WERMACHT, o órgão maior de criptoanálise, a ABWEHR ficou sob a chefia do Almirante CANARIS, embora o Exército, Marinha e Aeronáutica continuassem a possuir suas próprias equipes.

A do Exército, denominada H.N.W., era a mais antiga e mais eficente e seus elementos operavam como uma organização separada dentro de um Exército ou de um Grupo de Exércitos, constituindo-se em companhias e pelotões de informações de campanha. Conseguiram solucionar as mensagens oriundas do criptógrafo M – 209 (até hoje em uso no Brasil) praticamente desde os dias em que os Exércitos alemão e americano se chocaram na ÁFRICA DO NORTE, em fins de 1942.

A agência criptoanalítica da Marinha, o "B-Dienst" (Serviço de Observação) obteve importantíssimos sucessos. Graças a ela, os alemães, já no início da guerra, podiam ler alguns dos códigos e cifras mais secretos do Almirantado Britânico. Isto deu-lhes grandes vitórias no início da guerra e o enorme triunfo na guerra submarina até 1943.

Entretanto, a dispersão de esforços e a rivalidade entre os diversos órgãos de criptoanálise da ALEMANHA impediram que este país obtivesse melhores resultados.

Estados Unidos

Caracterizou-se, por ocasião da I Guerra Mundial, pela fragilidade de seus sistemas. Autores diversos dizem que os EUA devem ter sido motivo de riso de todo criptoanalista do mundo durante a 1ª Guerra Mundial e nas décadas de 20 e de 30. A causa disto, provavelmente, seria a inércia burocrática e exigüidade de orçamento. Entretanto, tanto o Exército como a Marinha possuíam agências de criptoanálise desde há muito. Ambas, organizadas por ocasião da I Guerra Mundial achavam-se, nos anos 20, perfeitamente estruturadas, embora com pequenos efetivos e lutando com a falta de verbas e de crédito por parte das altas autoridades.

Em 1930 o S.I.S. (Signal Intelligence Service) possuía três jovens criptoanalistas e dois mensageiros.

A lei federal de comunicações dos EUA de 1934, proibia a interceptação de mensagens de países estrangeiros por parte de americanos, pois isto não seria cavalheiresco.

Pelos exemplos acima, demonstra-se que não foi fácil a missão dos primeiros criptoanalistas americanos. Mas passaremos por cima destas dificuldades que duraram até os últimos anos da década de 30 e mesmo de como foi montado o sistema que foi o mais brilhante da II Guerra e iremos aos dias atuais, para que se possa ter idéia de quão importante é, para um país que procura manter a sua posição de potência mundial, a tarefa de criptoanálise.

É sabido que, com o término da II Guerra Mundial e o advento da guerra fria, os EUA passaram a dispor de um sistema de comunicações estratégico cujos postos espalhados por todo o mundo transmitem um total de cerca de duzentas e cinqüenta mil mensagens *por dia*. E para que a segurança destas comunicações se torne verdadeira e eficiente foi criada a Agência Nacional de Segurança, a NSA, a maior organização criptológica da história.

A NSA apareceu em 1952 como resultante da extinta AFSA, a Agência de Segurança das Forças Armadas, esta criada em 1949 para centralizar os esforços dos órgãos similares do Exército, Marinha e Força Aérea (embora estes não tenham sido extintos e tenham ficado com a incumbência de prover a segurança e análise das comunicações de caráter tático).

Dado à natureza sigilosa de suas atividades somente se veio a ter vaga notícia de sua existência em 1957, embora hoje em dia seja bastante conhecida. Suas finalidades principais são prover segurança e informações. Para isto cria e supervisiona a criptografia para todos os órgãos de governo dos EUA, e ao mesmo tempo intercepta, faz análise de tráfego e criptoanalisa mensagens de todas as outras nações, amigas ou adversárias.

A agência funciona em WASHINGTON, suas instalações só são menores que as do Pentágono e do Departamento de Estado. O edifício é dotado de dezenas de escritórios, instalações de computadores, um restaurante para 1.400 pessoas, um auditório para 500, oito bares, agência postal, ambulatório com salas de cirurgia,

agência bancária, lavanderia, etc.

Na década de 1960 seu efetivo, que vinha sendo constantemente aumentado, andava por volta de 14.000 pessoas, homens e mulheres, acrescentando-se a isto cerca de 1.000 pessoas que trabalham no exterior. O orçamento da agência não é conhecido nem mesmo pelos congressistas, sabendo-se, entretanto, que deve ser cerca de duas vezes o da CIA. Como os desta, todos os seus fundos são contabilizados acrescentando-se alguns milhões de dólares a cada item do orçamento federal.

Os funcionários são selecionados através dos mais rigorosos padrões pelo Departamento de Defesa, que incluem investigações secretas sobre sua lealdade e ainda testes pelo detetor de mentiras. Além disto, qualquer funcionário pode vir a ser dispensado sumariamente por decisão superior sem que lhe caiba qualquer recurso trabalhista.

Grande parte do pessoal que lá trabalha consiste em cientistas, engenheiros e técnicos em línguas estrangeiras e de modo geral são selecionados ao terminarem as universidades.

A Agência trabalha em três grandes ramos, a saber:

- O maior de todos denomina-se Seção de Produção, ou PROD e encarrega-se das informações de comunicações. Por isto entende-se a criptoanálise, análise de volume de tráfego e análise de texto claro. Grande parte deste serviço é feito por máquinas como radares, sistemas de controle de mísseis, satélites artificiais e computadores especiais. Para isto dispõe de cerca de 2.000 posições de interceptação por todo o mundo. Os seus criptoanalistas de primeira ordem, aqueles que realmente pesquisam e encontram soluções são cerca de 200 e trabalham em equipes. Acredita-se que a NSA decifre sistemas de todas as nações;
- Outro ramo é a seção de pesquisa e desenvolvimento, que estuda novos princípios de cifragem e novos métodos de transmissão;
- O terceiro ramo destina-se à segurança das comunicações e é o COMSEC. É responsável pela proteção das comunicações secretas do governo. Para isto, prescreve ou aprova os sistemas que cada órgão deve usar e como devem ser usados. Elabora a doutrina de segurança criptográfica e supervisiona a sua execução.

Produz ou controla a produção de todo o material criptológico (incluindo equipamento criptográfico, instruções, peças sobressalentes e material complementar) para todos os usuários, inclusive Forças Armadas; controla ainda o emprego e proteção de todo este material, bem como sua retirada de uso. Estuda ainda cada criptosistema proposto para determinar quão seguro ele é, isto é, quantas mensagens poderão ser enviadas por ele sem mudança de chaves, obtendo-se a segurança desejada. Baseando-se neste estudo prescreve o período de mudança de chaves necessário a cada sistema.

A NSA é sem dúvida a maior e mais eficiente "câmara negra" de todo o mundo. Entretanto, é possuída por um país que por muito tempo relegou a criptoanálise a um plano bastante inferior. Foi preciso que Pearl Harbour tivesse ocorrido para que a consciência dos dirigentes dos EUA despertasse para a sua importância. Felizmente, não foi tarde demais, mas de qualquer forma, Pearl Harbour já tinha ocorrido.

Brasil

Partamos da hipótese que no Brasil não exista um órgão especialmente destinado à criptoanálise de mensagens, sejam de origem interna sejam de outros países. Admitamos ainda que o Exército, particularmente, não tenha um serviço a isto destinado, e também para a elaboração de sistemas para o seu uso, bem como ao levantamento da confiabilidade dos que hoje emprega; que não haja uma diretriz que regule a utilização desses sistemas pelos diversos escalões; que a maioria dos seus oficiais não tenha conhecimento de quanto tem sido influenciado o curso da história pela ação da criptoanálise.

O que poderia ser feito a curto, médio e longo prazo para minorar e eliminar os problemas causados por esta situação hipotética? Passamos a alinhar algumas idéias neste sentido.

Necessitaríamos, sem dúvida, de um órgão que, em nível nacional, a exemplo do que ocorre com a NSA nos EUA e agências similares nos demais países coordenasse o trabalho das agências dos demais órgãos de governo, como os Ministérios Militares, das Comunicações, Relações Exteriores, Interior, Justiça, etc. . .

Este órgão, naturalmente, seria diretamente ligado ao Serviço Nacional de Informações e, sem que houvesse o perigo de vir ferir suscetibilidades, seria o responsável pela elaboração e *controle da execução da política brasileira de segurança das comunicações,* bem como abrigaria o órgão de criptoanálise mais elevado. Teria a palavra final na liberação de todos os elementos diretamente envolvidos neste tipo de atividade. Teria os mais completos registros sobre o assunto, uma vez que a ele seria enviada uma síntese do trabalho das demais agências e que a ela recorreriam para resolver problemas acima de suas capacidades técnicas e materiais.

Tal órgão recrutaria os elementos mais destacados na matéria e seria dotado de facilidades de processamento de dados próprios, fator indispensável a seu bom êxito.

Contaria com auxílio não só dos órgãos diretamente ligados ao governo como também, de maneira indireta, de outras entidades como aquela que congrega rádio-amadores, empresas civís brasileiras no exterior, etc. . . .

Poderia ainda coordenar e auxiliar associações não oficiais destinadas à descoberta e estímulo a pessoas com aptidões à atividade criptoanalítica, mediante a publicação de trabalhos e revistas, realização de concursos e intercâmbio. Isto daria lugar à catalogação de elementos aproveitáveis imediata ou remotamente.

Baixaremos agora um pouco de escalão, e conjecturemos sobre o Exército.

Parece-nos que o ponto de mais difícil solução na criação de um sistema de criptoanálise é justamente a seleção do pessoal com as características necessárias. O criptoanalista precisa possuir determinadas qualidades inatas sem as quais dificilmente terá sucesso. Precisa possuir aquilo que YARDLEY denomina "cérebro de cifra". Seria isto a capacidade da mente em realizar a operação psicológica básica da criptoanálise — o reconhecimento de um tipo de modelo, a integralização de um texto fragmentário a que nunca tenha visto antes.

Cada problema representa para ele um desafio, pois seu interesse reside não no que contém aquele texto, mas no ato de solucioná-lo. Deve possuir uma capacidade de concentração tal que o faça debruçar-se sobre a tarefa por horas a fio sem que a fome, sede ou fadiga venham perturbá-lo. Terá tão grande desprendimento que o faça entregar-se totalmente a uma tarefa que a priori está destinada ao total desconhecimento por parte de outras pessoas, até mesmo familiares. Sua paciência o fará recomeçar sempre que, após dias ou meses de trabalho estafante, chegar a um impasse. Naturalmente, será inteligente em alto grau. Finalmente, deverá possuir uma certa dose de intuição que até mesmo se aproxime do sobrenatural.

Convenhamos que este não é o tipo de trabalho que atraia a maioria das pessoas ou para o qual muitos sejam passíveis de indicação.

Por isso, a seleção teria que ser feita em um horizonte muito amplo para que alguns poucos possam afinal sobressair.

Durante a II Guerra Mundial os alemães faziam uma primeira triagem entre os universitários por meios de problemas de palavras cruzadas. Para tornar mais ativa a participação acenavam para aqueles que não conseguissem resolvê-los satisfatoriamente com o recrutamento para os Exércitos do Leste . . .

Parece-nos que uma forma atrativa e que apresentaria bons resultados consistiria na elaboração periódica de concursos sobre o assunto, os quais ofereceriam a todos os acertadores diplomas e prêmios, principalmente sob a forma de publicações estrangeiras especializadas, aos que mais se destacassem. Com isto conseguir-se-ia despertar o interesse entre aqueles que por natureza possuissem as aptidões necessárias e poder-se-ia cadastrar esses elementos.

Tais concursos poderiam ser difundidos até mesmo pelo "Noticiário do Exército" que publicaria periodicamente também sínteses de fatos históricos de relevância sobre o assunto.

Paralelamente a isto constituir-se-iam cursos para o desenvolvimento dos elementos mais aptos. Tais indivíduos poderiam pertencer a qualquer Arma ou Serviço, mas dar-se-ia preferência aos de Comunicações ou possuidores do Curso da Escola de Comunicações, tendo em vista a familiaridade com os sistemas de comunicações, o que lhes facilitaria a tarefa.

Vemos a possibilidade de criação de até três tipos de cursos diferentes. No primeiro ministrar-se-ia conhecimentos sobre criptoanálise dos sistemas de campanha, a lápis e papel e instrumentos mais simples. Uma excelente fonte de consulta

básica para tal curso seria a obra "Cryptanalysis" de Helen Fouché Gaines.

Os elementos que o concluíssem com aproveitamento ficariam automaticamente matriculados no segundo, a ser feito por correspondência, independentemente do local em que estivessem servindo ou seja, em órgãos ligados à criptoanálise ou não. Tal curso seria simples; consistiria na remessa a cada semestre, por exemplo, de um folheto com exposição dos últimos progressos, novas formas de solução de sistemas e proposta de resolução de alguns problemas. Isto serviria para manter, sem muito esforço, o interesse e a atualização dos "iniciados". O primeiro curso teria a duração de cerca de seis meses e ambos poderiam ser realizados na Es Com ou na Es N I, conforme a maior conveniência para o Exército.

O terceiro curso seria certamente realizado na Es N I, que congregaria nele elementos não só das Forças Armadas como também de outros órgãos de governo.

Nele seria ensinada a criptoanálise de mais alto nível, em que avultam em importância os sistemas diplomáticos. Os alunos seriam selecionados entre os que, tendo se destacado nos cursos anteriores, fossem aprovados por severa seleção por parte dos elementos de segurança.

De grande importância seria o aproveitamento de elementos egressos do IME, por sua excelente formação matemática, que é, em síntese, considerada a ciência basilar de qualquer trabalho criptoanalítico. O conhecimento de línguas estrangeiras é outro fator de enorme importância no assunto.

Na AMAN, na Es A O e principalmente na ECEME seria largamente demonstrado a seus alunos a importância do assunto por meio de exemplos históricos como aqueles a que nos referimos na primeira parte deste trabalho. Isto serviria para desenvolver o espírito de segurança das comunicações e daria aos futuros comandantes o justo valor que devem ter os códigos e cifras, impedindo que venham a confiar cegamente em algo que julgariam impossível de ser decifrado por um eventual adversário e ao mesmo tempo tornando-os receptíveis à utilização do trabalho de seus próprios criptoanalistas.

As manobras deveriam se desenvolver com absoluto realismo no que diz respeito às comunicações. Nelas se constituiriam equipes de criptoanalistas que, sem dúvida, formariam uma figuração inimiga de inestimável valor, dando aos comandantes um quadro perfeito de possíveis fragilidades existentes em suas Brigadas, Divisões de Exército ou Exércitos.

O pessoal de criptoanálise seria lotado a partir do escalão Divisão de Exército, inclusive, com o valor de pelotão, provavelmente. Brigadas atuando isoladamente receberiam equipes ou grupos oriundos da Divisão para utiliza-los em seu proveito.

O escalão Exército teria, em princípio, um núcleo de companhia capaz de enquadrar vários pelotões.

Em períodos de paz os elementos usariam efetivos reduzidos uma vez que o adestramento seria mantido por correspondência. Seriam grupados então por ocasião de manobras e exercícios periódicos.

Os que permanecessem nas funções especificadas de criptoanalistas desempenhariam suas funções normalmente ligados à 2ª Seção de seus escalões e a elementos de escuta.

Os possuidores do curso de maior profundidade estariam aptos a serem aproveitados na constituição da "Câmara Negra" brasileira ligados ao órgão máximo de criptoanálise do País.

Parece-nos que já esbocamos o que seria o sistema nacional, em geral, e do Exército, em particular. Maiores detalhes serviriam apenas para alongar este trabalho sem maiores proveitos.

Não temos dúvida que as características do TO Continental ou as condicionantes de um conflito nuclear obrigarão, quando de um possível emprego de tropas brasileiras, à utilização de forças de certa forma independentes, altamente móveis e largamente dispersas. Isto conduzirá a grande emprego dos meios-rádio de comunicações por parte dos contendores, quer em âmbito local, quer em ligação com os escalões superiores e mais recuados. E este grande emprego fornecerá um veio riquíssimo de informações por meio de criptoanálise que, se por um lado cumpre negar ao adversário, por outro urge que tenhamos condições de aproveitar. E como o sistema a isto destinado não é passível de improvisação necessária é que se crie desde logo tal sistema, para que tenhamos meios de manter a fabulosa de invencibilidade que nossas forças armadas receberam dos que nos antecederam.

BIBLIOGRAFIA

1. BAUDOIN, Commandant. Éléments de Cryptographie — Paris — Éditions A. Pedone — 1946.
2. CARTIER, Raymond — A Segunda Guerra Mundial. La Seconde Guerre Mondiale. Pa... Rio de Janeiro — Librairie Larousse et Paris Match — Gráfica Editora Primor — 197...
3. GAINES, Helen Fouché — Cryptanalysis. A Study of Ciphers and Theyr Solution. New York — Dover Publications, Inc. — 1956.
4. KAHN, David. The Codebreakers. The Story of Secret Writing — 7ª Ed. New York — The Macmillan Company, 1972.
5. NORMAN, Bruce. Secret Warfare. The Battle of Codes and Ciphers. Washington, DC. Acropolis Books Ltda. 1973.
6. SALOMON, Délcio Vieira — como fazer uma monografia. Elementos de Metodologia do Trabalho Científico, 4ª Ed. — Belo Horizonte — Interlivros — 1974.
7. SACCO, Général L. Manuel de Cryptographie. Traduzido para o francês pelo Capt J. Brés. Paris. Payot — 1951.
8. SMITH, Dwight Laurence. Cryptography. The Science of Secret Writing. New York. W. W. Norton and Company. Inc. — 1943.

9. VAN, Wehrty Rodolf. Tannemberg. Aout 1914. Traduzido do alemão para o francês por R. Jovan – 1º Ed. – Paris. Payot – 1935.

10. YARDLEY, Herbert O. The American Black Chamber. Tradução e adaptação do Ten-Cel Cav QEMA Mario Orlando Ribeiro Sampaio – 1968.

11. CALVOCORESSI, Peter. Os Segredos da Guerra Concentrados na Estação X. Jornal do Brasil. Rio de Janeiro – 1974 – Caderno B.

12. COLMENARES, Narses J. Estudio Probabilístico del Idioma Español – Caracas – Universidad Metropolitana – 1974.

13. MONOGRAFIAS e Trabalhos em Grupo – Rio de Janeiro – ECEME – 1976.

14. THE, Cryptogram. Bethesda, USA – American Cryptogram Association 1974, 1976.