ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap Inf RAPHAEL PINA VIANA

COMUNICAÇÕES NA GUERRA IRREGULAR: COMUNICAÇÃO SEGURA DA EQUIPE PRECURSORA DE FORÇAS ESPECIAIS ATRAVÉS DA INTERNET DURANTE O CONTATO INICIAL

Rio de Janeiro

2022

Cap Inf RAPHAEL PINA VIANA

COMUNICAÇÕES NA GUERRA IRREGULAR: COMUNICAÇÃO SEGURA DA EQUIPE PRECURSORA DE FORÇAS ESPECIAIS ATRAVÉS DA INTERNET DURANTE O CONTATO INICIAL

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do grau especialização em Ciências Militares.

Orientador: Cap Inf ANDRÉ **WERNECK** SERENO CARVALHO

Rio de Janeiro

2022

Ficha catalográfica elaborada pelo Bibliotecário Francisco José de Paula Junior
CRB7/6686

V614

Viana, Raphael Pina.

Comunicações na guerra irregular: comunicação segura da equipe precursora de forças especiais através da internet durante o contato inicial / Raphael Pina Viana – 2022.

68 f. il.

Trabalho de Conclusão de Curso – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2022.

Orientação: Cap. André Werneck Carvalho

1. Forças especiais. 2. Criptografia. 3. Proteção cibernética. I Escola de Aperfeiçoamento de Oficiais. II Título.

CDD: 355

Cap Inf RAPHAEL PINA VIANA

COMUNICAÇÕES NA GUERRA IRREGULAR: COMUNICAÇÃO SEGURA DA EQUIPE PRECURSORA DE FORÇAS ESPECIAIS ATRAVÉS DA INTERNET DURANTE O CONTATO INICIAL

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do grau de especialização em Ciências Militares.

Aprovado em ____/____/____

COMISSÃO DE AVALIAÇÃO

_____

VINICIUS VALVERDE ANDRIES – Maj
Escola de Aperfeiçoamento de Oficiais do Exército
Presidente

_____

FELIPE LOPES BRANDÃO – Cap
Escola de Aperfeiçoamento de Oficiais do Exército
Membro

_____

ANDRÉ WERNECK SERENO CARVALHO – Cap
Escola de Aperfeiçoamento de Oficiais do Exército
Membro

AGRADECIMENTOS

A Deus, por me intruir e guiar quanto ao caminho que devo seguir.

A minha esposa, Cris, por todo apoio e dedicação, criando condições favoráveis para que eu possa exercer a profissão militar. Quem me inspira e incentiva, sendo alicerce essencial em minha vida, e que não foi diferente durante a condução dessa pesquisa.

Aos integrantes do Comando de Operações Especiais pelo esforço diuturno para manter o mais elevado nível de prontidão que se pode esperar de uma tropa de operações especiais.

Ao Cel QEM Jose Antonio Moreira Xexéo e ao Professor Cesar Augusto Marcondes pela disponibilidade e pelas orientações.

Aos companheiros da Arma de Comunicações Victor, Scherer e Victor Kumm pela atenção e pelas orientações.

Ao companheiro e irmão de arma Pimentel, pelo apoio no desenvolvimento de ilustrações que facilitaram sobremaneira o entendimento deste trabalho.

RESUMO

Esse trabalho tem por objetivo propor um emprego adequado da criptografia para proteger uma comunicação realizada através da Internet entre uma equipe precursora de forças especiais infiltrada em território inimigo e seu elemento de comando e controle. Para isso foram revisadas as cifras criptográficas AES, RSA e Diffie-Hellman, amplamente utilizadas nos protocolos IPSec e TLS, e a cifra One-Time Pad. Foi realizado um experimento de ataque genérico contra a troca de chaves Diffie-Hellman utilizando o algoritmo Baby-Step Giant-Step para se estimar o tempo que um supercomputador levaria para comprometer a segurança de um sistema de comunicações baseado nesta troca de chave. A partir dos resultados obtidos foram apresentadas propostas de configurações de rede privada virtual, bem como uma proposta de implementação de Voz sobre IP com esquema de segurança baseado em One-Time Pad para realização de ligações ultrassecretas. Essas propostas visam atender a necessidade de segurança da comunicação de uma equipe precursora de forças especiais, desdobrada, com a base de operações do Batalhão de Forças Especiais.

Palavras-chave: Forças Especiais, Operações Especiais, Comunicações, Criptografia, Segurança da informação, Proteção cibernética, Criptologia, Criptoanálise, Baby-Step Giant-Step, Diffie-Hellman, DHKE, One-Time Pad, OTP, VPN, Virutal Private Network

ABSTRACT

This research purpose is to propose a suitable employ of cryptography to protect the communications of a special forces pilot team, at enemy area, with it command and control element. To reach this objective has been reviewed cryptography ciphers AES, RSA, Diffie-Hellman, widely used in IPSec and TLS security protocols, and the cipher One-Time Pad. Was performed a experiment which consisted of a generic attack on Diffie-Hellman key exchange using the Baby-Step Giant-Step algorithm to estimate the time required to a supercomputer compromises the security of a communication system based on this key exchange. From the results was presented proposals of Virtual Private Network configurations and a proposals of a Voice over IP implementation with a security scheme based on One-Time Pad for top secret callings. This proposals purposes to attend the security requirements of the deployed special forces pilot team's communications with the Special Forces Battalion forward operations base.

Key words: Special Forces, Special Operations, Communications, Cryptography, Information security, Cyber protection, Cryptology, Cryptoanalisys, Baby-Step Giant-Step, Diffie-Hellman, DHKE, One-Time Pad, OTP, VPN, Virutal Private Network

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

BFEsp	Batalhão de Forças Especiais
A Op	Área de Operações
AES	Advanced Encryption Standard
AOGI	Área de Operações de Guerra Irregular
B Ap Op Esp	Batalhão de Apoio às Operações Especiais
BCA	Base de Coordenação Avançada
BOBFEsp	Base de Operações do Batalhão de Forças Especiais
BOE	Base de Operações Especiais
C^2	Comando e controle
CBC	Cipher Block Chaining
COpEsp	Comando de Operações Especiais
CT	Ciphertext (texto cifrado)
DHKE	Diffie Hellman Key Exchange
DOFEsp	Destacamento Operacional de Forças Especiais
ECB	Electronic Code Book
Eq Prec FEsp	Equipe Precursora de Forças Especiais
FEsp	Forças Especiais
FLOPS	Floating-point Operations per Second
HF	High Frequency
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IPSec	Internet Protocol Security

K	Key
Kpr	Private Key
Kpub	Public Key
MB	Megabytes
MITM	Man-In-The-Middle
NFS	Number Field Sieve
OTP	One-Time Pad
PT	Plaintext (texto em claro)
SSL	Secure Scokets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TO	Teatro de Operações
UDP	User Datagram Protocol
USSOCOM	United States Special Operations Command
UW	Unconventional Warfare
VoIP	Voz sobre IP
VPN	Virtual Private Network
ZI	Zona de Interior

SUMÁRIO

1. INTRODUÇÃO

De acordo com o Manual de Campanha EB70-MC-10.212 (Operações Especiais), o termo guerra irregular é definido da seguinte forma:

> Guerra Irregular: conflito armado executado por forças não regulares ou por forças regulares empregadas fora dos padrões normais da guerra regular, contra um governo estabelecido ou um poder de ocupação, com o emprego de ações típicas da guerra de guerrilhas. Divide-se em: guerra insurrecional, guerra revolucionária e guerra de resistência (BRASIL, 2017, p. 100).

Durante a segunda fase da guerra irregular, denominada contato inicial (faseamento conforme figura 1), uma equipe precursora de forças especiais (Eq Prec FEsp) infiltra-se de forma sigilosa na área operacional de guerra irregular (AOGI) para estabelecer o primeiro contato com a força irregular e realizar as tratativas iniciais.

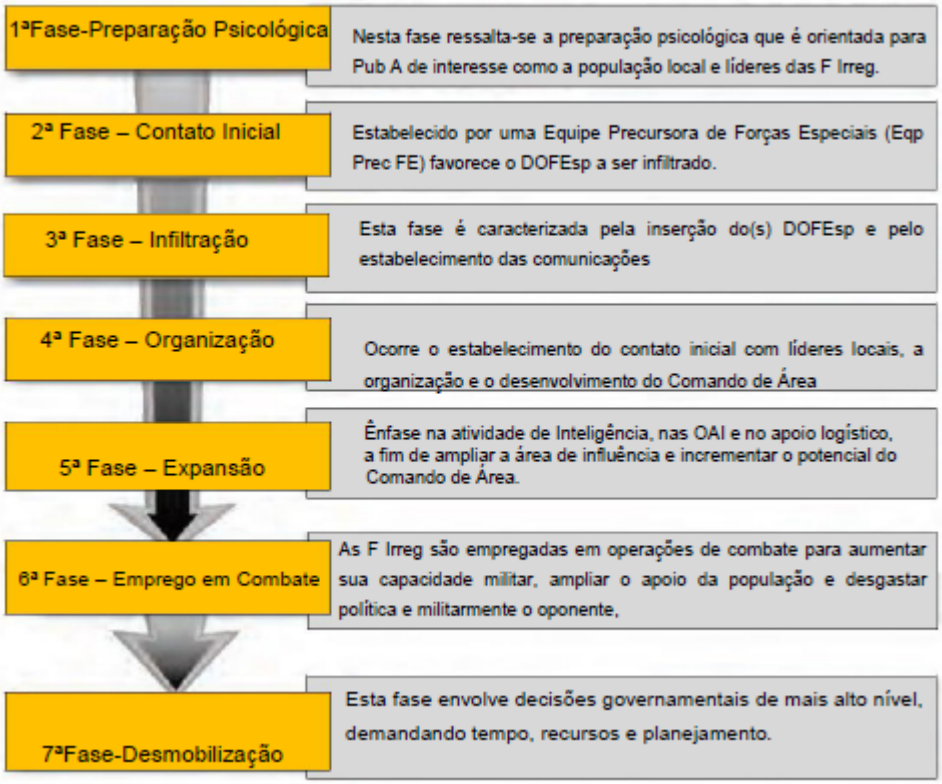


FIGURA 1 – Fases da Guerra Irregular
Fonte: BRASIL (2020, p. 15)

Nessa fase da guerra irregular, a utilização de meios não convencionais pode preponderar sobre a utilização de meios convencionais de emprego militar,

tendo em vista a necessidade de a equipe de forças especiais manter sua presença oculta da força inimiga na AOGI.

Em um ambiente operacional onde poderão estar ocorrendo buscas no espectro eletromagnético e no espaço cibernético, torna-se fator de êxito para a operação o estabelecimento de comunicação segura com o escalão superior, isto é, com garantia de integridade, autenticidade e confidencialidade (princípios da segurança das comunicações) e sem expor a localização da equipe infiltrada ao inimigo.

Um equipamento rádio pode não ser discreto o suficiente nessa fase da operação, pois devido a distância geográfica entre o elemento de comando e controle e a fração desdobrada, seria necessário utilizar um equipamento HF (high frequency) com potência elevada – tendo em vista a necessidade de fazer um enlace com a Base de Operações do Batalhão de Forças Especiais (BOBFEsp) que, nesta fase da guerra irregular, poderia estar até mesmo na zona do interior. Essa exploração rádio chamaria muita atenção no espectro eletromagnético em toda a AOGI, em especial se o equipamento utiliza criptografia, uma vez que exploração rádio criptografada pode ser avaliada pelo inimigo como indício de comunicação militar, o que poderá acarretar no aumento as operações de busca de elementos infiltrados naquela região. Além disso, outro inconveniente da utilização de equipamento rádio nessa fase é a dificuldade de se planejar e executar uma adequada estória-cobertura que justifique a utilização e transporte desse tipo de equipamento.

Uma solução mais discreta seria a utilização de um dispositivo móvel, como aparelho celular ou notebook, para realizar a comunicação através da Internet. O protocolo de segurança Transport Layer Security (TLS) – sucessor do conhecido Secure Sockets Layer (SSL) –, bem como o protocolo Internet Protocol Security (IPSec) são amplamente utilizados na Internet e por isso grande parte dos dados trafegados na rede já são criptografados. Tal situação favorece a utilização de criptografia através desse meio sem chamar a atenção no espaço cibernético. Contudo, esses protocolos, por si só, não garantem a segurança da conexão. Configurações erradas na implementação das cifras utilizadas pelos protocolos somadas a um elevado poder computacional da inteligência de sinais e cibernética da força inimiga podem comprometer a segurança da comunicação.

Esse trabalho buscou revisar protocolos de segurança de rede e cifras de criptografia e avaliar o risco de sua utilização baseado no poder computacional e nos ataques publicamente conhecidos com a finalidade de propor uma adequada utilização de meios não convencionais de comunicações militares para se estabelecer uma comunicação com garantia de confidencialidade, autenticidade e integridade, a partir de uma área sob controle do inimigo, sem revelar a posição do elemento de forças especiais (FEsp) infiltrado na AOGI.

1.1 PROBLEMA

A distância geográfica entre a AOGI e a BOBFEsp impõe o estabelecimento de uma estrutura de comando e controle de longo alcance. O contato inicial é uma fase da guerra irregular na qual a Eq Prec FEsp terá de utilizar meios não convencionais para estabelecer comunicações com seu elemento de comando e controle e tramitar informações, algumas vezes, ultrassecretas. Uma alternativa para o estabelecimento desse comando e controle é a utilização da rede mundial de computadores, a Internet, com a criptografia adequada.

A criptografia moderna trouxe uma ampla gama de cifras simétricas e assimétricas. Quase em sua totalidade, essas cifras são garantidas por segurança computacional (alguns autores se referem como segurança matemática). Esse modelo de segurança é baseado em problemas matemáticos que exigem um grande poder computacional para que um atacante possa decifrar a mensagem, podemos citar como exemplo a cifra assimétrica *RSA*, que tem sua segurança baseada na dificuldade da fatoração do produto de dois grandes números primos ou a cifra Diffie-Hellman que se baseia na resolução de logaritmos discretos. Desta forma, a segurança de sistemas que utilizam essas cifras está diretamente relacionada com o poder computacional da força inimiga.

1.1.1 **Antecedentes do Problema**

Nas últimas décadas, Estados têm ampliado sua capacidade de criptoanálise investindo em supercomputadores, computação distribuída e em pesquisas para desenvolvimento do computador quântico. Tal capacidade é mantida em sigilo, o que dificulta mensurar o poder computacional da força

inimiga e, consequentemente, avaliar corretamente a segurança das nossas comunicações.

Em 1949, um estudo de Claude Shannon definiu que cifras similares a One-Time Pad são teoricamente seguras. Isso significa que, diferente do que ocorre com a ampla maioria dos esquemas de segurança baseados em troca de chave por cifra assimétrica – que são computacionalmente seguros –, uma mensagem cifrada por One-Time Pad não pode ser decifrada, independente do poder computacional do atacante, a menos que se obtenha a chave. Porém, para garantir a segurança, a mesma chave não pode ser utilizada mais de uma vez. Isso resulta em uma quantidade limitada de dados que podem ser transmitidos em um esquema One-Time Pad, uma vez que o remetente e o destinatário da mensagem deverão possuir um número pré-estabelecido de chaves para tramitar suas mensagens e não poderão gerar novas chaves.

A necessidade de estabelecimento prévio de uma chave muito grande faz com que a One-Time Pad seja uma cifra impraticável para a maioria dos propósitos das aplicações na Internet. Contudo, em operações militares, onde as frações que serão desdobradas encontram-se inicialmente reunidas com seu elemento de comando e controle, é possível pré-estabelecer chaves de forma segura antes do desdobramento, fazendo com que a cifra *one-time pad* seja uma solução viável para a segurança.

Desta forma temos o seguinte dilema no cenário de segurança das comunicações nos dias de hoje: de um lado a cifra One-Time Pad pode garantir uma segurança plena contra ataques clássicos, sejam analíticos ou de força bruta, porém é de difícil implementação; de outro lado as cifras computacionalmente seguras são de implementação menos complexa, contudo, devido as evoluções dos recursos de tecnologia da informação, requerem constante avaliação do poder computacional do inimigo, o qual quase sempre é estimado e não confirmado.

1.1.2 **Formulação do Problema**

A partir do cenário exposto, formulou-se o seguinte problema de pesquisa: **como estruturar uma implementação com criptografia adequada para estabelecer comunicação segura para tramitar dados ultrassecretos através da Internet a partir de um território controlado pelo inimigo?**

1.2 OBJETIVOS

1.2.1 **Objetivo Geral**

Propor uma implementação com criptografia adequada para estabelecer comunicação segura para tramitar dados ultrassecretos através da Internet a partir de um território controlado pelo inimigo.

1.2.2 **Objetivos Específicos**

Com a finalidade de delimitar e alcançar o desfecho esperado para o objetivo geral, foram levantados objetivos específicos que conduziram à consecução do objetivo deste estudo, os quais são transcritos abaixo:

a) Revisar sumariamente a cifra AES;
b) Revisar sumariamente a cifra RSA;
c) Revisar sumariamente a cifra Diffie-Hellman;
d) Revisar sumariamente a cifra One-Time Pad;
e) Identificar os ataques mais eficientes conhecidos para comprometer sistemas de segurança conectados a Internet e as recomendações de segurança para impedi-los.
f) Calcular o tempo de execução de um ataque genérico sobre a troca de chaves Diffie-Hellman utilizando o algoritmo Baby-Step Giant-Step em um PC i7-10510U;
g) Estimar, comparando a capacidade de realização de operações de ponto flutuante por segundo (FLOPS), o tempo de execução de um ataque genérico sobre a troca de chaves Diffie-Hellman utilizando o algoritmo Baby-Step Giant-Step em um supercomputador publicamente conhecido;
h) Identificar o tamanho necessário de chave para um esquema baseado em One-Time Pad proteger chamadas de voz em Operações Especiais.

1.3 QUESTÕES DE ESTUDO

a) As cifras computacionalmente seguras estão suscetíveis a ataques

desencadeados por supercomputadores?

b) A cifra One-Time Pad oferece vantagem prática sobre as cifras computacionalmente seguras considerando o poder computacional conhecido hoje?
c) A implementação da cifra One-Time Pad nas Operações Especiais é viável?

1.4 JUSTIFICATIVA

Segurança das comunicações é um dos mais antigos assuntos de interesse das ciências militares. Através de casos documentados observa-se a importância da transmissão secreta de mensagens desde a Grécia antiga até os dias de hoje.

> There are documented cases of secret writing in ancient Greece, namely the scytale of Sparta, or the famous Caesar cipher in ancient Rome. (PAAR e PELZL, 2010, p. 2).[1]

Durante a Segunda Guerra Mundial, Alan Turing e sua equipe em Bletchley Park, decifravam as mensagens alemães cifradas pela máquina Enigma garantindo superioridade de informações para os Aliados. Sobre isso, Kerrigan (2020, p. 23) afirma que “no sentido mais estritamente técnico, as informações sobre mensagens (signals intelligence, SIGINT) se tornaram centrais na espionagem moderna”.

De acordo com o Manual de Campanha EB70-MC-10.212 (Operações Especiais), um dos fatores de êxito para as operações especiais é a “adequada estrutura de comando e controle” (BRASIL, 2017, p. 23). O Manual de Campanha EB20-MC-10.205 (Comando e Controle) define estrutura de comando e controle da seguinte forma:

> Conjunto de centros de comando e controle, subordinados a um mesmo comandante, que contém os **recursos adequados e perfeitamente configurados** para o fluxo das ordens e das informações para o exercício do comando, podendo ser estabelecida em nível nacional, de teatro de operações, de comando combinado ou em nível tático (BRASIL, 2015, p. 15, grifo nosso).

[1] Existem casos documentados de escrita secreta na Grécia antiga, chamada Cítala Espartana, ou a famosa Cifra de César na Roma antiga (tradução nossa).

Diante do exposto, observa-se que recursos de criptografia adequados e perfeitamente configurados para garantir a segurança das comunicações são essenciais para uma adequada estrutura de comando e controle e, consequentemente, compõem os fatores de êxito das operações especiais. A presente pesquisa buscou revisar sistemas de criptografia que podem ser utilizados pelo Comando de Operações Especiais (COpEsp), tendo em vista a constante evolução dos algoritmos de segurança da informação, e avaliar a utilização da cifra one-time pad como possibilidade de inovação para a segurança das comunicações ultrassecretas.

Sendo assim esse estudo se justifica pela importância do estudo da criptografia para alcançar a superioridade de informações, quer seja protegendo nossos ativos, quer seja obtendo informações protegidas, e se mostra alinhado com o Objetivo Estratégico do Exército (OEE) 1.1.1.3 que versa sobre “Reestruturar o Comando de Operações Especiais e modernizar Sistemas de Emprego Militar” no que tange a Capacidade Militar Terrestre superioridade de informações. Satisfaz, ainda, o OEE 4.2.1.5 ao propor adequações a estrutura de proteção cibernética de parte das redes e sistemas do Comando de Operações Especiais.

Esta pesquisa poderá, ainda, ser aproveitada por outros pesquisadores de segurança da informação mesmo que estejam fazendo pesquisas diversas às operações especiais.

2. REVISÃO DA LITERATURA

2.1 GUERRA IRREGULAR

De acordo com o Manual de Campanha EB70-MC-10.212 (Operações Especiais), guerra irregular é

> Conflito armado executado por forças não regulares ou por forças regulares empregadas fora dos padrões normais da guerra regular, contra um governo estabelecido ou um poder de ocupação, com o emprego de ações típicas da guerra de guerrilhas. Divide-se em: guerra insurrecional, guerra revolucionária e guerra de resistência (BRASIL, 2017, pg. 100).

As fases da guerra irregular são: preparação psicológica, contato inicial, infiltração, organização, expansão, emprego em combate, desmobilização (BRASIL, 2020, p. 15). Dentro da fase denominada contato inicial, a equipe precursora de forças especiais (Eq Prec FEsp) infiltra na área operacional de guerra irregular (AOGI) com o objetivo de estabelecer contato com representantes de uma organização de força irregular. A partir daí verificar a viabilidade da guerra irregular, realizar avaliação de área detalhada e subsidiar o planejamento da operação respondendo necessidades de inteligência (BRASIL, 2020, p. 34).

2.1.1 **A equipe precursora de forças especiais no contato inicial**

Segundo Verrastro (1993, p. 32) as principais missões da Eq Prec FEsp no contato inicial são: estabelecimento de contato com lideranças locais, visualização de prováveis componentes do Comando de Área, exfiltrar especialistas para elucidar dúvidas dos planejadores se for possível, levantar zonas de lançamento ou áreas de infiltração para o destacamento operacional de forças especiais (DOFEsp), levantar necessidades de inteligência com oportunidade para o DOFEsp, preparar comitê de recepção para a infiltração do DOFEsp, organizar e participar da segurança para a infiltração do DOFEsp, guiar o DOFEsp até a área de homizio, realizar a apresentação do DOFEsp e assessorá-lo nos primeiros contatos com os líderes locais.

Observa-se que a maioria das missões atribuídas à Eq Prec FEsp nessa fase só poderá ser cumprida com o estabelecimento de uma adequada estrutura de comando e controle com grande observância no que tange a segurança das comunicações uma vez que o enlace ocorre entre o interior de um território negado com uma Base de Operações Especiais (BOE) que pode estar na zona do interior ou junto ao Posto de Comando do Comando Operacional Conjunto. Quando mobiliada por quadros do 1º Batalhão de Forças Especiais (1º B F Esp), a BOE ou Base de Coordenação Avançada (BCA) é denominada Base de Operações do Batalhão de Forças Especiais (BOBFEsp).

Segundo o Manual de Campanha C 24-50 Segurança das Comunicações:

> Segurança das comunicações é a proteção que resulta de todas as medidas destinadas a não permitir ou a dificultar a obtenção, pelo inimigo ou por pessoas não autorizadas, de informe de valor militar, procedentes das comunicações (BRASIL, 1978, p. 1-2).

Com relação ao local onde a Base de Operações Especiais será estabelecida (ver figura 2), o Manual de Campanha EB70-MC-10.305 (O Comando de Operações Especiais) define que:

> O B Ap Op Esp é o responsável por estruturar a Base de Operações Especiais (BOE), estrutura logística e de Comando e Controle (C^2) das Operações Especiais, que interage com a cadeia logística singular ou conjunta existente, **dentro TO/A Op ou mesmo na zona de interior (ZI)** (BRASIL, 2019, p. 5-9, grifo nosso).

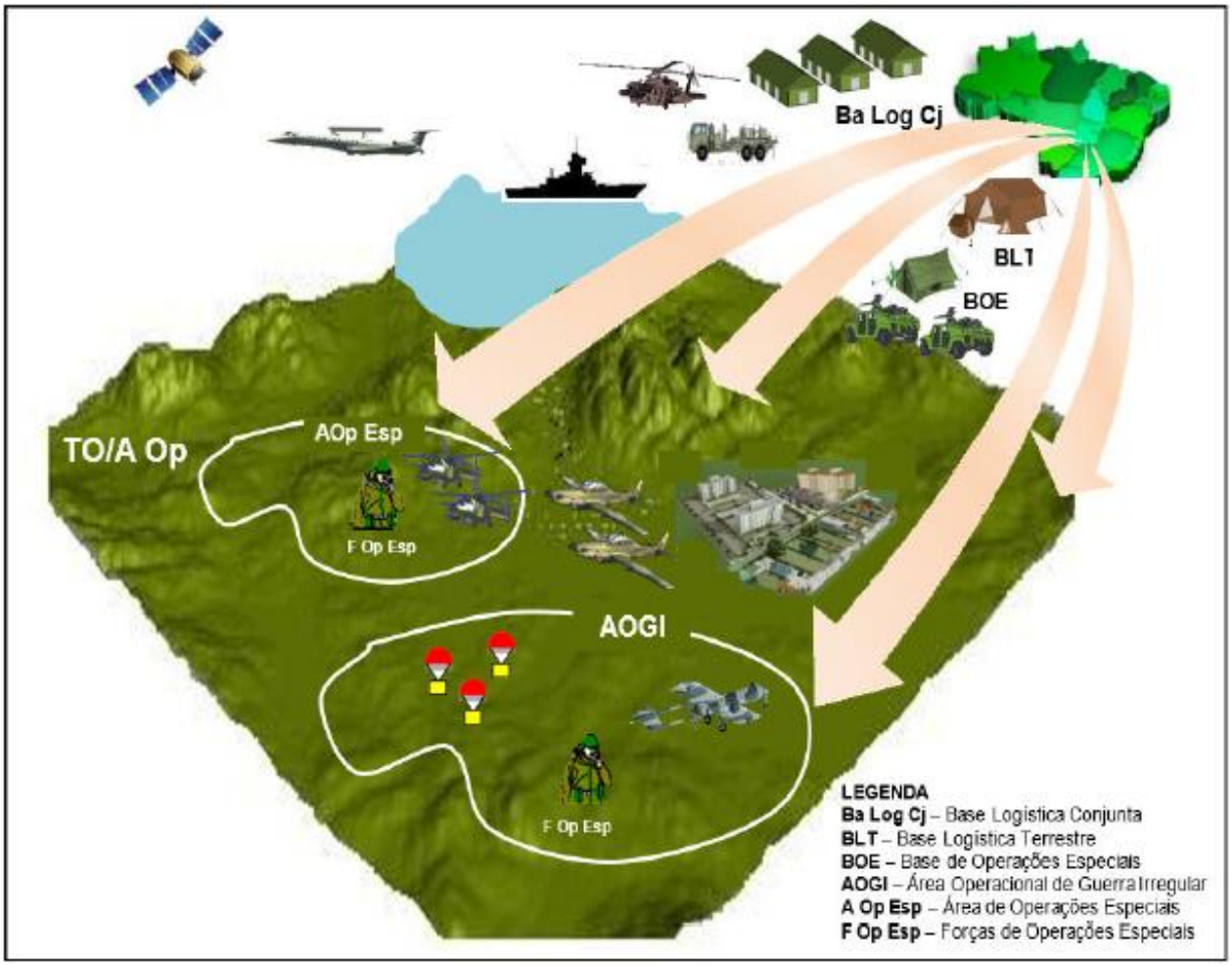


FIGURA 2 – Desdobramento das Forças de Operações Especiais
Fonte: BRASIL (2017, p. 5-10)

A doutrina norte americana de unconventional warfare (UW), termo utilizado para se referir a guerra irregular[*], é semelhante a doutrina brasileira de guerra irregular (ver faseamento da UW na figura 3)

.

[*] Observa-se que o termo "irregular warfare" na doutrina norte americana se refere a todas as operações que o USSOCOM é capaz de desempenhar, enquanto que o termo "unconventional warfare", abreviado UW, refere-se ao conjunto de atividades relacionadas ao desenvolvimento de um movimento de resistência ou uma insurgência. Dessa forma o termo análogo a guerra irregular é unconventional warfare e não irregular warfare.

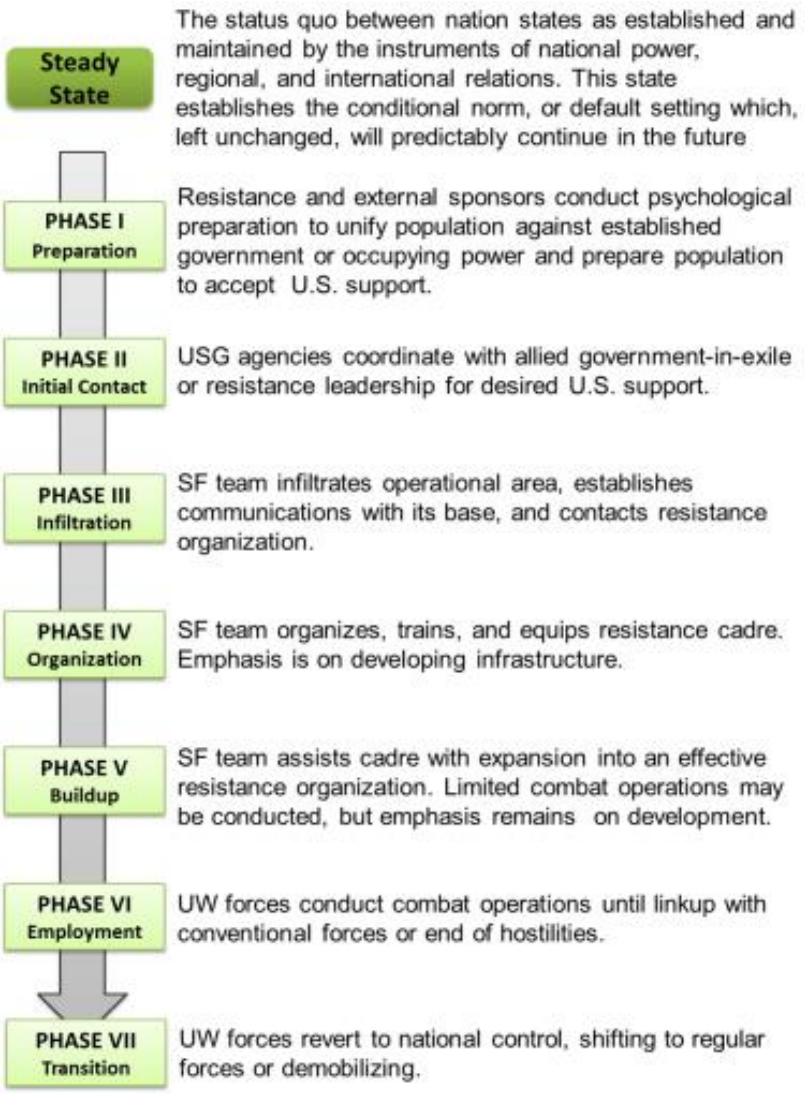


FIGURA 3 – Faseamento da guerra irregular segundo a doutrina norte americana
FONTE: EUA (2016, p. 10)

Após o onze de setembro, durante as operações de contraterrorismo no Afeganistão, os destacamentos de forças especiais norte americanos realizaram, dentre outras operações especiais, ação indireta, que segundo o Manual de Campanha EB70-MC-10.212 (Operações Especiais):

> Consiste na **organização, desenvolvimento, equipagem, instrução, direção e/ou assessoramento** de forças irregulares, regulares, auxiliares e de atores estatais e não estatais, para a consecução de objetivos políticos, econômicos, psicossociais e/ou militares em situação de guerra e de não guerra. As ações indiretas são realizadas por integrantes das forças especiais (BRASIL, 2017, p. 3-6, grifo nosso)

Naquela ocasião, a força irregular a ser dirigida era a Aliança do Norte, grupo paramilitar que oferecia resistência ao Talibã. O Talibã por sua vez é um grupo paramilitar, que, segundo os EUA, estaria protegendo Osama Bin Laden, responsável pelo ataque terrorista nos EUA em 11 de setembro de 2001.

Observa-se que, apesar de a operação ter se desenvolvido no escopo de contraterrorismo, para realizar as ações indiretas, fases da guerra irregular foram planejadas e executadas.

Com relação ao contato inicial com as lideranças da Aliança do Norte, Jorge explana:

> O plano de ação da CIA apontava para o uso de uma equipe paramilitar da própria agência e aviões não-tripulados Predador dentro do Afeganistão, para trabalhar com as forças de oposição ao Talebã, especialmente a Aliança do Norte, e **preparar o terreno para a inserção das Forças Especiais** do Exército norte-americano. A CIA vinha operando no Afeganistão há um bom tempo – ao menos desde que os soviéticos estiveram lá nos anos 1980. A CIA conhecia as tribos, os grupos étnicos, os líderes, a cultura e, em algum nível, os idiomas, e também quem iria e quem não iria cooperar com os EUA (JORGE, 2009, p. 33).

Stone, traz um relato semelhante:

> CIA paramilitary operatives entered Afghanistan on 26 September 2001 **ahead of U.S. Special Operations Forces (SOF) in order to link up with Northern Alliance forces, secure helicopter landing zones for follow-on SOF, and guide SOF teams** – who arrived with their arsenal of laser target designators to enable U.S. aircraft to strike Taliban positions – to the enemy. These CIA officers were inserted ahead of the SOF because of their ability to get on the ground quickly, their language skills and knowledge of the terrain, and their existing contacts with anti-Taliban groups (STONE, 2003, p. 2, grifo nosso).[2]

[2] Operadores paramilitares da CIA entraram no Afeganistão em 26 de setembro de 2001 antes das Forças de Operações Especiais (F Op Esp) para fazer contato com as forças da Aliança do Norte, assegurar uma zona de pouso de helicóptero segura para receber as F Op Esp e guiar as F Op Esp – que chegaram com seu arsenal de designadores lasers para viabilizar o ataque de aeronave nas posições do Talibã – até o inimigo. Esses oficiais da CIA foram inseridos antes das F Op Esp devido a sua capacidade de infiltrar mais rápido, suas habilidades linguísticas e conhecimento do terreno, e seus contatos prévios com grupos anti-Talibã (tradução nossa).

É notório que esses relatos apontam grande semelhança entre as atividades que foram desenvolvidas por oficiais da Central Intelligence Agency (CIA) e as missões da Eq Prec FEsp no contato inicial segundo Verrastro.

Conclui-se que os EUA optaram por evitar o emprego de meios militares no contato inicial buscando realizar ações com o mínimo de visibilidade nessa fase da operação. Cabe ressaltar que a CIA é uma agência governamental que em sua origem absorveu quadros e atribuições do extinto Office of Strategic Services (OSS), unidade de guerra irregular homóloga a unidade britânica Special Operations Executive (SOE), ambas empregadas na Segunda Guerra Mundial para fomentar movimentos de resistência, realizar propaganda e sabotagem. Dessa forma, além das atividades de obtenção e análise de dados, cabe a CIA atividades denominadas “covert actions” que o National Security Act of 1947 do Senado dos EUA define da seguinte forma:

> ‘‘covert action’’ means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly (EUA, p. 84, 1947)[3]

Com relação as considerações sobre o comando e controle na guerra irregular a Nota de Aula NA 2-7 (Guerra Irregular) expõe o seguinte:

> 3.4-1 **O DOFEsp não pode se comunicar com a BOBFEsp da mesma maneira que em outros tipos de operações**. Mesmo que os meios e as possibilidades de contato estejam facilitados, o destacamento deve ter muito cuidado antes de colocar qualquer mensagem no espectro eletromagnético dentro do território inimigo. Ao contrário de unidades convencionais, as organizações de GI sempre se arriscam com algum grau de exposição a cada contato. O DOFEsp **não deve confundir a criptografia nas comunicações com baixa assinatura eletrônica**. O DOFEsp deve equilibrar o desejo do Cmt da FCjOpEsp em briefings baseados em computadores e comunicações em tempo real com as limitações do ambiente operacional. Para isso, sempre devem operar sob a **suposição de que o inimigo está tentando localizar a sua posição**,

[3] “ação coberta” é a atividade ou atividades do governo dos EUA para influenciar condições políticas, econômicas ou militares no exterior, onde se entende que o o papel do governo dos EUA não será aparente ou conhecido publicamente (tradução nossa).

> crescendo de importância a utilização das Comunicações Sigilosas em áreas urbanas e rurais.
>
> 3.4-2 Antes da infiltração na AOGI o DOFEsp deve considerar se sua assinatura irá comprometer a missão e **se há um meio mais adequado no interior da AOGI que pode beneficiar as comunicações internas e externas**. As operações de GI apresentam desafios únicos por causa da negação da presença de tropa que possua níveis de equipamento e adestramento incompatíveis com as ações evidenciadas pelas Forças de Guerrilha. Assim, mesmo com a utilização das medidas normais de proteção eletrônica (MPE), os contatos externos devem ser evitados. O DOFEsp pode atenuar, no interior da AOGI, alguns aspectos de risco através de boas medidas de segurança operacional e exploração das comunicações sigilosas. (BRASIL, 2020, p. 40, grifo nosso)

Diante da dificuldade de a Eq Prec FEsp manter sua presença oculta da força inimiga, deve ser avaliado, mediante exame de situação, o emprego de estória-cobertura, de forma a descaracterizar o pessoal e material militar, optando, nesse caso, pelo emprego de meios não convencionais. Segundo a Nota de Aula NA 2-7 (Guerra Irregular), “esta descaracterização pode permitir que os integrantes do DOFEsp possam se misturar com as forças irregulares e impedir sua identificação pelo inimigo” (BRASIL, 2020, p. 66).

2.2 A INTERNET

Segundo Kurose e Ross

> A Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de computação ao redor do mundo. [...] há muitos tipos de enlaces de comunicação, que são constituídos de diferentes tipos de meios físicos, entre eles cabos coaxiais, fios de cobre, fibras óticas e ondas de rádio (KUROSE e ROSS, 2013, p. 3).

Tal definição é ilustrada na figura 4.

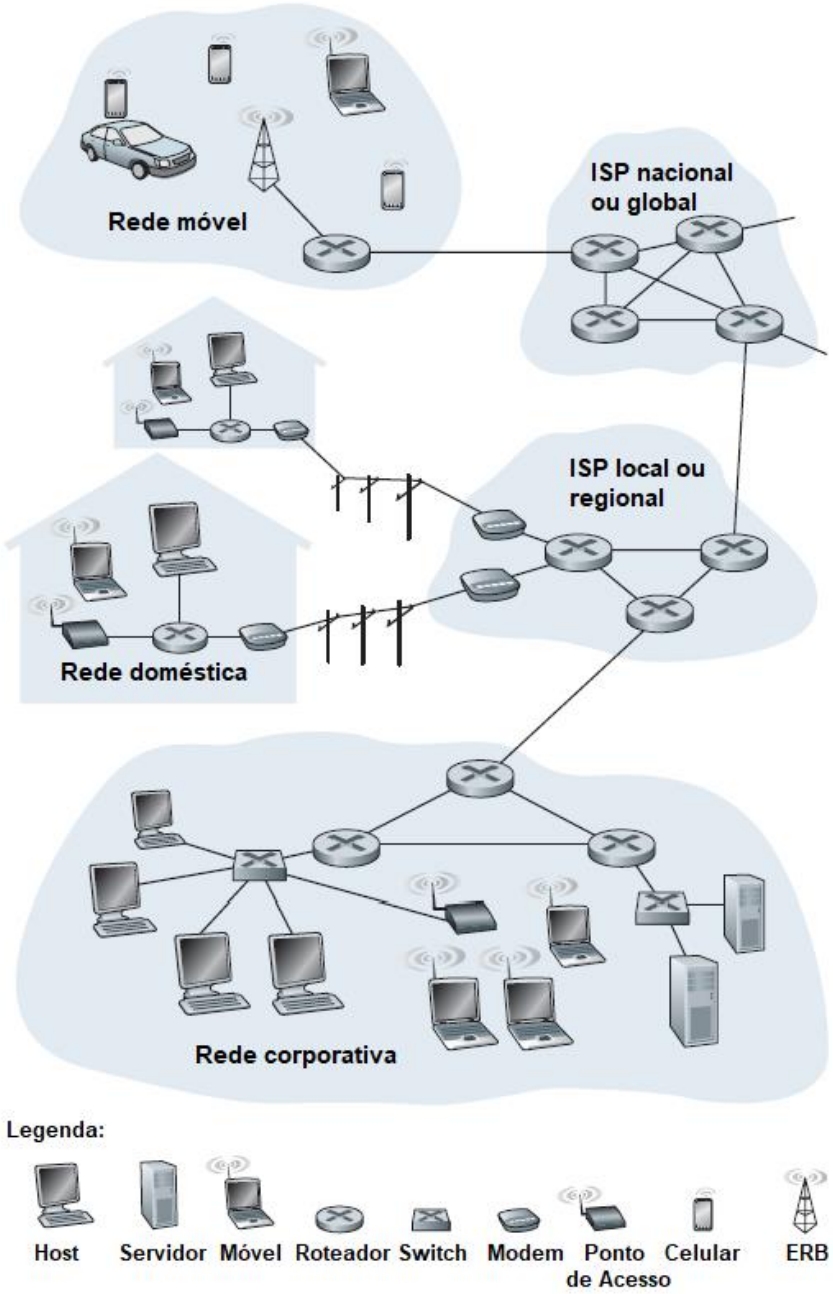


FIGURA 4 – Extrato da Internet
Fonte: Kurose e Ross (2013, p. 2)

A Internet oferece infraestrutura adequada para o enlace, inclusive com medidas de redundância (caminhos alternativos para o tráfego de dados entre dois dispositivos finais).

Segundo os índices de rede levantados pela CISCO, em 2009, o tráfego de dados na internet atingiu uma média de 15 exabytes* por mês (CISCO, 2010, p. 1). Esse grande volume de dados trafegando na internet, diferente do que ocorre no espectro eletromagnético, não permite uma ação de busca baseada

* 1 exabyte = 1.000.000.000 gigabytes

somente no suposto aumento de tráfego de dados gerado pelo enlace entre a Eq Prec FEsp e a BOBFEsp. Para realizar uma ação de busca será necessário analisar algum outro aspecto, como por exemplo: endereço lógico utilizado pela BOBFEsp, endereço lógico utilizado pela Eq Prec FEsp, rota de comutadores que estabelece o enlace, localização da Eq Prec FEsp, localização da BOBFEsp, dentre outros.

Contudo, como a infraestrutura da Internet é dependente de diversos dispositivos intermediários que encaminham os dados através do Internet Protocol (IP), a utilização de criptografia é essencial para que se garanta a confidencialidade dos dados e que não se permita a alteração dos dados por nenhum dispositivo intermediário. Sendo esse um problema comum para diversas aplicações que utilizam a Internet, grande parte dos dados trafegados são criptografados. Dessa forma, utilizando a criptografia correta, os pacotes de dados da Eq Prec FEsp e da BOBFEsp não destoarão dos demais pacotes de dados que já trafegam na Internet.

2.2.1 **A Internet em camadas: modelo OSI**

Em 1984, a International Organization for Standardization (ISO) lançou o modelo Open Systems Interconnection (OSI), que estabeleceu camadas (ver figura 5) sob as quais os protocolos de rede utilizados pela Internet estão organizados.

Conforme publicado na norma ISO/IEC 7498-1 de 1994:

> O propósito desse Modelo de Referência de Interconexão de Sistemas Abertos é fornecer uma base comum para a coordenação de padrões de desenvolvimento para fins de interconexão de sistemas, enquanto permite que os padrões existentes sejam colocados em perspectiva dentro do Modelo de Referência geral (ISO/IEC, 1994, tradução nossa).

FIGURA 5 – Camadas do modelo OSI
Fonte: Elias e Lobato (2013, p. 48)

As camadas do modelo OSI são numeradas de 1 a 7 a partir da camada física até a camada de aplicação. Essa pesquisa terá o foco sobre medidas de segurança que podem ser implementadas nas camadas 3 (Rede), 4 (Transporte) e 6 (Apresentação).

O IP Security (IPSec) e p Transport Layer Security (TLS) são protocolos desenvolvidos para prover segurança a partir da camada de rede e detransporte respectivamente, segundo Alshamsi e Saito, são as mais robustas e potenciais ferramentas para a segurança das comunicações na Internet (2004, p. 1).

2.2.2 **Encapsulamento de dados**

Segundo Elias e Lobato, encapsulamento de dados é o “processo que assegura a correta transferência e recuperação de dados – Protocol Data Unit (PDU)” (Elias e Lobato, 2013, p. 54).

O encapsulamento de dados segue o modelo OSI. Nesse processo, cada camada adiciona aos dados seu cabeçalho, que contém informações de controle utilizadas pelo protocolo. Em seguida, a camada atual passa o pacote

consolidado (chamado PDU) para a camada inferior fazer o mesmo. A figura 6 ilustra o processo de encapsulamento de dados.

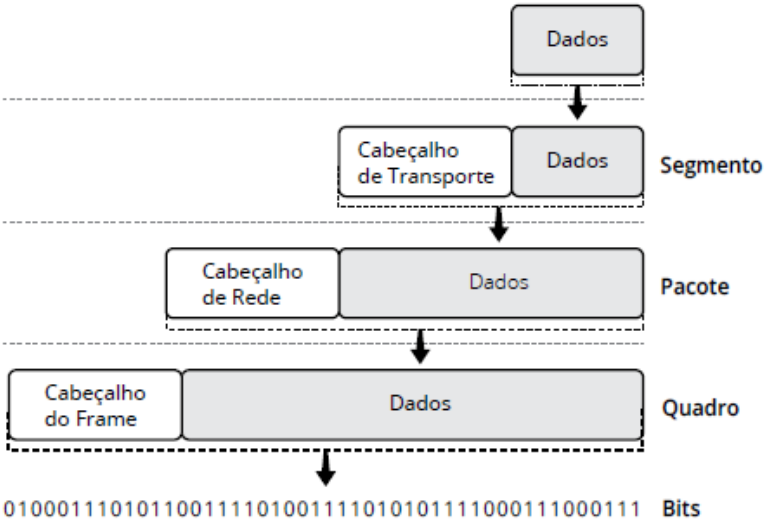


FIGURA 6 – Encapsulamento de dados no modelo OSI
Fonte: Elias e Lobato (2013, p. 55)

2.2.3 **Roteamento de pacotes através do Internet Protocol (IP)**

De acordo com Kurose e Ross, “roteamento refere-se ao processo de âmbito geral da rede que determina os caminhos fim a fim que os pacotes percorrem desde a origem até o destino” (KUROSE e ROSS, 2013, p. 225).

Esse processo ocorre na camada 3 (Rede) do modelo OSI.

> A camada de rede da Internet é responsável pela movimentação, de um hospedeiro para outro, de pacotes da camada de rede, conhecidos como **datagrama**. O protocolo de camada de transporte da Internet (TCP ou UDP) em um hospedeiro de origem passa um segmento da camada de transporte e um endereço de destino à camada de rede, exatamente como você passaria ao serviço de correios uma carta com um endereço de destinatário. A camada de rede então provê o serviço de entrega do segmento à camada de transporte no hospedeiro de destino. Essa camada inclui o famoso protocolo IP [...] (KUROSE e ROSS, 2013, p. 38).

O endereço IP é um endereço lógico que, segundo Elias e Lobato (2013) identifica a estação do usuário na rede, identifica a rede física e é roteável entre as redes físicas. A figura 7 faz uma comparação entre o protocolo IP e um sistema de envio de correspondências.

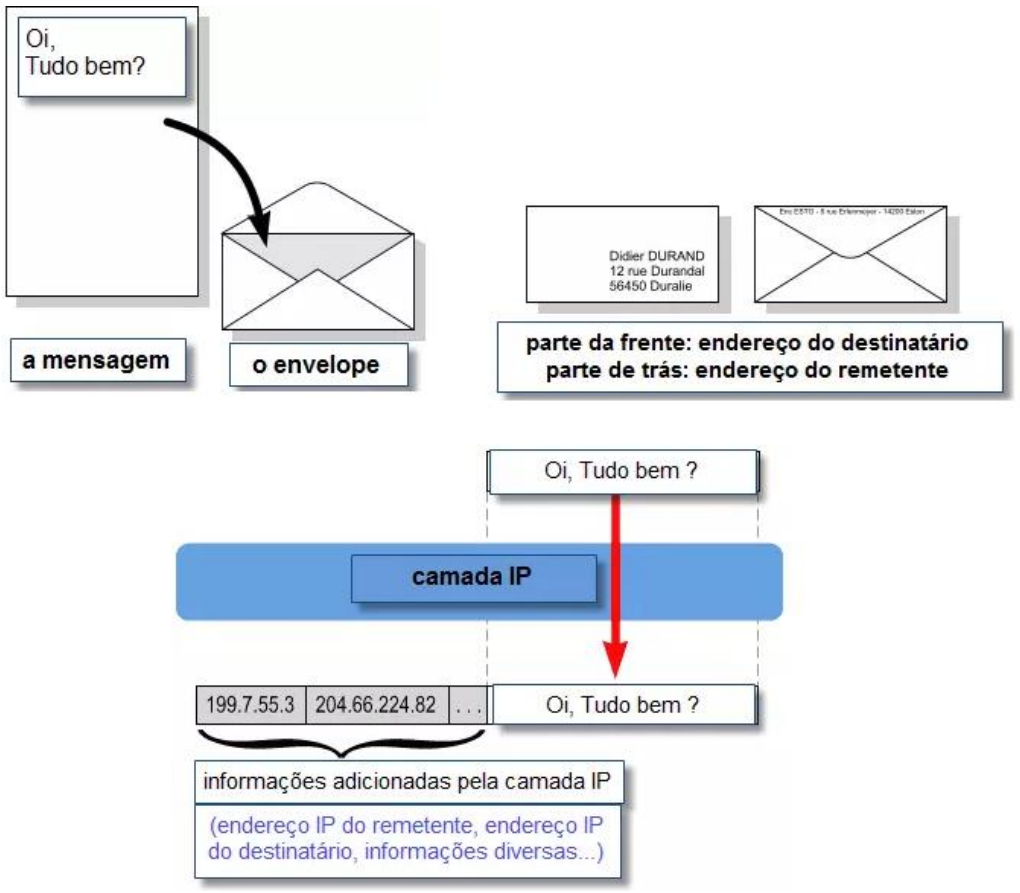


FIGURA 7 – Comparação entre o protocolo IP e um sistema de envio de correspondências
Fonte: CCM.net (2020)

Para fins de avaliação de segurança da Eq Prec FEsp e da BOBFEsp, deve-se observar que o endereço lógico do remetente e do destinatário constarão no pacote que estará sendo encaminhado pela rede. Sendo os endereços IP distribuídos pela Internet Assigned Numbers Authority (IANA) – e redistribuídos por instâncias inferiores – conforme orientação geográfica, é possível delimitar a localização de um dispositivo conectado a Internet através de seu endereço lógico. Assim sendo, a Eq Prec FEsp e a BOBFEsp deverão utilizar medidas para que seu tráfego de dados não seja classificado como suspeito pelas ações de busca da força inimiga e, a partir daí, sua localização comece a ser levantada.

2.3 SEGURANÇA DAS COMUNICAÇÕES

Conforme destacado no subitem 2.1.1, o Manual de Campanha C 24-50 (Segurança das Comunicações) traz a seguinte definição:

> Segurança das comunicações é a proteção que resulta de todas as medidas destinadas a não permitir ou a dificultar a obtenção, pelo inimigo ou por pessoas não autorizadas, de informe de valor militar, procedentes das comunicações (BRASIL, 1978, p. 1-2).

O Manual de Campanha EB70-MC-10.232 (Guerra Cibernética) traz uma definição atualizada, em concordância com princípios da norma ISO/IEC 27001 de 2013.

> SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC) – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações (BRASIL, 2017, p. 19).

> O sistema de gestão de segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação aplicando um processo de gerenciamento de risco e dá confiança às partes interessadas que os riscos estão adequadamente gerenciados (ISO/IEC, 2013, tradução nossa).

De acordo com Green,

> Criptografia é forte na teoria, mas na prática é propensa a falhas como qualquer outro aspecto de um sistema de segurança. Isso ocorre especialmente quando implementações criptográficas são desenvolvidas por não especialistas sem experiência e cuidado suficiente, como é o caso de muitos sistemas criptográficos empregados hoje (GREEN, 2018, p. XV, tradução nossa).

Em concordância, o Manual de Campanha C 24-50 (Segurança das Comunicações) expõe:

> Os sistemas criptográficos são elaborados por elementos especializados. Erro muito grave, que compromete a segurança, é o emprego de códigos e cifras improvisadas por subordinados e sem autorização do comando superior. Estas iniciativas dão aos seus criadores **falsa noção de segurança**, pois na quase totalidade são de fácil interpretação pelo inimigo. [...] **Todos os meios de comunicações são suscetíveis de interceptação pelo inimigo**, uns mais do que outros. **É a situação que vai indicar qual o meio mais seguro**, no momento, para se transmitir determinada mensagem (BRASIL, 1978, p. 2-7, grifo nosso).

Com relação a classificação de informações, o Exército Brasileiro considera os graus de sigilo: reservado, secreto e ultrassecreto, os quais as Instruções Gerais para Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011) definem da seguinte forma:

> I - a informação de grau de sigilo ULTRASSECRETO é aquela cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave, tal como a referente a (à):
> a) soberania e à integridade territorial nacionais;
> b) relações internacionais do País;
> c) plano e operação militar que afetem as letras “a” e “b” do presente inciso;
> d) projeto de pesquisa e desenvolvimento científico e tecnológico de interesse da Defesa Nacional; e
> e) programa econômico.
>
> II - a informação de grau de sigilo SECRETO é aquela cujo conhecimento não autorizado possa acarretar dano grave, tal como a referente a (à):
> a) sistema;
> b) instalação;
> c) programa;
> d) projeto;
> e) plano ou operação de interesse da Defesa Nacional;
> f) assunto diplomático e de Inteligência; e
> g) plano ou seus detalhes.
>
> III - a informação de grau de sigilo RESERVADO é aquela cujo conhecimento não autorizado possa acarretar dano, tal como a que frustre ou comprometa:
> a) objetivo de interesse do Poder Executivo;
> b) objetivo ou atividade de interesse do Comando do Exército; e
> c) plano, operação ou objetivo nele previsto ou referido. (BRASIL, 2014, p. 12)

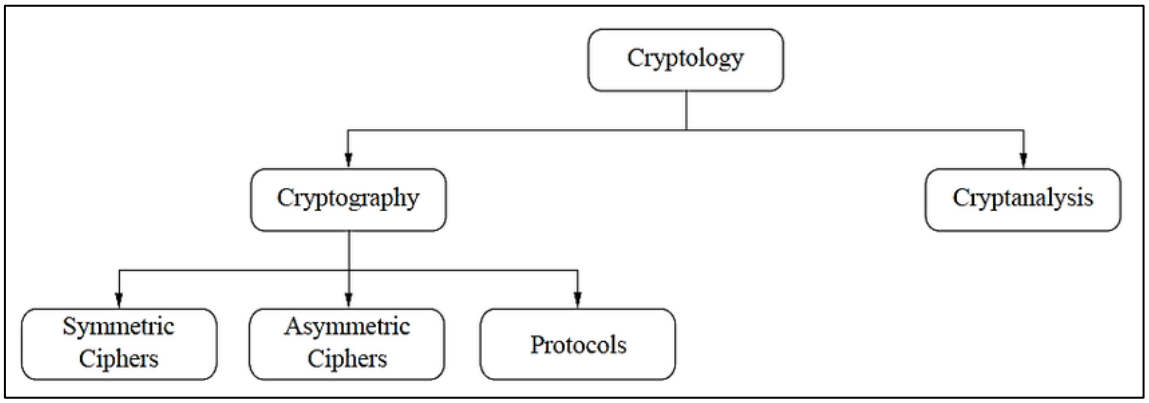
Desta forma, observa-se que as informações que serão tratadas em comunicações da Eq Prec FEsp com a BOBFEsp durante a fase de contato inicial da guerra irregular poderão ser eventualmente classificadas como ultrassecretas ou reservadas, normalmente classificadas como secretas. Em consequência, o nível de segurança dessas comunicações deverá ter condições de garantir a salvaguarda de informações ultrassecretas.

Ainda segundo as Instruções Gerais para Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011) sobre os prazos para restrição de acesso de material classificado:

> Art. 8º Os prazos máximos de restrição de acesso à informação classificada vigoram na data de sua produção e são os seguintes:
> I - para o grau de sigilo ULTRASSECRETO: 25 (vinte e cinco) anos;
> II - para o grau de sigilo SECRETO: 15 (quinze) anos; e
> III - para o grau de sigilo RESERVADO: 5 (cinco) anos. (BRASIL, 2014, p. 12)

2.3.1 **Criptologia**

Paar e Pelzl definem criptografia como “a ciência da escrita secreta com a finalidade de esconder o significado da mensagem” (2010, p. 3, tradução nossa) e criptoanálise como a “ciência e algumas vezes a arte de *quebrar* sistemas criptográficos” (2010, p. 3, tradução nossa). Definem, ainda, criptologia como o termo geral do qual derivam essas duas ciências (Paar e Pelzl, 2010, p. 3), conforme organograma 1.

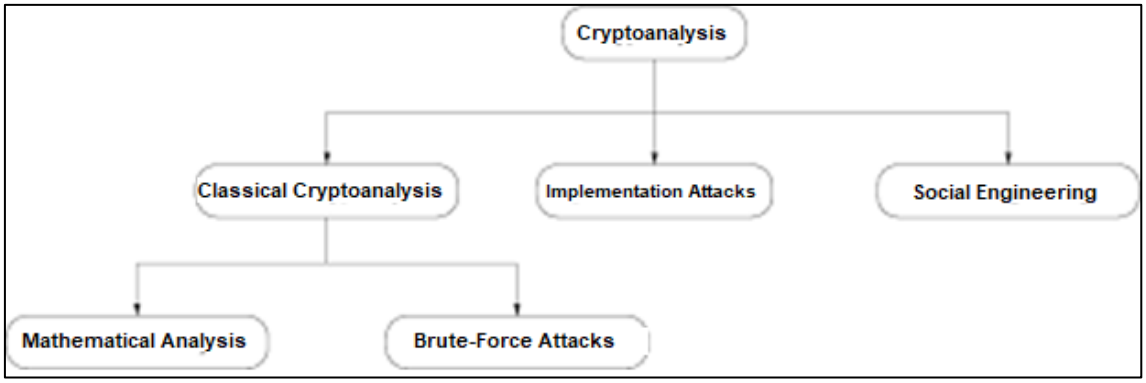


ORGANOGRAMA 1 – Criptologia
Fonte: Paar e Pelzl (2010, p. 3)

Com relação aos ramos da criptografia, Aumasson afirma que cifra simétrica “é o tipo mais simples de encriptação. Na encriptação simétrica, a chave usada para decriptar é a mesma chave usada para encriptar” (2018, p. 1, tradução nossa). Sobre a cifra assimétrica, Aumasson afirma que “a chave usada para decriptar é diferente da chave usada para encriptar” (2018, p. 1, tradução nossa). Já protocolos criptográficos, conforme Paar e Pelzl, “lidam com a aplicação de algoritmos criptográficos. Algoritmos simétricos e assimétricos podem ser vistos como blocos de construção com os quais aplicações como comunicações seguras na Internet podem ser realizadas” (2010, p. 3, tradução nossa).

2.3.2 **Cifras computacionalmente seguras e poder computacional do atacante**

Dentro do escopo da criptoanálise existem diferentes abordagens para atacar uma cifra criptográfica. No organograma 2 estão as possíveis abordagens.



ORGANOGRAMA 2 – Criptoanálise
Fonte: Paar e Pelzl (2010, p.10)

Segundo Paar e Pelzl, criptoanálise clássica “é a ciência de recuperar o texto em claro x a partir do texto cifrado y, ou, alternativamente, recuperar a chave k a partir do texto cifrado y” (2010, p. 10, tradução nossa).

O ataque de Força-Bruta, segundo Aumasson, é definido por “tentar todas as chaves até que você encontre a correta” (2018, p. 41, tradução nossa). Na cifra AES onde a chave pode ter 256 bits isso significa tentar 2^{256} possibilidades. Segundo Paar e Pelzl esse ataque levaria várias décadas mesmo para computadores quânticos utilizando os algoritmos conhecidos (2010, p. 12), isso

faz com que a cifra AES utilizando uma chave de 256 bits seja considerada computacionalmente segura (ver quadro 1).

Ataques de implementação são referidos por Paar e Pelzl como ataques de canal lateral (termo conhecido em inglês: side-channel attack). Tratam-se de ataques a partir da aferição de sinais como: consumo de energia elétrica, radiação eletromagnética, tempo de processamento, dentre outros, desde que o atacante tenha acesso físico ao dispositivo onde o sistema criptográfico está implementado.

Engenharia social é um tipo de ataque no qual “truques ou espionagem clássica envolvendo humanos podem ser utilizados para se obter uma chave secreta” (Paar e Pelzl, 2010, p. 10, tradução nossa).

Tam. da chave	**Estimativa de segurança**
56-64 bits	Curto prazo: poucas horas ou dias
112-128 bits	Longo prazo: várias décadas na ausência de computador quântico
256 bits	Longo prazo: várias décadas mesmo com computadores quânticos utilizando os algoritmos de computação quântica conhecidos

QUADRO 1 – Tempo estimado para ataque de força bruta bem sucedido sobre cifra simétrica
Fonte: Paar e Pelzl (2010, p. 12, tradução nossa)

Observamos que a cifra simétrica AES 256 garante segurança contra ataques de força bruta. Além disso, “atualmente não há ataque analítico **conhecido** contra o AES” (Paar e Pelzl, 2010, p. 116, tradução nossa, grifo nosso).

Contudo, toda cifra simétrica enfreta o problema da distribuição de chave.

> A chave deve ser estabelecida entre Alice e Bob usando um canal inseguro. Lembre-se que o enlace de comunicação para a mensagem não é seguro, então enviar a chave através desse canal diretamente – o que deve ser a forma mais conveniente de transportar a chave – não pode ser feito (PAAR e PEZLZ, 2010, p.150, tradução nossa).

Com base nesse e em outros problemas que as cifras simétricas não são capazes de lidar, foram desenvolvidas as cifras assimétricas, as quais utilizam um par de chaves. A chave pública é utilizada para criptar a mensagem, enquanto que a chave privada é utilizada para decriptar.

Dessa forma, as cifras assimétricas passaram a complementar as cifras simétricas. As cifras assimétricas são utilizadas – dentre outras aplicações – para estabelecer uma chave, a partir daí as cifras simétricas utilizam a chave estabelecida (tendo em vista que são cifras de mais rápida execução, pois exigem menos processamento).

"Existem só três famílias de algoritmos de chave-pública que são de relevância prática. Podem ser classificadas com base nos seguintes **problemas computacionais**: fatoração de inteiros, logaritmo discreto e curvas elípticas" (Paar e Pelzl, 2010, p. 155, tradução nossa, grifo nosso).

O quadro 2 define o nível de segurança de cifras simétricas e assimétricas com base no comprimento da chave.

Algoritmo	Cifra	Nível de Segurança (bits)			
		80	128	192	256
Fatoração de inteiros	RSA	1024 bits	3072 bits	7680 bits	15360 bits
Logaritmo discreto	DH, DSA, Elgamal	1024 bits	3072 bits	7680 bits	15360 bits
Curvas elípticas	ECDH, ECDSA	160 bits	256 bits	384 bits	512 bits
Chave simétrica	AES, 3DES	80 bits	128 bits	192 bits	256 bits

QUADRO 2 – Comprimento da chave para diferentes níveis de segurança
Fonte: Paar e Pelzl (2010, p. 156, tradução nossa)

O quadro acima está em concordância com as recomendações de comprimento de chave do National Institute of Standards and Technology (NIST), com a ressalva de que as cifras de algoritmos de curvas elípticas estão com a observação de que a força da sua segurança irá mudar significativamente quando a computação quântica for uma consideração prática (EUA, 2020).

Cabe ressaltar que "a relação entre força criptográfica e segurança não é tão direta no caso assimétrico" (PAAR e PEZLZ, 2010, p. 156, tradução nossa). A descoberta de um algoritmo na computação clássica ou quântica que resolva esses problemas computacionais em menos tempo poderá expor a segurança dessas cifras. Além disso, uma vez que a chave simétrica é dependente da segurança da chave assimétrica nesse sistema amplamente utilizado na Internet, a exposição da chave assimétrica coloca em risco toda a comunicação.

Deve-se levar em consideração, ainda, a lei de Moore que desde 1965 tem sido satisfatória em prever que a capacidade de processamento dobra, aproximadamente, a cada 18 meses (MOORE, 1965). Esse desenvolvimento

tecnológico é relevante para a criptologia uma vez que torna obsoletos em pouco tempo hardwares e implementações de criptografia e criptoanálise baseados na segurança computacional. Além disso, desenvolvimentos na área da criptologia como, por exemplo, a melhoria de algoritmos, podem tornar implementações criptográficas obsoletas antes mesmo dos efeitos esperados pela lei de Moore.

Tendo em vista que o poder computacional de criptoanálise de um Estado costuma ser informação sigilosa, conclui-se, então, que o grande desafio para garantir a segurança das comunicações utilizando modelos criptográficos baseados em segurança computacional é conseguir mensurar o poder computacional da força inimiga para utilizar o nível de criptografia adequado.

2.3.3 **Cifra teoricamente segura: one-time pad**

A one-time pad “é a mais segura cifra. De fato, ela garante pefeito sigilo: **mesmo se um atacante possuir ilimitado poder computacional**, é impossível aprender algo sobre o texto em claro exceto o seu tamanho” (AUMASSON, 2018, p. 7, tradução nossa, grifo nosso).

Em 1949 Claude Shannon publicou um artigo chamado “Communication Theory of Secrecy Systems”, no qual ele provou que todas as cifras teoricamente seguras (inquebráveis) devem ter as mesmas características da cifra one-time pad (SHANNON, 1949). Essas características, segundo Paar e Pelzl são três: a chave precisa ter o mesmo comprimento da mensagem, a chave precisa ser totalmente aleatória, a chave não poderá ser utilizada novamente em outra mensagem (2010, p. 37).

A cifra one-time pad é uma cifra simétrica de fluxo que utiliza a operação exclusive or (XOR). “A operação XOR cumpre um importante papel na criptografia moderna” (PAAR e PELZL, 2010, p. 33). Isso ocorre devido a ser uma operação bit a bit completamente reversível (ver quadro 3) sendo assim muito usada nas funções de cripto e decripto. A operação XOR resulta 1 toda vez que os dois bits comparados forem diferentes e resulta 0 toda vez que forem iguais. Observe no quadro 3 que se compararmos o texto em claro plaintext (PT) com a chave K obteremos o texto criptografado ciphertext (CT), se fizermos o inverso e compararmos CT com K obteremos PT, daí sua relevância para criptografia.

PT	K	CT
0	0	0
0	1	1
1	0	1
1	1	0

QUADRO 3 – Operação XOR
Fonte: Paar e Pelzl (2010, p. 33)

Observa-se que um ataque de força bruta a um texto que foi cifrado com uma chave do mesmo tamanho da mensagem em claro é um ataque impossível, uma vez que, ainda que existisse poder computacional para verificar todas as possibilidades, ao executar o ataque o atacante se depararia com todas as formações de texto possíveis para aquele número de caracteres e jamais poderia concluir qual solução de fato corresponde a mensagem em claro. O quadro 4 ilustra tal situação citada. Supondo um texto em claro “EXERCITO” e a chave “aolsrfgr” resultando no texto cifrado “$7)!1/3=”. Ao realizar um ataque de força bruta o atacante encontrará, dentre os demais resultados, o susposto texto em claro “ONE_TIME” para a chave “kyl~ef~x”. De posse desse resultado o atacante pode ser induzido a crer que encontrou o texto protegido, uma vez que o termo “ONE_TIME” é um termo conhecido, mas estará errado, pois o texto protegido nesse exemplo é “EXERCITO”. Isso é uma demonstração de que a cifra *one-time pad* não é vulnerável a ataques analíticos ou de força bruta.

Uma mensagem criptografada com One-Time Pad pelas forças amigas:								
PT (mensagem protegida)	E	X	E	R	C	I	T	O
K (chave utilizada)	a	o	L	S	r	f	G	r
CT (mensagem criptografada)	$	7	)	!	1	/	3	=
Um possível resultado errado encontrado através de ataque de força bruta da força inimiga:								
CT interceptado	$	7	)	!	1	/	3	=
K (chave da força bruta)	k	y	L	~	e	f	~	x
PT suposto (errado)	O	N	E	_	T	I	M	E

QUADRO 4 – Exemplo de força bruta mal sucedida sobre One-Time Pad
Fonte: O autor

Esse é um exemplo do que Shannon provou: não é possível fazer um ataque de força bruta uma vez que o tamanho da chave seja igual ao tamanho da mensagem (SHANNON, 1949), pois todos os resultados serão possíveis.

Isso prova que one-time pad é a cifra mais segura em termos computacionais, uma vez que sua segurança está baseada na teoria da comunicação de sistemas secretos, proposta por Shannon, e não na teoria dos números.

Contudo o grande desafio da implementação da one-time pad é a quantidade de memória que se gasta com a chave (para criptografar um arquivo de 1 gigabyte seria necessária uma chave de 1 gigabyte), e a construção de uma chave verdadeiramente aleatória – que não seja baseada em algoritmos pseudo aleatórios, dos quais o atacante poderia se beneficiar sabendo quais são os parâmetros utilizados para a pseudoaleatoriedade.

Dessa forma a cifra one-time pad se tornou impraticável para a maioria das aplicações da Internet, visto que não é viável que todos os usuários da Internet se reunam fisicamente para estabelecer trocas de chaves por um canal seguro antes de iniciar uma conexão remota. A outra solução seria fazer trocas de chaves utilizando cifras assimétricas para utilizar one-time pad, porém isso dobraria o volume de tráfego de dados da Internet uma vez que a chave tem o mesmo tamanho do conteúdo a ser criptografado e a segurança teórica da one-time pad estaria reduzida a segurança computacional da cifra assimétrica. Assim, as cifras simétricas de bloco se mostraram solução mais adequada para a necessidade de segurança do usuário da Internet.

Concluímos, no entanto, que para aplicações militares a cifra one-time pad pode ser uma alternativa adequada, uma vez que antes das tropas serem desdobradas estão reunidas e, assim, podem estabelecer chaves por meio de um canal seguro. Sendo o desafio para essa implementação a segurança do armazenamento da chave nos dispositivos conduzidos pela Eq Prec FEsp em território controlado pelo inimigo.

2.3.4 **Advanced Encryption Standard (AES), a cifra Rijndael**

Segundo Paar e Pelzl, o Advanced Encryption Standard (AES) é a cifra simétrica mais usada nos dias de hoje. Apesar do termo “standard” (padrão) no nome da cifra referir-se apenas a um padrão estabelecido para aplicações

governamentais dos Estados Unidos, a cifra de bloco AES é também obrigatória em vários padrões industriais e é usada em muitos sistemas comerciais. Entre os padrões comerciais que incluem AES estão o padrão de segurança da Internet IPSec, TLS, o padrão de criptografia Wi-Fi IEEE 802.11i, SSH, Skype e diversos produtos de segurança pelo mundo (2010, p. 87).

Em 1997, o National Institute of Standards and Technology (NIST) fez uma convocação para propostas de um novo Advanced Encryption Standard (AES) – Padrão de Criptografia Avançado. Em três etapas subsequêntes de avaliação do AES, o NIST e a comunidade científica internacional discutiram as vantagens e desvantagens das cifras que foram apresentadas como candidatas. Em 2001 – após cinco anos de concurso –, o NIST declarou a cifra Rijndael como novo AES. Rijndael foi desenvolvida por dois jovens criptógrafos belgas (Paar e Pelzl, 2010, p. 88).

A figura 8 ilustra uma rodada da cifra AES.

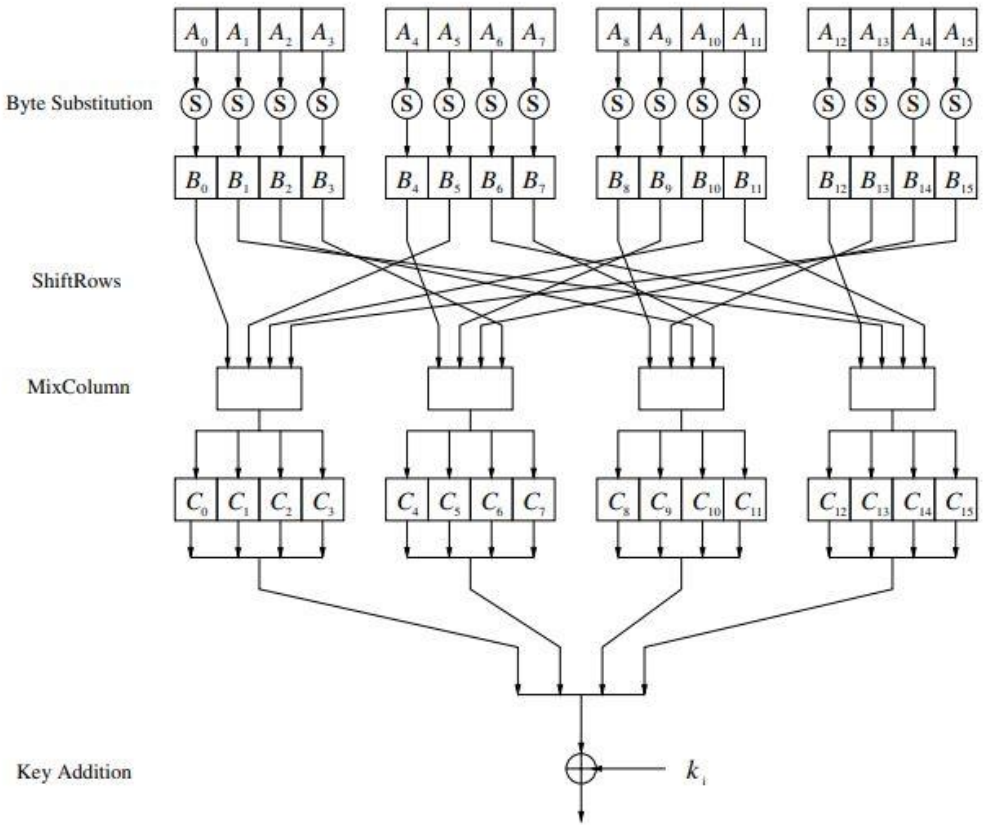
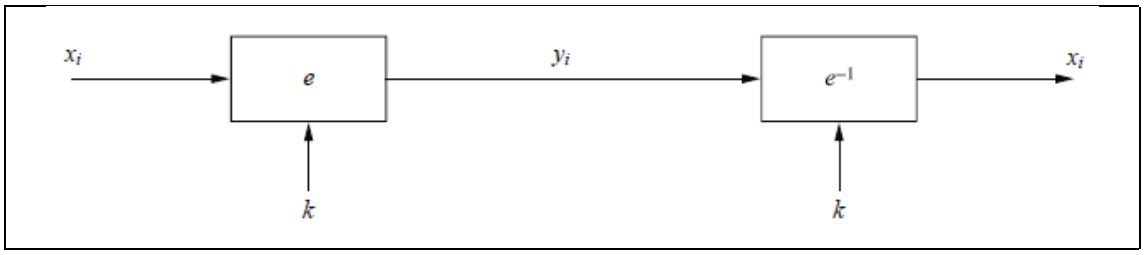


FIGURA 8 – Rodada AES
FONTE: Paar e Pelzl (2010, p. 100)

Segundo Paar e Pelzl, AES tem sido estudado intensamente desde o final da década de 90 e **ainda não foi encontrado um ataque melhor do que a força bruta** (2010, p. 117, grifo nosso).

Contudo, não se deve utilizar o modo de operação *Electronic Code Book* (ECB), revisado no quadro 5, para concatenar os blocos cifrados por AES, uma vez que a utilização da mesma chave em todos os blocos, independente do dado cifrado resultante do bloco anterior, resulta que dados em claro idênticos serão sempre criptografados em dados cifrados idênticos, gerando uma grande vulnerabilidade principalmente na transmissão de imagens, conforme figura 9 (Paar e Pelzl, 2010, p. 127). Em vez disso, recomenda-se a utilização de outro modo de operação como por exemplo o *Cipher Block Chaining* (CBC), revisado no quadro 6.



QUADRO 5 – Encriptação e decriptação no modo ECB
Fonte: Paar e Pelzl (2010, p. 125)

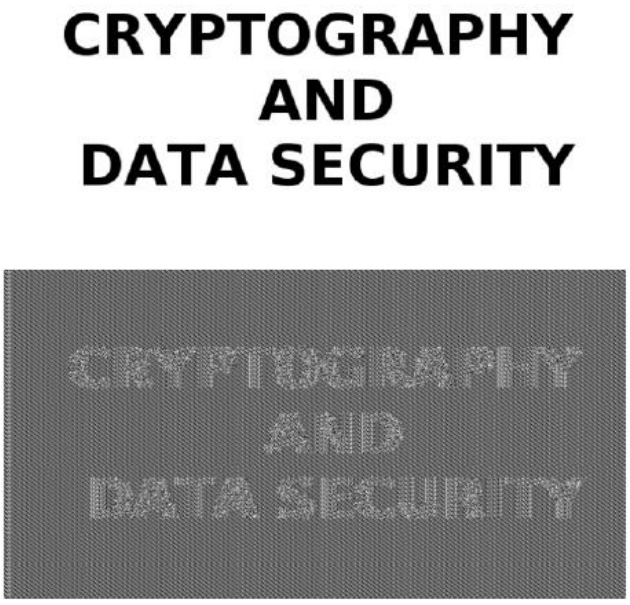
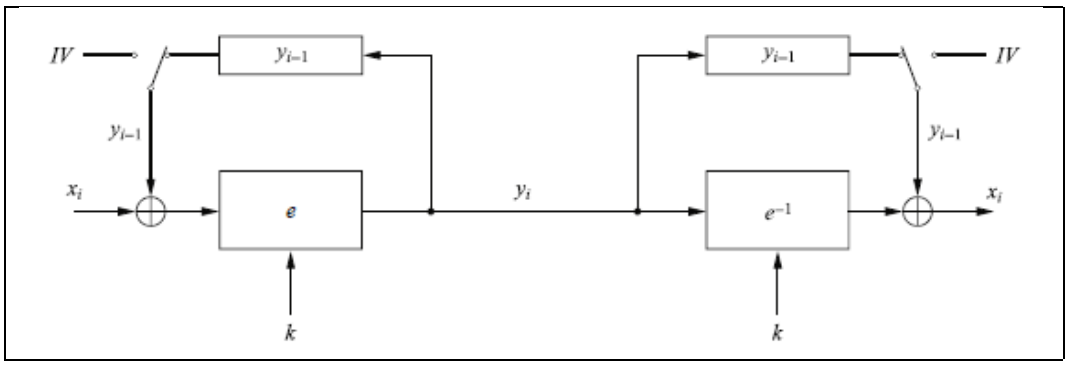


FIGURA 9 – Imagem em claro e encriptada utilizando AES 256 ECB
Fonte: Paar e Pelzl (2010, p. 127)



QUADRO 6 – Encriptação e decriptação no modo CBC
Fonte: Paar e Pelzl (2010, p. 128)

2.3.5 **Cifra assimétrica: criptografia de chave pública**

As cifras simétricas são de rápido processamento, porém se faz necessário um canal seguro para negociar a chave que será utilizada entre os pares que estão se comunicando. As cifras assimétricas complementam as cifras simétricas na Internet, pois apesar de serem computacionalmente mais lentas, seu esquema de chave pública e chave privada permite uma negociação de chave através um canal de comunicação inseguro e esta chave passará a ser utilizada então por uma cifra simétrica como o AES. A segurança das cifras assimétricas é baseada em problemas matemáticos de difícil resolução, tais como fatoração de grandes inteiros ou logarítimos discretos, por isso diz-se que as cifras assimétricas são **matematicamente** seguras.

2.3.5.1 Diffie-Hellman

A troca de chaves Diffie-Hellman, proposta por Whitfield Diffie e Martin Hellman em 1976, foi o primeiro esquema assimétrico publicado em literatura aberta. Os desenvolvedores foram influenciados pelo trabalho de Ralph Merkle. Esse esquema forneceu uma solução prática para o problema de distribuição de chave, isto é, permitiu que dois pares compartilhassem uma chave secreta comum através de um canal de comunicação inseguro (Paar e Pelzl, 2010, p. 206).

A idéia por trás do Diffie-Hellman é que a exponenciação no conjunto $\mathbb{Z}^*_p$ – conjunto dos números primos inteiros diferentes de zero – é uma função de uma via e essa exponenciação é comutativa (Paar e Pelzl, 2010, p. 206). Esse

fundamento que dá base ao Diffie-Hellman está representado na fórmula do quadro 7.

$k = (\alpha^x)^y \equiv (\alpha^y)^x \bmod p$

QUADRO 7 – Ideia base por trás da troca de chaves Diffie-Hellman
Fonte: Paar e Pelzl (2010, p. 206)

Na prática, primeiramente será escolhido um grande número primo p e então um número inteiro $\alpha \in \{2, 3, ..., p - 2\}$. Esses valores (p e α) são conhecidos como parâmetros de domínio e são compartilhados entre os pares que estão estabelecendo a comunicação. Feito isso, cada par escolherá uma chave privada $k_{pr} \in \{2, 3, ..., p - 2\}$ e calculará uma chave pública $k_{pub} \equiv \alpha^{Kpr} \bmod p$. Após troca das chaves públicas, cada par calculará a chave que será utilizada na comunicação elevando a chave pública recebida à potência da sua chave privada, desta forma ambos os pares terão chegado a mesma chave sem tê-la exposto no canal inseguro pelo qual a comunicação está sendo estabelecida, conforme exemplo no quadro 8 no qual foram utilizados parâmetros de valores muito baixos para fins didáticos.

Considere os parâmetros de domínio p = 29 e α = 2		
Alice		**Bob**
Escolhe $a = k_{pr,A} = 5$		Escolhe $b = k_{pr,B} = 12$
$A = k_{pub,A} = 2^5 \equiv 3 \bmod 29$		$B = k_{pub,B} = 2^{12} \equiv 7 \bmod 29$
	$A=3$ →	
	← $B=7$	
$k_{AB} = B^a \equiv 7^5 = 16 \bmod 29$		$k_{AB} = A^b = 3^{12} \equiv 16 \bmod 29$

QUADRO 8 – Exemplo de estabelecimento de chave com Diffie-Hellman
Fonte: Paar e Pelzl (2010, p. 207, tradução nossa)

Conforme AUMASSON, a troca de chave Diffie Hellman anônima pode ser facilmente comprometida caso um atacante na situação de *man-in-the-middle* se passa por Bob para Alice ao mesmo tempo que se passa por Alice para Bob (2018, p. 209), conforme ilustrado na figura 9.

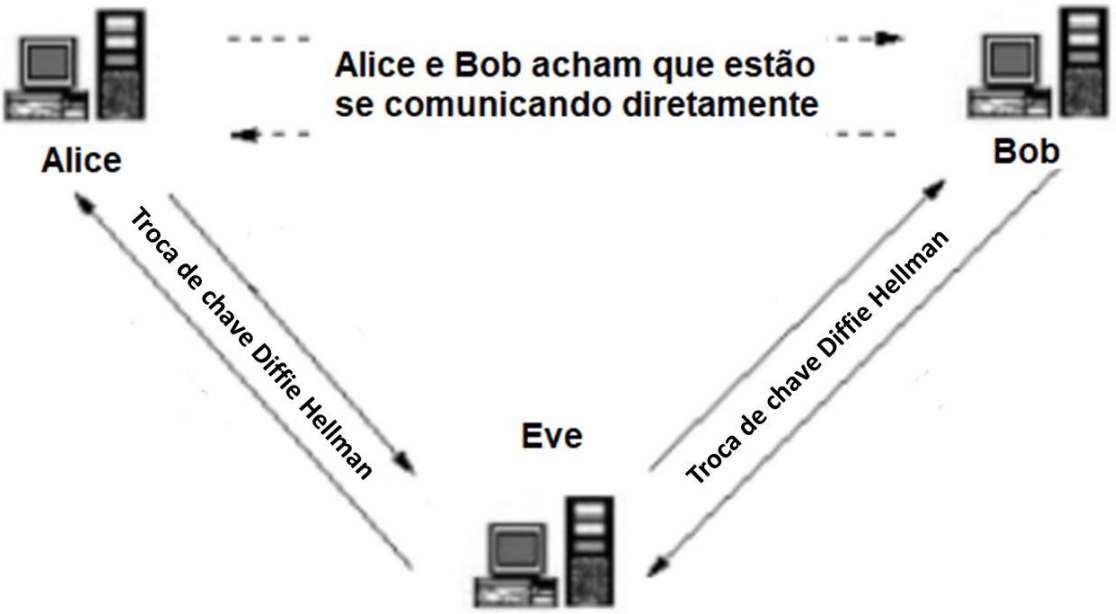


FIGURA 10 – Ataque Man-In-The-Middle sobre troca de chave Diffie Hellman anônima
Fonte: Adaptado de <https://commons.wikimedia.org/wiki/File:Man-in-the-middle_attack.png>, acesso em 21 de ago. de 2022.

Para impedir esse ataque é necessário ter uma forma de autenticar as partes. Diffie Hellman autenticada foi desenvolvida para evitar esse ataque utilizando um esquema de assinaturas como RSA-PSS (*RSA Public-key signature scheme)* (AUMASSON, 2018, p. 210).

Conforme publicado por Lim e Lee, o módulo P de uma troca de chave Diffie Hellman não deve permitir a existência de subgrupos, para tal (P – 1) / 2 deve ser um número primo. Se o módulo P atender a essa premissa dizemos que P é um primo seguro (LIM e LEE, 1997, p. 15).

Observadas as considerações supracitadas na troca de chave Diffie Hellman, restará ao atacante na condição de man-in-the-middle registrar os parâmetros de domínio P e α e o volume de dados criptografados transmitidos na conversa entre Alice e Bob para posterior tentativa de criptoanálise. Daí surge o conceito de *Forward Secrecy* (sigilo futuro), que, segundo AUMASSON, é a garantia de que mesmo que os segredos de longo prazo sejam expostos, segredos compartilhados em outras execuções do protocolo não serão comprometidos (2018, p. 207). Diffie Hellman autenticada provê sigilo futuro baseado em um esquema efêmero de troca de chaves – novas chaves são trocadas, por exemplo, a cada conexão.

Desta forma, caso o atacante obtenha êxito na criptoanálise obterá apenas um trecho da conversa entre Alice e Bob. Para realizar essa criptoanálise o atacante disporá de algoritmos genéricos (que servem para atacar qualquer módulo P) ou algoritmos não genéricos (que servem para atacar um esquema que utiliza um número primo específico, o qual o atacante já tem dados pré computados para viabilizar o ataque). A exemplo de algoritmo genérico de ataque temos o Baby-Step Giant-Step de Daniel Shanks (PAAR e PELZL, 2010, p. 221), e a exemplo de algoritmo não genérico temos o *Number Field Sieve* (NFS), utilizado por Adrian et al para provar que esquemas de segurança com módulos P de 512 bits podem ser comprometidos e estimar que com recursos a nível de Estado a *National Security Agency* (NSA - agência governamental norte americana de inteligência de sinais) poderia comprometer módulos P de 1024 bits (ADRIAN et al, 2015).

2.3.5.2 RSA

Após a introdução da cifra desenvolvida por Whitfield Diffie e Martin Hellman em 1976, surgiu uma nova área de estudo para a criptografia: a criptografia de chave pública, também conhecida como cifra assimétrica. Em 1977, Ronald Rivest, Adi Shamir e Leonard Adleman propuseram um esquema que se tornou a cifra assimétrica mais usada do mundo, o RSA (Paar e Pelzl, 2010, p. 173).

Existem várias aplicações para o RSA, porém na prática ele é mais usado para transportar chaves e para assinaturas digitais. É importante notar que o RSA não tem a intenção de substituir cifras simétricas por ser muito mais lento do que cifras como o AES. Isso se deve a grande necessidade de processamento na aplicação do RSA (assim como em toda cifra assimétrica). Na prática, RSA é utilizado em conjunto com uma cifra simétrica, como o AES. (Paar e Pelzl, 2010, p. 174).

O quadro 9 ilustra como são geradas as chaves RSA.

Gerar chave RSA

Saída: chave pública: $k_{pub} = (n, e)$ e chave privada: $k_{pr} = (d)$

1. Escolher dois grandes primos p e q.
2. Calcular $n = p \cdot q$
3. Calcular $\Phi(n) = (p - 1)(q - 1)$
4. Selecionar um expoente público $e \in \{1, 2, \ldots, \Phi(n) - 1\}$ tal que
$$mdc(e, \Phi(n)) = 1$$
5. Calcular a chave a chave privada d tal que
$$d \cdot e \equiv \mod \Phi(n)$$

QUADRO 9 – Gerar chave RSA
Fonte: Paar e Pelzl (2010, p. 176, tradução nossa)

Os quadros 10 e 11 ilustram, respectivamente, a função de encriptar e decriptar utilizando RSA

.

Encriptar com RSA: Dada a chave pública $(n, e) = k_{pub}$ e o texto em claro x, a função encriptar é dada por:

$$y = e_{Kpub}(x) \equiv x^e \mod n$$

Onde $x, y \in Z_n$

QUADRO 10 – Encriptar com RSA
Fonte: Paar e Pelzl (2010, p. 174, tradução nossa)

Decriptar com RSA: Dada a chave privada $d = k_{pr}$ e o texto cifrado y, a função decriptar é dada por:

$$x = d_{Kpr}(y) \equiv y^d \mod n$$

Onde $x, y \in Z_n$

QUADRO 11 – Decriptar com RSA
Fonte: Paar e Pelzl (2010, p. 175, tradução nossa)

3. METODOLOGIA

Com o intuito de se chegar à resposta do problema formulado, foi realizada uma pesquisa bibliográfica sobre livros, trabalhos acadêmicos e publicações relacionadas a criptologia a fim de identificar os protocolos de rede, as cifras e os tamanhos de chave que proporcionam maior segurança, e os ataques mais eficientes conhecidos contra esquemas de criptografia.

Foi realizada, ainda, uma pesquisa laboratorial para estimar a capacidade de um Estado comprometer a segurança de uma troca de chave Diffie-Hellman com um algoritmo de ataque genérico. Para isso, foi utilizado um computador com processador i7-10510U para realizar um ataque genérico utilizando o algoritmo Baby-Step Giant-Step sobre a troca de chaves Diffie-Hellman. Os resultados obtidos foram utilizados para se estimar o desempenho de supercomputadores realizando o mesmo ataque. Para realizar essa estimativa foram comparadas as capacidades de realização de operações de ponto flutuante por segundo (FLOPS) entre o PC utilizado no experimento e o supercomputador constante da lista pública Top500. Comparamos o tempo de execução estimado para a quebra da segurança com o prazo de restrição de acesso à informação ultrassecreta constante das Instruções Gerais para Salvaguarda de Assuntos Sigilosos (IGSAS) do Exército Brasileiro para concluir se tal esquema seria ou não adequado para tramitar dados ultrassecretos.

Avaliamos a frequência de repetição de números primos de 1024 bits gerados pela biblioteca OpenSSL para concluir a eficiência dessa biblioteca contra ataques não genéricos sobre a troca de chaves Diffie-Hellman em um esquema efêmero.

Levantamos o volume de dados em bytes tramitados em uma ligação VoIP para concluir se é viável a utilização de aplicações VoIP baseadas em One-Time Pad nas operações especiais.

3.1 OBJETO FORMAL DE ESTUDO

Esta pesquisa teve como objeto formal de estudo a segurança das comunicações através da Internet, verificada por meio das variáveis definidas e operacionalizadas da seguinte forma:

TIPO	VARIÁVEL	DIMENSÃO	INDICADOR	FORMA DE MEDIÇÃO
Dependente	Segurança da Comunicação	Confidencialidade	A partir do texto cifrado não é possível obter o texto em claro com oportunidade	Tempo para quebra da cifra com melhor ataque conhecido é maior do que validade do dado ultrassecreto
		Autenticidade	Não é possível elemento não autorizado se passar por elemento autorizado	Utiliza ou não sistema de autenticação que inviabilize ataque Man-In-The-Middle
		Integridade	Não é possível um elemento intermediário no canal de comunicação inserir ou retirar dados da mensagem original sem ser identificada alteração	Utiliza ou não função hash segura
Independente	Segurança do AES	Confidencialidade	A partir do texto cifrado não é possível obter o texto em claro com oportunidade	Tempo estimado para comprometer a segurança do esquema é maior do que validade do dado ultrassecreto (baseado em experimento e pesquisa bibliográfica)
	Segurança do RSA		A partir da chave pública não é possível obter a chave privada com oportunidade	
	Segurança da troca de chaves Diffie-Hellman			
	Viabilidade do One-Time Pad nas Op Esp	Armazenamento seguro da chave	Tamanho da chave compatível com dispositivos de armazenagem	Análise do volume de dados de uma ligação de voz

Buscou-se determinar se as cifras computacionalmente seguras são vulneráveis a ataques desencadeados por supercomputadores. Buscou-se ainda verificar a viabilidade da implementação da cifra One-Time Pad nas Operações Especiais tendo como indicador de viabilidade verificar se o tamanho da chave necessária para se manter 10 minutos por dia de ligação de voz durante 6 meses de operação é compatível com os dispositivos de armazenamento disponíveis.

3.2 AMOSTRA

A amostra escolhida para estudo foram as cifras e protocolos aprovados e recomendados pelo National Institute of Standards and Technology (NIST), sendo elas a cifra de bloco Rijndael (AES), as cifras assimétricas RSA e Diffie-Hellman, e os protocolos TLS e IPSec, amplamente utilizados em redes virtuais

privadas. Além destas, incluiu-se na amostra a cifra One-Time Pad por ser considerada cifra teoricamente segura. Com relação aos ataques, foram escolhidos aqueles que podem ser desencadeados por um atacante que esteja interceptando a conversa na condição de man-in-the-middle. Os supercomputadores escolhidos para estimativa de tempo de execução do ataque genérico foram o Frontier dos Estados Unidos, o Sunway TaihuLight da China e o Chervonenkis da Rússia tendo em vista a posição de destaque desses supercomputadores na lista pública Top500 e por serem os supercomputadores de maior capacidade desses países de relevante capacidade de inteligência de sinais.

3.3 DELINEAMENTO DA PESQUISA

Quanto a finalidade, essa pesquisa é aplicada, uma vez que propõe adequações práticas à segurança das comunicações do Comando de Operações Especiais.

Quanto aos procedimentos técnicos, essa pesquisa é bibliográfica, uma vez que se vale de livros, publicações e outras pesquisas que estão no estado da arte do tema segurança baseada em criptografia. Contudo, é também uma pesquisa laboratorial, pois foram realizados experimentos para levantamento de estimativas de segurança de cifras computacionais e análises da viabilidade da One-Time Pad.

Quanto a natureza, essa pesquisa é experimental. Foram realizadas experimentações práticas de algoritmos para a quebra de sistemas criptográficos para estimar se o sistema é seguro ou não ao ataque de um supercomputador.

Quanto a forma de abordagem, essa pesquisa é quantitativa e analítica, pois buscou-se identificar o padrão de aumento de tempo de execução de determinado ataque em relação ao aumento do tamanho do módulo de uma cifra assimétrica e então estimar o tempo que um Estado utilizando todo o recurso do seu supercomputador de maior capacidade levaria para realizar o mesmo ataque e comprometer um sistema de segurança.

Quanto aos objetivos, essa pesquisa é explicativa, pois compreende os fatores determinantes da segurança de sistemas criptográficos.

3.4 PROCEDIMENTOS PARA REVISÃO DA LITERATURA

A revisão da literatura foi feita por meio de consulta a manuais militares nacionais e estrangeiros, trabalhos acadêmicos, livros e publicações de referência sobre o assunto criptologia.

Para tal foram consultadas as seguintes bases de dados: Biblioteca de Digital do Exército (BDEx), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Scientific Eletronic Library Online (SciELO) e Google Acadêmico, além de publicações técnicas literárias.

Nessas fontes, buscou-se utilizar as seguintes ideias-chave para pesquisa:

- Segurança das comunicações
- Criptografia
- One-time pad
- Supercomputadores
- Diffie-Hellman
- Virtual Private Network
- Criptoanálise
- Forças Especiais
- Operações Especiais

3.5 INSTRUMENTOS

O instrumento utilizado para a coleta de dados no experimento de ataque genérico sobre a troca de chaves Diffie-Hellman foi uma ficha de coleta de dados (conforme apêndice A), que teve como objetivo registrar os dados obtidos para posterior identificação de padrões relacionados ao aumento do comprimento do módulo.

3.6 ANÁLISE DOS DADOS

Foi registrado o tempo de execução do ataque genérico Baby-Step Giant-Step sobre a troca de chaves Diffie Hellman para tamanhos de módulo de 8 a 31 bits. Após análise dos dados obtidos foi identificado um padrão de aumento de tempo de execução proporcional ao aumento do tamanho do módulo. Dessa

forma foi estimado o tempo que se levaria para comprometer um sistema utilizando módulos maiores e, por comparação de FLOPS do computador utilizado no experimento e dos supercomputadores selecionados como amostra, foi estimada a capacidade destes supercomputadores comprometerem um sistema de segurança baseado em troca de chaves Diffie-Hellman utilizando algoritmo de ataque a módulo genérico.

Utilizando-se dos mesmos registros, foi estimada a necessidade de armazenamento de dados para se realizar o ataque genérico Baby-Step Giant-Step contra sistemas que utilizam módulos maiores.

Foram gerados diversos números primos de 1024 bits com a biblioteca OpenSSL para verificar se há risco de repetição dos números primos comprometendo um esquema efêmero de troca de chaves.

Foi registrado o volume de dados de ligação de voz utilizando dois aplicativos diferentes para identificar o tamanho necessário de chave, em um esquema baseado em One-Time Pad, para realizar 10 minutos de ligações de voz por dia durante 6 meses de operações e assim concluir a viabilidade ou não da utilização da cifra One-Time Pad nas operações especiais.

4. RESULTADOS

4.1 ATAQUE GENÉRICO A TROCA DE CHAVES DIFFIE HELLMAN UTILIZANDO BABY-STEP GIANT-STEP

Através de comando do OpenSSL, conforme quadro 12, foram gerados números primos de 8 a 31 bits.

```
>openssl dhparam -C -2 16
```

QUADRO 12 – Comando utilizado para gerar número primo através do OpenSSL
Fonte: O autor.

Utilizamos o algoritmo de ataque genérico Baby-Step Giant-Step, que tem complexidade O($\sqrt{|G|}$), sendo considerado um dos algoritmos contra primos genéricos de maior performance para resolver o problema computacional do logaritmo discreto. Ressaltamos que existem algoritmos não genéricos que possuirão maior performance, por isso o tamanho do módulo da troca de chave Diffie Hellman não deve se basear na proteção contra ataques genéricos.

Registramos o tempo de execução do algoritmo para observarmos o quanto este tempo aumentava em relação ao aumento de bits no tamanho do módulo P. Para isso, buscamos gerar o maior número primo possível para determinado tamanho do módulo P e adotamos chaves privadas Kpv = P - 2, isto foi feito para que as chaves estivessem no limite posterior da varredura e assim obtessemos um tempo de execução próximo ao máximo possível para aquele tamanho de módulo. Os resultados constam no quadro 13 e no gráfico 1 a seguir.

Tam. (bits)	P	|G|	$\sqrt{\|G\|}$	K Pv	Tempo médio de execução (s)
8	179	178	14	177	0,013
9	467	466	22	465	0,018
10	1019	1018	32	1017	0,023
11	1907	1906	44	1905	0,030
12	3779	3778	62	3777	0,039
13	8147	8146	91	8145	0,05
14	15683	15682	126	15681	0,07
15	32603	32602	181	32601	0,09
16	52379	52378	229	52377	0,12
17	115547	115546	340	115545	0,17
18	262643	262642	513	262641	0,25
19	497507	497506	706	497505	0,33
20	1028579	1028578	1015	1028577	0,48
21	2072699	2072698	1440	2072697	0,67
22	4192547	4192546	2048	4192545	0,97
23	8379467	8379466	2895	8379465	1,40
24	11067803	11067802	3327	11067801	1,65
25	33329579	33329578	5774	33329577	3,30
26	63204347	63204346	7951	63204345	4,81
27	132322643	132322642	11504	132322641	7,50
28	262493579	262493578	16202	262493577	13,28
29	533157683	533157682	23091	533157681	21,62
30	1059702443	1059702442	32554	1059702441	38,93
31	2117289347	2117289346	46015	2117289345	67,14

QUADRO 13 – Tempo de execução GiantStep em troca de chaves Diffie-Hellman utilizando parâmetros curtos
Fonte: O autor.

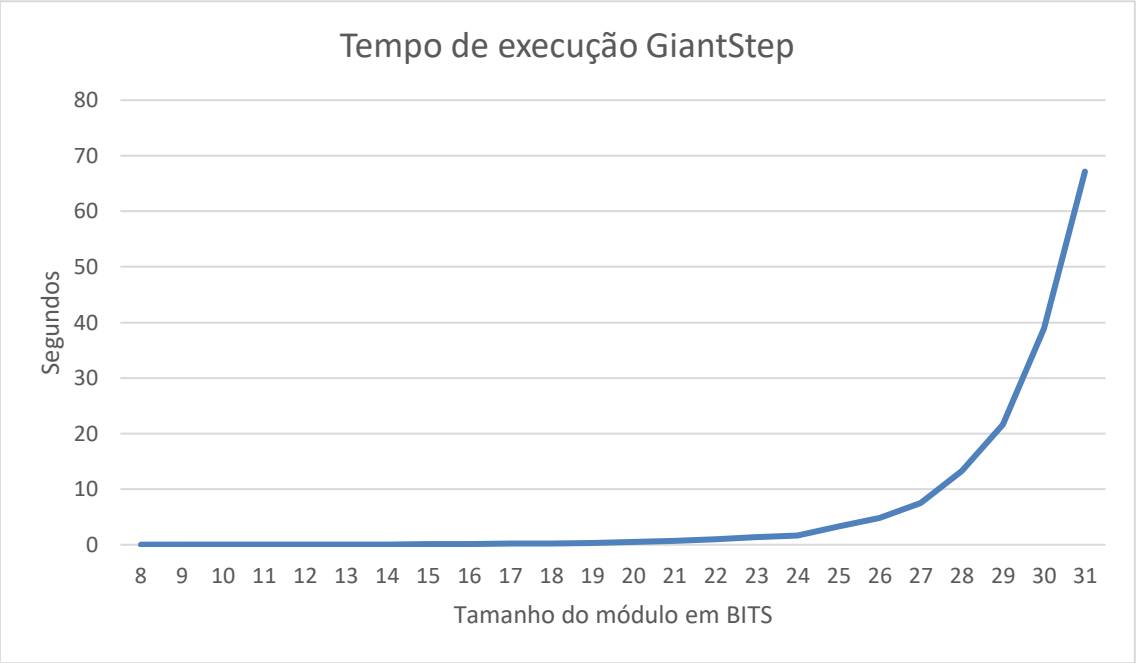


GRÁFICO 1 - Tempo de execução GiantStep à cifra Diffie-Hellman utilizando parâmetros curtos.
Fonte: O autor.

Nesse experimento foi registrado, ainda, o tamanho do banco de dados que foi criado pela primeira fase do algoritmo, chamada BabyStep, conforme quadro 14 e gráfico 2, a seguir.

Tam. (bits)	P	|G|	$\sqrt{\|G\|}$	K Pv	Tamanho Banco de Dados (bytes)
8	179	178	14	177	145
9	467	466	22	465	232
10	1019	1018	32	1017	337
11	1907	1906	44	1905	478
12	3779	3778	62	3777	676
13	8147	8146	91	8145	993
14	15683	15682	126	15681	1380
15	32603	32602	181	32601	2039
16	52379	52378	229	52377	2704
17	115547	115546	340	115545	4197
18	262643	262642	513	262641	6453

19	497507	497506	706	497505	8989
20	1028579	1028578	1015	1028577	13038
21	2072699	2072698	1440	2072697	18551
22	4192547	4192546	2048	4192545	26459
23	8379467	8379466	2895	8379465	37482
24	11067803	11067802	3327	11067801	43928
25	33329579	33329578	5774	33329577	79283
26	63204347	63204346	7951	63204345	110014
27	132322643	132322642	11504	132322641	160272
28	262493579	262493578	16202	262493577	226138
29	533157683	533157682	23091	533157681	322692
30	1059702443	1059702442	32554	1059702441	455379
31	2117289347	2117289346	46015	2117289345	657099

QUADRO 14 – Tamanho do banco de dados BabyStep utilizando parâmetros curtos
Fonte: O autor.

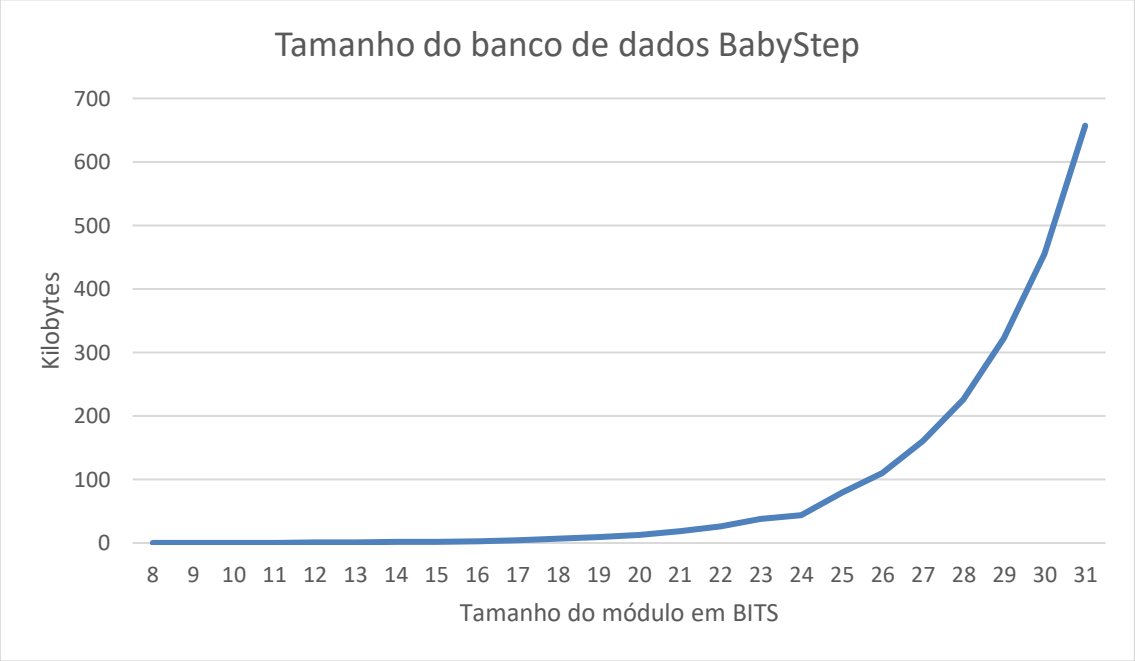


GRÁFICO 2 - Tamanho do banco de dados BabyStep utilizando parâmetros curtos.
Fonte: O autor.

Para chegar a esses resultados foi utilizado um PC i7-10510U 1,80 GHz (8 CPUs) 64 bits com 8192 MB de memória RAM executando uma implementação multithreading em C# que alcançou em média 90% da utilização da CPU, conforme figura 9.

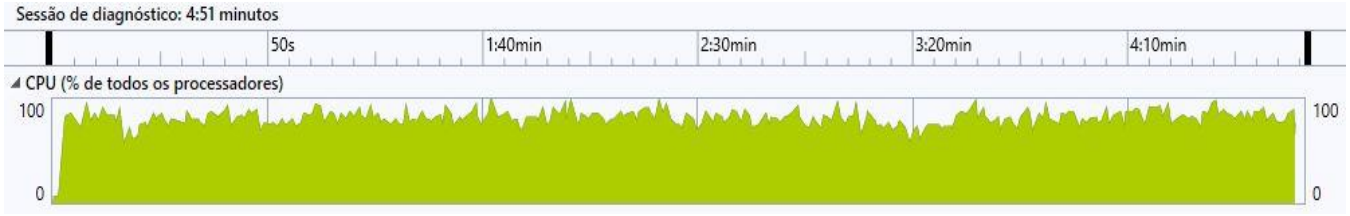


FIGURA 11 - Utilização de CPU durante execução do algoritmo Baby-Step Giant-Step
Fonte: Analisador de Perfil do Visual Studio 2019.

4.2 ANÁLISE DE PRIMOS GERADOS PELA BIBLIOTECA OPENSSL

Foram analisados 5080 números primos de 1024 bits gerados por linha de comando da biblioteca OpenSSL. Para isso foi utilizado o comando do quadro 15.

```
>openssl dhparam -text -2 1024
```

QUADRO 15 – Comando utilizado para gerar número primo através do OpenSSL
Fonte: O autor

Da análise dos números primos gerados foi observado que nenhum número primo se repetiu e que todos eram considerados primos seguros, isto é (P – 1) / 2 corresponde a outro número primo.

4.3 VOLUME DE DADOS EM LIGAÇÃO DE VOZ

Através do WireShark foi analisado o volume de dados enviados e recebidos sobre o protocolo UDP em uma ligação de voz de 10 minutos. Foi utilizado o aplicativo WhatsApp e o aplicativo Telegram. Os resultados obtidos constam no quadro 16, a seguir:

Aplicativo	Bytes enviados e recebidos
WhatsApp	4.781.534 bytes
Telegram	4.993.193 bytes

QUADRO 16 – Volume de dados em ligação de voz de 10 minutos
Fonte: O autor

5. DISCUSSÃO DOS RESULTADOS

5.1 BABY-STEP GIANT-STEP

Após computarmos o tempo de execução do algoritmo em relação ao aumento do tamanho do módulo P, conforme quadro 9 na seção anterior, verificamos que o aumento percentual do tempo de execução se manteve quase constante. Não poderia ser constante uma vez que os módulos P não têm diferença exata entre si resultando em um aumento irregular da quantidade de elementos do corpo finito gerado pelo próximo módulo P, porém esse aumento é limitado ao tamanho do módulo P que é equivalente a ordem crescente das potências de 2 e, no caso do algoritmo BabyStep GiantStep, esse aumento corresponde a aproximadamente 1,414 vezes por bit, já que esse algoritmo diminui a complexidade da tarefa à raiz quadrada da ordem do corpo finito.

Em acordo com o esperado, a cada bit adicionado ao módulo P encontramos, em média, um aumento de 1,462 vezes no tempo de execução. Conforme gráfico 3.

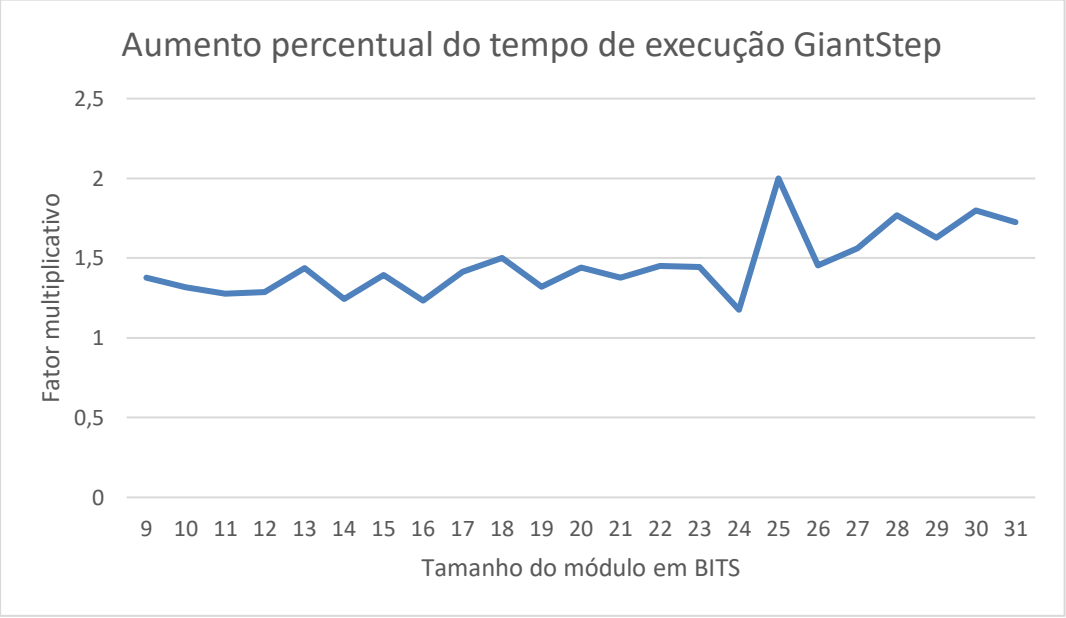


GRÁFICO 3 – Aumento percentual do tempo de execução. Desvio padrão: 0,2.
Fonte: O autor.

Utilizamos essa média do aumento do tempo de execução como razão de uma progressão geométrica para estimar o tempo que nosso PC levaria para quebrar sistemas baseados na troca de chave Diffie Hellman com parâmetros

maiores. A partir daí comparamos os dados do fabricante sobre a capacidade de realização de operações de ponto flutuante por segundo (FLOPS) do nosso PC com a capacidade de FLOPS dos supercomputadores americano, russo e chinês mais bem classificados na lista Top500 de junho de 2022 para estimar a capacidade desses países de quebrar um sistema baseado na troca de chave Diffie Hellman com o algoritmo BabyStep GiantStep. As estimativas constam no quadro 17, a seguir.

Tam. do módulo P (bits)	PC i7-10510U	Frontier 	Sunway TaihuLight 	Chervonenkis 
	115,2 GFLOPS	1102 PFLOPS	93 PFLOPS	21,53 PFLOPS
	Tempo para comprometer a segurança (em **anos**[4])			
90	14096,10156	0,001474	0,017460977	0,075423637
91	28379,63168	0,002967	0,035154124	0,151850143
92	54635,73538	0,005711	0,067677814	0,29233798
93	102120,9348	0,010675	0,12649819	0,546415778
94	192007,2726	0,020072	0,237841267	1,027368221
95	403354,1654	0,042166	0,499638708	2,158216435
96	732553,7443	0,076579	0,907421412	3,919655891
97	1491556,386	0,155923	1,84760533	7,980831198
98	2686499,286	0,280839	3,327792664	14,37458048
99	5559312,47	0,581155	6,886374156	29,74606579
100	12196912,25	1,275031	15,10843324	65,26169489
101	23574892,29	2,464453	29,20244722	126,1415509
102	49706833	5,196213	61,57233507	265,9650331
103	100163737,3	10,470837	124,0737907	535,9434527
104	212511901,4	22,215400	263,2405488	1137,081795
105	449005704,4	46,937801	556,1877112	2402,482914

QUADRO 17 – Estimativas de tempo de execução de Giant-Step por supercomputadores
Fonte: O autor.

[4] Os dados em vermelho correspondem aos tempos de execução sem oportunidade para revelar um segredo ultrassecreto, uma vez que este tem validade de 25 anos.

Uma vez que a maioria dos sistemas que realizam trocas de chaves Diffie Hellman hoje já possuem módulo P de 1024 bits ou mais com a finalidade de proteger-se de ataques não genéricos, observa-se que, com base em nosso experimento, o algoritmo Baby-Step Giant-Step não seria eficaz para a criptoanálise mesmo com recursos a nível de Estado. Além disso, há necessidade de uma grande capacidade de armazenamento, cuja nossa estimativa é apresentada no gráfico 4 a seguir.

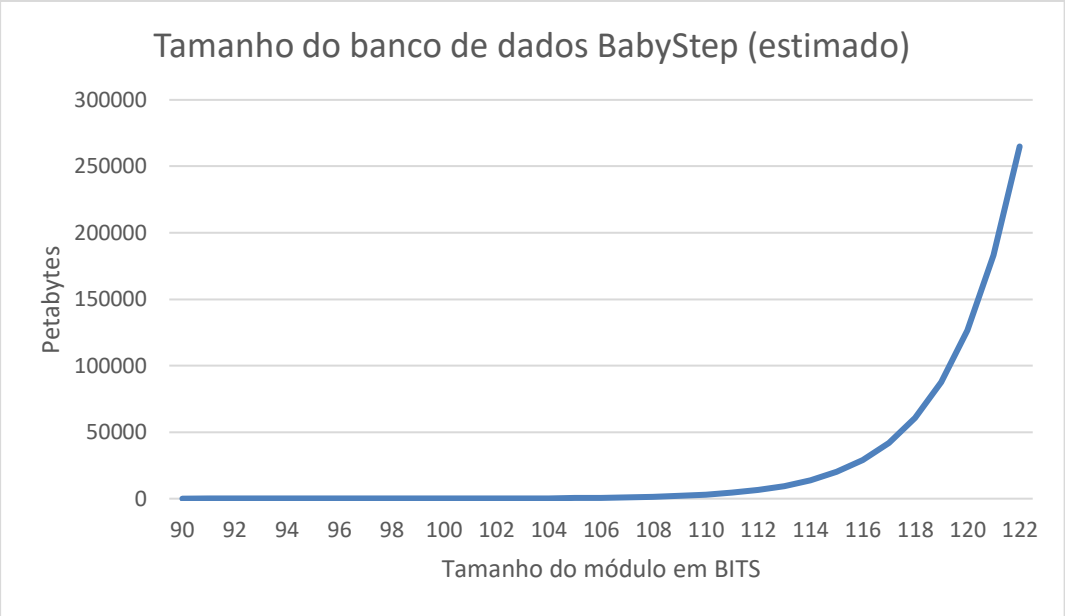


GRÁFICO 3 – Estimativa para tamanho de dados BabyStep.
Fonte: O autor.

É importante ressaltar que esses resultados foram obtidos com o algoritmo Baby-Step Giant-Step que é um algoritmo para atacar um módulo P genérico. Contra números primos específicos existem algoritmos com maior performance, como o Number Field Sieve conforme demonstrado por Adrian, David et Al (2015). **Estes algoritmos contra primos específicos são responsáveis pela recomendação atual do tamanho de 2048 bits para módulos Diffie-Hellman** e pela necessidade de mudar os números primos com frequência num esquema efêmero de troca de chaves.

5.2 PRIMOS GERADOS PELO OPENSSL

Conforme verificamos, todos os números primos de 1024 bits gerados por linha de comando da biblioteca OpenSSL no experimento citado na seção 4.2

eram primos seguros e não se repetiram. Sendo assim, concluímos que a biblioteca OpenSSL está gerando primos com segurança adequada para um esquema efêmero de troca de chaves Diffie-Hellman, contudo não foi analisado se a aleatoriedade com que esses primos são gerados é criptograficamente segura.

5.3 VIABILIDADE DA ONE-TIME PAD NAS OPERAÇÕES ESPECIAIS

Com base nos resultados apresentados na seção 4.3, observa-se que em uma ligação de voz de 10 minutos são transmitidos (enviados ou recebidos) menos do que 5 MB. Uma vez que a cifra One-Time Pad requer 1 byte de chave para cada byte de mensagem a ser transmitida, concluímos que 5 MB de chave seriam adequados para proteger 10 minutos de ligação de voz em um esquema baseado em One-Time Pad. Considerando uma operação de 6 meses, na qual ocorram ligações diárias de 10 minutos para reportar a situação da Eq Prec FEsp para a BOBFEsp, a necessidade de memória para armazenar a chave em um esquema One-Time Pad seria de 900 MB.

A partir dessas estimativas concluímos que um esquema de criptografia baseado em One-Time Pad é viável nas operações especiais. Além disso, um esquema baseado em One-Time Pad apresenta vantagens práticas sobre os esquemas computacionalmente seguros, uma vez que não pode ser comprometido por criptoanálise independente do poder computacional do inimigo.

6. CONCLUSÃO

A grande distância geográfica entre a Eq Prec FEsp e a BOBFEsp impõe a necessidade do estabelecimento de um comando e controle de longo alcance. A ausência de apoio militar na AOGI e as peculiaridades da fase de contato inicial com a força irregular, levam a necessidade da Eq Prec FEsp se valer de meios de comunicação não convencionais com segurança uma vez que, por vezes, serão tramitados dados ultrassecretos inerentes a atividade das Forças Especiais.

Após revisão sumária das principais cifras utilizadas pelos protocolos IPSec e TLS e identificação dos ataques conhecidos mais eficientes sobre essas cifras, concluímos que para proteger seu sistema de comando e controle o Comando de Operações Especiais poderá se apoiar em uma adequada implementação de Virtual Private Network (VPN), observando cuidadosamente os parâmetros das cifras criptográficas, as configurações e atualizações dos serviços e os protocolos de rede que serão utilizados. Como produto desta pesquisa, sintetizamos tais recomendações no apêndice B.

Face ao exposto neste trabalho, notamos que a maior vulnerabilidade nos sistemas de comunicações protegidos por criptografia são erros na configuração e implementação. Implementações com parâmetros para negociação de chaves menores que 2048 bits podem estar suscetíveis a ataques de supercomputadores. Já nos sistemas corretamente implementados e configurados a maior vulnerabilidade está na troca de chaves realizada por cifras assimétricas. Ainda que as cifras assimétricas, corretamente empregadas, proporcionem um elevado grau de segurança, não é possível afirmar que a proteção baseada no problema do logaritmo discreto ou da fatoração de grandes inteiros não possa ser ameaçada por uma descoberta na área da matemática ou por desenvolvimento tecnológico – como já vem sendo estimado devido as pesquisas para o desenvolvimento do computador quântico.

Apesar da possibilidade do comprometimento da segurança da comunicação através de ataques empregando recursos estatais sobre cifras assimétricas ser bastante mitigada com a utilização de esquemas efêmeros de troca de chaves, consideramos como alternativa adequada e viável para a proteção das comunicações que tramitam dados ultrassecretos a implementação de uma aplicação de Voz sobre IP (VoIP) baseada em One-Time Pad, uma vez

que esta cifra fornece vantagem prática sobre as cifras computacionalmente seguras.

Propomos um serviço de Voz sobre IP hospedado em uma VPN (configurada conforme recomendações no apêndice B) e com criptografia na camada de aplicação baseada na cifra One-Time Pad. Essa VPN não deve ter saída para a Internet. Smartphones com a BOBFEsp e com elementos da Eq Prec FEsp deverão estar configurados para acessar a VPN (não deverão desativar a VPN em nenhuma situação) e deverão possuir um aplicativo de Voz sobre IP que utilize criptografia baseada em One-Time Pad. Tanto o servidor quanto a VPN deverão ser administrados pelo Exército Brasileiro (COpEsp ou CTA). Conforme calculado na seção anterior, para uma operação de 6 meses cada smartphone deverá ter 1 gigabyte de chave One-Time Pad distinta das chaves dos demais smartphones. O servidor de Voz sobre IP deverá possuir todas as chaves. O esquema desta implementação de comando e controle para tramitar dados ultrassecretos entre a Eq Prec FEsp e a BOBFEsp está ilustrado na figura 12, a seguir:

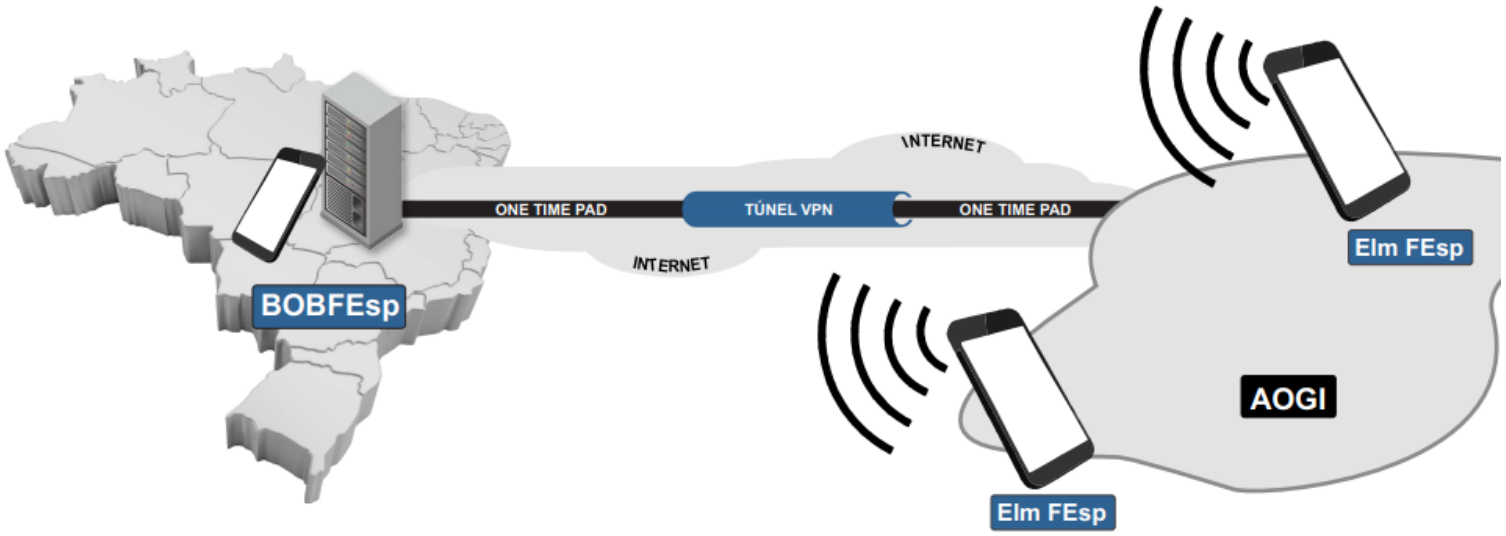


FIGURA 12 – Proposta de implementação para proteção do C² de operações especiais
Fonte: O autor

Para gerar esse banco de chaves One-Time Pad aleatórias propomos uma implementação em rede privada local que utilize o tempo entre o pressionar das teclas do teclado e movimentos do mouse dos computadores ligados a rede para gerar as chaves, de forma a utilizar o fator humano para garantir um banco

de chaves com chaves realmente aleatórias. Após reunir esse banco de chaves ele deve ser embaralhado aleatoriamente antes de ser incluído no banco de chaves do servidor VoIP. Devem ser adotadas medidas de segurança para a inserção de chaves no servidor VoIP, não deve haver implementação sem autenticação que manipule o banco de chaves remotamente.

Sendo o comando e controle adequado um fator de êxito das operações especiais e a cifra One-Time Pad o mais poderoso recurso para proteção da informação frente as ameaças dos dias de hoje, cifra a qual comprovamos a viabilidade nas operações especiais, concluímos que a proteção cibernética proporcionada pelo esquema que sugerimos desenvolve a capacidade militar terrestre de superioridade de informações garantindo às operações especiais um enlace de comunicação rápido e um canal de comando e controle seguro empregando meios compatíveis com as particularidades das operações especiais.

REFERÊNCIAS

ADRIAN, David et al. **Imperfect Forward Secrecy:** How Diffie-Hellman Fails in Practice. Denver, Colorado, EUA, 2015.

ALSHAMSI, AbdelNasir e SAITO, Takamichi. **A Technical Comparison of IPSec and SSL**, 2004. 10 f. TOKYO UNIVERSITY OF TECHNOLOGY. Hachioji City, Tokyo, Japão, 2004.

AUMASSON, Jean-Philippe. **Serious Cryptography:** a practical introduction to modern encryption. 1. ed. San Francisco: No Starch Press, 2018. 312 p.

BRASIL. Exército. **EB10-IG-01.011 Instruções Gerais para a Salvaguarda de Assuntos Sigilosos**, 1. ed., Brasília, DF, 2014.

BRASIL. Exército. **EB70-MC-10.212 Operações Especiais**, 3. ed., Brasília, DF, 2017.

BRASIL. Exército. **EB70-MC-10.305 O Comando de Operações Especiais**, 1. ed., Brasília, DF, 2019.

BRASIL. Exército. **EB70-MC-10.232 Guerra Cibernética**, 1. ed., Brasília, DF, 2017.

BRASIL. Exército. **C 24-50 Segurança das Comunicações**, 1. ed., Brasília, DF, 1978.

BRASIL. Exército. Centro de Instrução de Operações Especiais. **NA 2-7 Guerra Irregular**, 1. ed. Niterói, RJ, 2020.

CCM.net. O que é TCP/IP, como funciona e para que serve. 2020. Disponível em: <https://br.ccm.net/faq/12065-o-que-e-tcp-ip-como-funciona-e-para-que-serve>. Acesso em: 1 de mar. de 2022.

CISCO. **Visual Networking Index**. EUA. 2010.

ELIAS, G.; LOBATO, L. C. **Arquitetura e Protocolos de Rede TCP-IP**. 2. ed. Rio de Janeiro: Escola Superior de Redes, 2013. 414 p.

EUA, Department of Defense, **JP 3-05.1 Unconventional Warfare Pocket Guide**, 1. ed., Washington, DC, EUA, 2016.

EUA. Department of Commerce. **NIST Special Publication 800-57:** Recommendation for Key Management Part 1, Washington, D.C., EUA, 2020.

EUA. National Security Act of 1947. **To promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with Other departments and agencies of the**

Government concerned with the national security. Washington, DC, EUA, 1947.

GREEN, M. D. Prefácio In: AUMASSON, Jean-Philippe. **Serious Cryptography:** a practical introduction to modern encryption. 1. ed. San Francisco: No Starch Press, 2018. 312 p.

GÜNEYSU, Tim et al. **Cryptoanalysis with COPACOBANA**. 2008. 16 f. IEEE TRANSACTIONS ON COMPUTERS.

ISO; IEC. **27001**: Information technology — Security techniques — Information security management systems — Requirements. Suíça. 2013.

ISO; IEC. **7498-1**: Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. Suíça. 1994.

JORGE, Bernardo Wahl Gonçalves de Araújo. **As Forças de Operações Especiais dos Estados Unidos e a Intervenção no Afeganistão: Um Novo Modo de Guerra Americano?** 2009. 135 f. Dissertação (Relações Internacionais) – UNESP, UNICAMP e PUC-SP, São Paulo, 2009

KERRIGAN, Michael. **Enigma:** a verdadeira história da quebra do código secreto e como ajudou a vencer a segunda guerra mundial. 1. ed. São Paulo: M. Books do Brasil, 2020. 224 p.

KUMAR, Sandeep et al. **Breaking Ciphers with COPACOBANA – A Cost-Optimized Parallel Code Breaker**. 15 f. Horst Görtz Institute for IT Security, Ruhr University Bochum, Institute of Computer Science and Applied Mathematics, Faculty of Engineering, Christian-Albrechts-University of Kiel. Alemanha

KUROSE, J.; ROSS, K. **Rede de Computadores e a Internet:** uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013. 634 p.

LIM, Chae Hoon; LEE, Pil Joong, **A Key Recovery Attack on Discrete Log-based Schemes Using a Prime Order Subgroup**. 1997. 15 f. Information and Communications Research Center, Future Systems, Seoul, KOREA; Dept. of Electronic and Electrical Engineering, Pohang University of Science and Technology (POSTECH), Pohang, KOREA. 1997.

MOORE, Gordon E., **Cramming more components onto integrated circuits**. 1965. 4 f. Eletronics Vol 38. Califórnia, EUA, 1965.

PAAR, C.; PELZL, J. **Understanding cryptography:** a textbook for students and practitioners. 2. ed. Heidelberg: Springer, 2010. 372 p.

Plano Estratégico do Exército (2020-2023). Disponível em: <https://www.ceadex.eb.mil.br>. Acesso em: 27 de fev. de 2022.

SHANNON, Claude E., **Communication Theory of Secrecy Systems**, 1949. 60 f. Bell System Technical Journal, Nova York, EUA, 1949.

STONE, Kathryn, **“All Necessary Means” – Employing CIA Operatives In a Warfighting Role Alongside Special Operations Forces**. 2003. 55 f. Strategy Research Project – US Army War College, Pensilvânia, EUA, 2003.

VERRASTRO, Pedro Arnaldo Amorim. **Emprego de Destacamentos Operacionais de Forças Especiais no Estabelecimento de Áreas Operacionais de Guerra Irregular**. 1993. 48 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 1993.

APÊNDICE A – FICHA DE COLETA DE DADOS BABY-STEP GIANT-STEP

Tam. Módulo P	P	Ord	M ($\sqrt{Ord}$)	K Pv	Tam. Banco de dados	Throughput Escrita	Tempo de Execução Baby-Step	Throughput Leitura	Tempo de Execução Giant-Step

APÊNDICE B – RECOMENDAÇÕES DE SEGURANÇA PARA VPN

IPSec Mode	Tunnel
Auth Protocol	Certificado*
Key Exchange	IKEv2
Perfect Forward Secrecy	On
Encryption	aes-256 (nunca utilizar modo de operação ECB, recomendada-se utilizar CBC)
Integrity	sha-256
Diffie-Hellman group	Group 14 (2048 bits)

***** Caso não seja possível gerenciar certificados digitais a chave pré compartilhada (Pre Shared Key) deve ser totalmente aleatória e alterada com a frequência que for viável, nesse caso a probabilidade de um atacante a nível de Estado comprometer a segurança da rede aumentará significativamente.